

TC.
ANKARA ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
KAMU HUKUKU ANABİLİM DALI

**BİLİŞİM SİSTEMİNE GİRME (TCK 243) VE SİSTEMİ
ENGELLEME, BOZMA, VERİLERİ YOK ETME VEYA
DEĞİŞTİRME (TCK 244) SUÇLARI**

Tezli Yüksek Lisans Tezi

Melike Hafsa MUCUK

ANKARA 2022

TC.
ANKARA ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
KAMU HUKUKU ANABİLİM DALI

**BİLİŞİM SİSTEMİNE GİRME (TCK 243) VE SİSTEMİ
ENGELLEME, BOZMA, VERİLERİ YOK ETME VEYA
DEĞİŞTİRME (TCK 244) SUÇLARI**

Tezli Yüksek Lisans Tezi

Melike Hafsa MUCUK

**Tez Danışmanı
Prof. Dr. Muharrem ÖZEN**

ANKARA 2022

TC.
ANKARA ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
KAMU HUKUKU ANABİLİM DALI

**BİLİŞİM SİSTEMİNE GİRME (TCK 243) VE SİSTEMİ
ENGELLEME, BOZMA, VERİLERİ YOK ETME VEYA
DEĞİŞTİRME (TCK 244) SUÇLARI**

Yüksek Lisans Tezi

Tez Danışmanı
Prof. Dr. Muharrem ÖZEN

Tez Jürisi Üyeleri

Adı ve Soyadı

İmzası

- 1- Prof. Dr. Muharrem ÖZEN
- 2- Prof. Dr. Metin FEYZİOĞLU
- 3- Doç. Dr. Önder TOZMAN

Tez Savunma Tarihi

20.07.2022

T.C.
ANKARA ÜNİVERSİTESİ
Sosyal Bilimler Enstitüsü Müdürlüğü'ne,

Prof. Dr. Muharrem ÖZEN danışmanlığında hazırladığım “BİLİŞİM SİSTEMİNE GİRME (TCK 243) VE SİSTEMİ ENGELLEME, BOZMA, VERİLERİ YOK ETME VEYA DEĞİŞTİRME (TCK 244) SUÇLARI (Ankara 2022)” adlı yüksek lisans tezimdeki bütün bilgilerin akademik kurallara ve etik davranış ilkelerine uygun olarak toplanıp sunulduğunu, başka kaynaklardan aldığım bilgileri metinde ve kaynakçada eksiksiz olarak gösterdiğimi, çalışma sürecinde bilimsel araştırma ve etik kurallarına uygun olarak davrandığımı ve aksinin ortaya çıkması durumunda her türlü yasal sonucu kabul edeceğimi beyan ederim.

20.07.2022

MELİKE HAFSA MUCUK

İÇİNDEKİLER

İÇİNDEKİLER	i
KISALTMALAR	iv
GİRİŞ	1
BİRİNCİ BÖLÜM	4
BİLİŞİM ALANINDA SUÇLARA İLİŞKİN GENEL AÇIKLAMA VE TEMEL KAVRAMLAR.....	4
I. GENEL OLARAK	4
II. KAVRAMLAR.....	6
A. BİLİŞİM	6
B. BİLİŞİM SİSTEMİ	7
C. BİLİŞİM SİSTEM AĞLARI	12
D. VERİ	13
E. BİLİŞİM SUÇLARI	15
a. TERİM SORUNU	15
b. TANIM SORUNU	17
c. BİLİŞİM SUÇLARININ TASNİFİ	19
F. BİLİŞİM ALANINDAKİ SUÇLARA İLİŞKİN DÜZENLEMELER	21
a. AVRUPA KONSEYİ SİBER SUÇ SÖZLEŞMESİ	21
b. TÜRK HUKUKUNDA BİLİŞİM ALANINDA SUÇLAR	23
1. Tarihsel Gelişim	23
2. Düzenleniş Biçimi.....	25
İKİNCİ BÖLÜM.....	28
BİLİŞİM SİSTEMİNE GİRME SUÇU	28
I. GENEL OLARAK	28
A. HUKUKİ KONU	32
B. MADDİ KONU	34
C. FAİL.....	34
D. MAĞDUR.....	35
E. SUÇUN UNSURLARI.....	38
a. MADDİ UNSUR.....	38
b. MANEVİ UNSUR.....	49
c. HUKUKA AYKIRILIK	51
F. SUÇA ETKİ EDEN HALLER	57
a. DAHA AZ CEZAYI GEREKTİREN HAL.....	57

b. NETİCESİ SEBEBİYLE AĞIRLAŞMIŞ HAL.....	61
G. SUÇUN ORTAYA ÇIKIŞ BİÇİMLERİ.....	64
a. TEŞEBBÜS.....	64
b. İŞTİRAK	66
c. İÇTİMA	68
H. YAPTIRIM, SORUŞTURMA, KOVUŞTURMA.....	74
II. VERİ NAKİLLERİNİN TEKNİK ARAÇLARLA İZLENMESİ SUÇU (TCK 243/4).....	77
A. GENEL OLARAK	77
B. MADDİ KONU	78
C. HUKUKİ KONU	79
D. FAİL.....	80
E. MAĞDUR.....	81
F. SUÇUN UNSURLARI.....	82
a. MADDİ UNSUR.....	82
b. MANEVİ UNSUR.....	85
c. HUKUKA AYKIRILIK	86
G. SUÇUN ÖZEL GÖRÜNÜŞ BİÇİMLERİ	87
a. TEŞEBBÜS.....	87
b. İŞTİRAK	88
c. İÇTİMA	89
H. SORUŞTURMA, KOVUŞTURMA, YAPTIRIM.....	91
ÜÇÜNCÜ BÖLÜM	92
SİSTEMİ ENGELLEME, BOZMA, VERİLERİ YOK ETME VEYA DEĞİŞTİRME SUÇLARI.....	92
I. GENEL OLARAK	92
A. HUKUKİ KONU	96
B. MADDİ KONU	98
C. FAİL.....	101
D. MAĞDUR.....	103
E. SUÇUN UNSURLARI.....	106
a. MADDİ UNSUR.....	106
b. MANEVİ UNSUR.....	129
c. HUKUKA AYKIRILIK	131
F. SUÇA ETKİ EDEN SEBEPLER	134
G. SUÇUN ORTAYA ÇIKIŞ BİÇİMLERİ.....	137
a. TEŞEBBÜS.....	137

b. İŞTİRAK	138
c. İÇTİMA	139
1. Genel Olarak	139
H. YAPTIRIM, SORUŞTURMA, KOVUŞTURMA.....	149
II. BİLİŞİM SİSTEMİ ARACILIĞIYLA HAKSIZ YARAR SAĞLAMA SUÇU	152
A. GENEL OLARAK	152
B. HUKUKİ KONU	155
C. MADDİ KONU	155
D. FAİL.....	158
E. MAĞDUR.....	158
F. SUÇUN UNSURLARI.....	159
a. MADDİ UNSUR.....	159
b. MANEVİ UNSUR.....	162
c. HUKUKA AYKIRILIK	163
G. SUÇUN ÖZEL GÖRÜNÜŞ ŞEKİLLERİ	163
a. TEŞEBBÜS.....	163
b. İŞTİRAK	165
c. İÇTİMA	167
İ. YAPTIRIM, SORUŞTURMA, KOVUŞTURMA.....	180
SONUÇ	183
KAYNAKÇA.....	187
ÖZET	194
ABSTRACT.....	195

KISALTMALAR

ABÜHFD	: Antalya Bilim Üniversitesi Hukuk Fakültesi Dergisi
AIHS	: Avrupa İnsan Hakları Sözleşmesi
AKSSS	: Avrupa Konseyi Siber Suç Sözleşmesi
AÜHFD	: Ankara Üniversitesi Hukuk Fakültesi Dergisi
AÜSBFD	: Ankara Üniversitesi Siyasal Bilgiler Fakültesi Dergisi
AYM	: Anayasa Mahkemesi
Bkz.	: Bakınız
BM	: Birleşmiş Milletler
C.	: Cilt
CD	: Ceza Dairesi
CMK	: Ceza Muhakemesi Kanunu
DEÜHFD	: Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi
E.	: Esas
EİK	: Elektronik İmza Kanunu
EÜHFD	: Erciyes Üniversitesi Hukuk Fakültesi Dergisi
ETCK	: Eski Türk Ceza Kanunu
FSEK	: Fikir ve Sanat Eserleri Kanunu
GÜHFD	: Galatasaray Üniversitesi Hukuk Fakültesi Dergisi
HHFD	: Hacettepe Hukuk Fakültesi Dergisi
HSK	: Hakimler Savcılar Kurulu
İÜHFM	: İstanbul Üniversitesi Hukuk Fakültesi Mecmuası
K.	: Karar
K.T.	: Karar Tarihi
OECD	: Ekonomik İş Birliği ve Kalkınma Örgütü
S.	: Sayılı
s.	: Sayfa
SDÜHFD	: Süleyman Demirel Üniversitesi Hukuk Fakültesi Dergisi
ss.	: Sayfa Sayısı
T.	: Tarih
TBBD	: Türkiye Barolar Birliği Dergisi

TCK : Türk Ceza Kanunu
YCGK : Yargıtay Ceza Genel Kurulu



GİRİŞ

Teknolojik gelişmeler sonucu yaşanan sosyo-ekonomik dönüşüm toplumu, hayatın neredeyse tüm alanlarında derinden etkilemiş ve bu dönem toplumu “bilgi toplumu” adıyla anılmaya başlanmıştır. Teknolojik gelişmelerin sonucu olarak yaşanan bilişim devrimi, bilginin işlenmesi ve saklanması alanında da kendini göstermiş; coğrafi sınırlar önemsiz hale gelerek bilgiye ulaşmada, bilginin aktarılmasında yaşanan radikal değişim insan hayatını her yönüyle etkisi altına almıştır.¹ Bilginin işlenmesi ve iletilmesi çok kolay bir hale geldiğinden, söz konusu teknolojilerin kötüye kullanılması ihtimali karşısında bilgilerin ve bilhassa özel hayatın gizliliği bağlamında kişisel verilerin korunması ihtiyacı ortaya çıkmıştır.² Zira insan hayatı için faydalı olması amacıyla geliştirilen bilişim teknolojilerinin kötü niyetli kimseler tarafından suiistimal edilmesi, yeni suç tiplerinin ortaya çıkması ve kanunda mevcut bazı suçların yeni metotlarla işlenmesinde bu teknolojilerin araç olarak kullanılması durumunu doğurmuştur.³ Mevcut mevzuatlar bu suçların cezalandırılmasında yetersiz kaldığından ve suçların sınır aşan yapısından dolayı bu suçlarla mücadele etmek için gerek ulusal gerek uluslararası çalışmalar yapılmıştır.

Bilişim teknolojilerinde yaşanan süratli gelişmeler, bu gelişmelere paralel yeni düzenleme yapılmasını dahi zora sokmaktadır. Çünkü yapılan bu düzenlemelerin kapsamı ne kadar geniş oluşturulsa oluşturulsun, bu düzenlemelerin gelecekte çıkacak sorunlar bakımından yetersiz kalması kaçınılmazdır. Teknolojik araçların kullanılması suretiyle

¹ Yenidünya, Caner / Değirmenci, Olgun, **Mukayeseli Hukukta ve Türk Hukukunda Bilişim Suçları**, İstanbul, Legal Yayınevi, 2003, s. 13-14.

² Tezcan, Durmuş, “Bilgisayar Karşısında Özel Hayatın Korunması”, **Anayasa Yargısı 8 (Anayasa Mahkemesinin 29.Kuruluş Yıldönümü Sempozyumu, Ankara, 25-27 Nisan 1991)**, s. 385.

³ Yenidünya/ Değirmenci, s. 14; Sokullu Akıncı, Füsün, “Avrupa Konseyi Siber Suç Sözleşmesinde Yer Alan Maddi Ceza Hukukuna İlişkin Düzenlemeler ve Özellikle İnternette Çocuk Pornografisi”, **İÜHFİM**, C. 59, S. 1-2 2001, s. 11-12.

veya bunlara karşı haksızlık teşkil eden fiillerin işlenmesi, söz konusu araçların ve içerisindeki verilerin korunması ihtiyacını ortaya çıkarmıştır. Ancak bu koruma haksızlık içeriğine göre farklı hukuk dallarındaki müeyyidelerle sağlanabilecek nitelikteyse ceza hukukunda geçerli olan ultima ratio ilkesi gereğince önce özel hukuk veya idare hukuku yaptırımlarına başvurulacak; bu müeyyidelerle korumanın yetersiz kaldığı durumda cezai müeyyidelere başvurulacaktır.⁴

Nihayetinde diğer hukuk dallarındaki müeyyidelerin yetersiz kalması sonucu haksızlık içeriği fazla olan bazı fiillerin suç olarak öngörülmesi zorunluluğu doğmuştur. Zira bu fiillerin biçimsel kanunilik ilkesi ve kıyas yasağı gereği mevzuattaki mevcut suç tipleriyle cezalandırılması mümkün değildir. Gerçekten de bir verinin elde edilmesi durumunda, taşınır bir malın bulunduğu yerden alınması söz konusu olmadığından, bu fiil hırsızlık suçu içerisinde; verinin silinmesi durumundaysa fiziken bir müdahale olmadığından ve veri mal kavramı içinde değerlendirilebilecek bir değer olmadığından, bu fiil mala zarar verme suçu içerisinde değerlendirilemeyecektir. Klasik suç tipleriyle cezalandırılmayan bu tarz yeni değer ihlalleri örneğin bilişim sistemine girme, sistemi engelleme gibi fiiller mevcut suçlardan hiçbirinin tipikliğine uymadığından cezasız kalacaktır. Ancak yeni düzenlemelerle bu durum engellenmiş, hak ihlallerinin cezasız kalmasının önüne geçilmiştir.

Bilişim suçları 5237 S TCK'nın Özel Hükümler Kitabının “*Topluma Karşı Suçlar*” kısmının onuncu bölümünde 243 ve 246. maddeleri arasında “*Bilişim Alanında Suçlar*” başlığı altında hüküm altına alınmıştır. Onuncu bölümde sırasıyla “*Bilişim sistemine girme*” (TCK 243), “*Sistemi engelleme, bozma, verileri yok etme veya değiştirme*” (TCK 244), “*Banka veya kredi kartlarının kötüye kullanılması*” (TCK 245), “*Yasak cihaz veya programlar*” (TCK 245/A), “*Tüzel kişiler hakkında güvenlik tedbiri*

⁴ Ersoy, Yüksel, “Genel Hukuki Koruma Çerçevesinde Bilişim Suçları”, AÜSBFD, C. 49, S. 3, 1994, s. 155-156.

uygulanması” (TCK 246) madde başlıkları altında tipik fiiller ve bu fiiller karşılığında uygulanacak yaptırım gösterilmiştir.

Çalışmamızın amacı bilişim alanındaki suçlardan TCK 243 (bilişim sistemine girme suçu) ve TCK 244. (Sistemi engelleme, bozma, verileri yok etme ve değiştirme suçları) maddelerinin incelenmesidir. Bu inceleme çerçevesinde ilk bölümde bilişim alanına ilişkin genel açıklamalara ve tanımlara yer verilmiştir. İkinci bölümde, TCK 243. maddesinde düzenlenen Bilişim Sistemine Girme Suçunun; üçüncü bölümdeyse TCK 244. maddesinde düzenlenen Sistemin Engellenmesi, Bozulması, Verilerin Değiştirilmesi veya Yok Edilmesi Suçlarının analitik incelenmesi gerçekleştirilmiştir.

BİRİNCİ BÖLÜM

BİLİŞİM ALANINDA SUÇLARA İLİŞKİN GENEL AÇIKLAMA VE TEMEL KAVRAMLAR

I. GENEL OLARAK

Yaşadığımız bu çağ bilişim toplumu olarak isimlendirilmiş olup, tarım devrimi ve endüstri devriminin ardından üçüncü büyük dönüm noktası olarak kabul edilmiştir.⁵ Bu çağda yaşanan süratli gelişmeler toplumu her yönüyle bir dönüşüme sokmuş, geliştirilen teknolojiler çok hızlı bir şekilde insanlar tarafından benimsenip, sosyal hayata entegre edilmiştir. Söz konusu bilişim teknolojilerinin kötüye kullanılması sonucu ortaya çıkan haksızlıkların, hukuk tarafından düzenleme altına alınması zorunluluğu doğmuştur.⁶ Ancak bilişim teknolojilerinin teknik yapısından dolayı düzenleme getirmek kolay olmamış, getirilen düzenlemelerse bilişim teknolojileriyle ilgili ortaya çıkan her soruna çözüm üretebilecek nitelikte olmamıştır.

Bilişim sistemleri üzerinden gerçekleştirilen suçlarda ağların sınır tanımayan yapısı, suçun işlendiği yerin tespiti ve hangi ülke hukukunun uygulanacağını belirlenmesi noktasında problem teşkil etmektedir.⁷ Bilişim suçlarının gerek mesafe tanımaması gerek faillerin bulunmasındaki zorluklar gerekse delillerin azlığı ve kısa sürede yok olması, suçun tespit edilmesi ve muhakemesini sıkıntılı bir süreç haline getirmektedir. Özellikle mesafe suçu olarak işlenmiş bilişim suçlarında muhakeme sürecinde iş birliğinin etkili şekilde sağlanamaması, suçların soruşturulmasında yetkin kişilerin, kovuşturmasında uzman hâkimlerin yer almaması bu faaliyetlerin sonuçsuz

⁵ Köksal, Aydın, **Adı Bilgisayar Olsun**, İstanbul, Cumhuriyet Kitapları, 2010, s. 248.

⁶ Kayıtlara geçen ilk bilişim suçu 1966'da Amerika'da yayınlanan bir gazete haberinde "bilgisayar uzmanı banka hesabında tahrifat yapmakla suçlanıyor" başlığıyla kaydedilmiştir. Akbulut, Berrin, **Bilişim Alanında Suçlar**, Ankara, Adalet Yayınevi, 2017, s. 51.

⁷ Özen, Muharrem/ Baştürk, İhsan, **Bilişim-İnternet ve Ceza Hukuku**, Ankara, Adalet Yayınevi, 2011, s. 5.

kalmasına sebep olmaktadır. Ayrıca failler anonim yani gerçek kimliklerini gizleyerek hareket etme imkanına sahip olduğundan ve klasik suçlarda olduğu gibi failin coğrafi kısıtlamaya tabi olmaksızın suçu işleyebilmesi dolayısıyla bu suçların faillerinin yakalanma riskleri geleneksel suçlarla kıyaslandığında daha düşük bir ihtimaldir.⁸ Kısacası bu suçların işlenmesi kolay, tespiti zor olduğundan bilişim suçlarının işlenme oranları çok yüksektir.⁹

Bilişim suçlarına ilişkin siyah rakamların yüksek olması, faillerin bu suçları işlemesinde bir başka sebeptir. Çünkü bu durum faillerde suçun yaptırımsız kalacağına dair güven uyandırmaktadır. Gerçekten de bilişim suçu mağdurlarının, bu suçları resmi mercilere ihbar veya şikâyet etmekten itibaren, güven kaybetmek gibi çeşitli sebeplerle çekinmesi, bilişim suçlarına ilişkin sağlıklı istatistiklerin ortaya konmasını engellenmektedir.¹⁰

Bilişim teknolojileri kullanılarak işlenen haksızlıkların artması, dünya genelinde bu haksızlıklara ilişkin bir kanunlaştırma çalışmasının başlamasını tetiklemiş ve Türk Kanun Koyucusu da bu gelişmelere paralel mevzuatımızda bilişim alanında suçları düzenlemiştir. 06.06.1991’de kabul edilen, 14.06.1991’de yürürlüğe giren 3756 S. Kanunla ETCK’ya “Bilişim Alanında Suçlar” başlığı altında on birinci bab eklenmiştir.¹¹ Ancak 1994 sonrası internet ve kişisel bilgisayar kullanımının hızla artması; ayrıca kredi ve banka kartı kullanımının yaygınlaşmasıyla ortaya çıkan yeni hak ihlallerinin önlenmesi için 5237 sayılı TCK ile bilişim suçlarına daha geniş bir çerçevede yer verilmiştir.¹²

⁸ Erdoğan, Yavuz, **Türk Ceza Kanunu’nda Bilişim Suçları**, İstanbul, Legal Yayıncılık, 2013, s. 87.

⁹ Karagülmez, Ali, **Bilişim Suçları ve Soruşturma- Kovuşturma Evreleri**, Ankara, Seçkin Yayıncılık, 2011, s. 66.

¹⁰ Karagülmez, s. 61; Tiedemann, Klaus (Çev. Feridun YENİSEY), “Bilgisayarlarla İşlenen Suçların Ceza Hukuku Yönünden İncelenmesi”, **İÜHF**, C. 41, S. 1-2, İstanbul, 1975, s. 321.

¹¹ 525/a, 525/b, 525/c ve 525/d maddelerinde bilişim suçları düzenlenmiştir.

¹² Dülger, Murat Volkan, **Bilişim Suçları ve İnternet İletişim Hukuku**, Ankara, Seçkin Yayıncılık, 2021, s. 52.

Suç incelemesine geçmeden önce bu suçlarla ilgili bazı kavramların açıklanması, suçların anlaşılmasını da kolaylaştıracığından öncelikle bu bölümde kavram ve tanımlar üzerinde durulacaktır.

II. KAVRAMLAR

A. BİLİŞİM

Bir disiplin olarak bilişim alanına ismini veren Philippe Dreyfus, Fransızca “information” (bilgi) ve “automatique” (otomatik) kelimelerini birleştirerek “informatique” kavramını elde etmiş¹³; bu kelimeyi Aydın Köksal bilişim olarak Türkçeleştirmiştir.¹⁴ Bilişim kavramına ilk kez 1989 tarihli TCK ön tasarısında yer verilmiştir.¹⁵

Günümüzde bilişim, bilginin işlenmesiyle ilgili olarak belgeleme tekniğinin yerini almış bir disiplindir.¹⁶ Doktrinde bilişim alanına¹⁷ ilişkin çok sayıda benzer tanımlamalar yapılmıştır.¹⁸ Ancak birçok farklı tanım yapılsa da bilişim alanını ifade etmek için yazarlar ortak üç özellik üzerinde durmaktadır. Bunlar verinin saklanması/depo edilmesi, işlenmesi ve aktarılmasıdır. Buradan yola çıkarak en genel tabiriyle bilginin otomatik işlenmesi disiplini olarak nitelendirilebilecek bilişim¹⁹ verinin saklanması, elektronik

¹³ Ketizmen, Muammer, **Türk Ceza Hukukunda Bilişim Suçları**, Ankara, Seçkin Yayınevi, 2008, s. 10.

¹⁴ Bilişim kelimesi “bilmek” fiilinin işteş çatıda çekiminden elde edilmiştir. Köksal, s. 44.

¹⁵ 765 S TCK’da her ne kadar bilişim kavramına 525/a-d madde metinlerinde yer verilmemiş olsa da 3756 S kanunla yapılan değişiklik neticesinde “Bilişim Alanında Suçlar” başlığıyla düzenleme yoluna gidilmiştir. Taşkın, s. 6; Yenidünya/ Değirmenci, s. 28.

¹⁶ Akbulut, s. 13.

¹⁷ Doktrinde bilişimi bağımsız bir bilim dalı olarak görmeyen, matematik, mantık, fizik vb alanların alt dalı olarak nitelendiren görüş için bkz. Kurt, Levent, **Açıklamalı-İçtihatlı Tüm Yönleriyle Bilişim Suçları ve Türk Ceza Kanunu’ndaki Uygulaması**, Ankara, Seçkin Yayıncılık, 2005, s. 24.

¹⁸ “Bilişim; teknik, ekonomik, sosyal, hukuk ve benzeri alanlardaki verinin saklanması, saklanan bu verinin otomatik olarak işlenmesi, organize edilmesi, değerlendirilmesi ve aktarılması ile ilgili bir bilim dalıdır. Yenidünya/ Değirmenci, s. 27; Yazıcıoğlu’na göre bilişim “bilgisayarlardan da faydalanmak suretiyle bilginin saklanması, iletilmesi ve işlenerek kullanılır hale gelmesini konu alan akademik ve mesleki disipline verilen addır. Yazıcıoğlu, Yılmaz, **Bilgisayar Suçları**, İstanbul, Alfa Yayınları, 1997, s. 131; “Bilişim insanların teknik, ekonomik, siyasal ve toplumsal alanlardaki iletişimde kullandığı bilginin, özellikle bilgisayar aracılığıyla düzenli ve akılcı biçimde işlenmesi, her türden düşünsel sürecin yapay olarak yeniden üretilmesi, bilginin bilgisayarlarda depolanması ve kullanıcıların erişimine açık bulundurulması bilimidir.” Dülger, s. 68.

¹⁹ Ketizmen, s. 10.

olarak işlenmesi ve aktarılmasıyla ilgilenen disiplindir. Başka bir deyişle bilişim disiplininin inceleme alanını veri işlem ve veri iletişim süreçleri oluşturmaktadır.²⁰

Bilişim ve bilişim sistemi terimlerine ilişkin net bir tanımın yapılmaması, sürekli ve hızlı bir gelişme ve değişme içerisinde olan mevcut teknolojik düzende gerek yapılan kanuni düzenlemelerin teknolojik gelişmelerin arkasında kalmaması gerek yapılan kalıp tanımların içerisine girmeyen sistemler bakımından haksızlık teşkil eden fiillerin kanunilik ilkesi ve kıyas yasağı bakımından kanunun uygulama alanı dışında kalmasını engellemek için daha isabetli bir tercih olacaktır.²¹

B. BİLİŞİM SİSTEMİ

765 sayılı ETCK'da "*bilgileri otomatik olarak işleme tabi tutan sistem*" ifadesi kullanılmış ancak bu ifadede ne anlaşılması gerektiği tartışmalara yol açmıştır.^{22 23} 5237 sayılı TCK'da ise bu ifade yerine bilgisayar sözcüğünü de içine alan, çok daha kapsayıcı bir kavram olan bilişim sistemi sözcüğüne yer verilmiştir.²⁴ Bu ifade hem mevcut sistemleri kapsamı açısından hem de teknolojik gelişmelere paralel olarak yeni bulunan sistemleri kapsamı açısından yerinde bir tercihtir.²⁵

²⁰ Değirmenci, Olgun, **Ceza Muhakemesinde Sayısal (Dijital) Delil**, Ankara, Seçkin Yayıncılık, 2014, s. 53.

²¹ Erdoğan, s. 8.

²² 3756 S Kanun değişikliğinin gerekçesinde "*bilgileri otomatik olarak işleme tabi tutan sistem*" ifadesinin yanına parantez içerisinde bilgisayar yazılmıştır. Yenidünya/ Değirmenci, s. 44; Taşkın, Şaban Cankat: **Bilişim Suçları**, İstanbul, Beta Yayınevi, 2008, s. 6.

²³ Doktrinde genel görüş bu ifadede bilgisayarın anlaşılması gerektiği yönündeydi. Yenidünya/ Değirmenci, s. 44; Yazıcıoğlu, s. 225; Kurt, s. 27.

²⁴ Bilişim kavramının bilgisayara göre daha kapsayıcı ve üst bir terim olarak nitelendirilmesini yazar eleştirmektedir. Yazar bilgisayar ve bilişim kavramının karşılaştırılmasını bilişim bir bilim alanı; bilgisayarınsa bir araç olması dolayısıyla yanlış bulmaktadır. Burada yazar karşılaştırmanın doğru olacağı iki kavramın bilgisayar ve bilişim sistemi olacağını belirtmiştir. Ayrıca yazar bilişim sistemi kavramının bilgisayardan çok daha geniş kapsamlı olduğunu; bilişim suçlarının işlenmesinde araç olarak kullanılan bilgisayar sayılmayan diğer araçları da kapsamı bakımından daha doğru bir tercih olduğunu belirtmiştir. Dülger, s. 66-67.

²⁵ Nitekim öğretide de bilişim sistemlerinin bilinçli bir seçim olduğu ve genişletici yorumla içinin doldurulması gerektiği ifade edilmektedir. Taşkın, s. 12; Dülger, s. 69.

Verileri toplamak, depolamak, organize etmek ve aktarmak bilişim sistemlerinin asli unsurlarıdır.²⁶ “*Bilginin saklanması, işlenmesi ve iletilmesini konu edinmiş*” bir disiplin olan bilişim hem veri işlem hem de veri iletişim sürecini içerdiğinden bilişim sistemleri de bu iki niteliği haiz olan sistemlerdir.²⁷ 5237 S TCK’nın 243. maddesinin gerekçesinde bilişim sistemleri “*verileri toplayıp yerleştirdikten sonra bunları otomatik işlemlere tabi tutma olanağı veren manyetik sistemler*” olarak tanımlanmıştır. Kanun gerekçesinde sadece veri işlem esas alınarak yapılan bilişim sistemi tanımı, veri iletişime yer verilmemesi sebebiyle eksik bir tanımdır.²⁸ Bilişim sistemlerinin insan müdahalesi olmadan başka bir ifadeyle otomatik olarak veri işleyebilmesi temel özelliği; gerekçede ifade edildiğinin aksine manyetik olması zorunlu bir özellik değildir.²⁹ Bütün bilişim sistemleri manyetik nitelikte olmadığından, bu sistemlerin kapsam dışında bırakılması haklı olarak eleştirilmektedir.³⁰ Gerekçe bağlayıcı olmadığından bilişim sistemlerinin belirlenmesi konusunda bu tanıma itibar edilmemesi gerekir.³¹

Türk ceza hukuku mevzuatında bilişim sistemi, ilk kez 20.09.2011 tarihli Ceza Muhakemesinde Ses ve Görüntü Bilişim Sisteminin Kullanılması Hakkında Yönetmelik’te “Tanımlar ve Kısaltmalar” başlıklı 3-1/b maddesinde “*Bilgisayar, çevre birimleri, iletişim altyapısı ve programlardan oluşan veri işleme, saklama ve iletmeye yönelik sistemi ifade eder.*” şeklinde tanımlanmıştır. Ancak yapılan tanım, bilişim sistemlerinin bilgisayar esas alınarak tanımlanması dolayısıyla eleştirilmiş ve veri işleyebilen, depolayabilen, aktarabilen sistemlerin bilgisayar olup olmadığına

²⁶ Bourgeois, Davis T./ Smith James L. / Wang, Shouhong / Mortatı, Joseph, **Information Systems for Business and Beyond**, s. 8.

²⁷ Ergül, İsmail, **Siber Suçların Cezalandırılması ve Türkiye’de Durum**, Ankara, Adalet Yayınevi, 2008 s. 10; Erdağ, Ali İhsan, Bilişim Alanında Suçlar (Türk ve Alman Ceza Hukukunda), **GÜHFD**, C. 14, S. 2, İstanbul 2010 s. 277.

²⁸ ERDAĞ, s. 277-278.

²⁹ KETİZMEN, s. 19.

³⁰ DEĞİRMENCİ: Delil, s. 53.

³¹ ERDOĞAN, s. 11.

bakılmaksızın bilişim sistemi kabul edilmesi gerektiği ifade edilmiştir.³² Bu doğrultuda veri işlem ve veri iletişim yapabilen ancak bilgisayar sayılmayan örneğin bilişim ağ sistemleri de bilişim sistemi sayılabileceğinden bu görüşün daha yerinde olduğunu düşünüyoruz.

Bilişim sistemlerini açık bilgisayar sistemleri, iletişim sistemleri ve gömülü bilişim sistemleri olarak üç alt kategoriye ayırmak mümkündür.³³ Açık bilgisayar sistemleri gündelik yaşamımızda kullandığımız bilgisayarlar; iletişim sistemleri bilişim sistemleri arasında haberleşmeye olanak sağlayan (örneğin: internet) sistemler; gömülü bilişim sistemleri ise çeşitli fonksiyonlar için faydalanılmakla birlikte esasen bir bilişim sisteminin parçası olarak işlev gören (örneğin navigasyon cihazları, POS cihazı, akıllı ev aletleri) cihazlardır.³⁴

Bilişim sistemleri ifadesinin üst başlık olması ve bilgisayarı da kapsamı³⁵ dolayısıyla bilgisayar bir bilişim sistemidir ancak her bilişim sistemi bilgisayar değildir.³⁶ Bilgisayarların geniş bir kitle tarafından kullanılması dolayısıyla bilişim suçları yaygın olarak bilgisayarlar aracılığıyla veya doğrudan bunlara ya da bunlar içindeki verilere karşı işlenmektedir. En yaygın kullanılan bilişim sistemi olan bilgisayara³⁷ bu çalışmada ayrı bir başlık altında değinilmeyecek olup, bilgisayarın diğer bilişim sistemlerinden ayrılan

³² Erdoğan, S. 16.

³³ Açıkgöz, Emre İkbāl, **Bilişim Sistemi Aracılığıyla Haksız Yarar Sağlama Suçu**, s. 24; Casey, Eoghan: **Digital Evidence and Computer Crime: Forensic Science, and the Internet**, s. 7; Tanrıku, Cengiz: **Ceza Muhakemesi Hukukunda Bilişim Sistemlerinde Arama ve Elkoyma**, Ankara, Adalet Yayınevi, 2014 s. 14.

³⁴ Casey, s. 8; Tanrıku, s. 14; Açıkgöz, s. 24-25.

³⁵ Karagölmez, s. 35.

³⁶ Taşkın, s. 4.

³⁷ TDK'nın sözlüğünde bilgisayar “Çok sayıda aritmetiksel veya mantıksal işlemlerden oluşan bir işi, önceden verilmiş bir programa göre yapıp sonuçlandıran elektronik araç, elektronik beyin.” şeklinde tanımlanmıştır.

“Bilgisayar veri saklayabilen depolayabilen ve bunları işleyebilen, depolanmış bir programı işletebilen ve işlem akışı ile sırasını otomatik olarak değiştirebilen bir aygıttır.” Yazıcıoğlu, s. 27-28.

“Bilgisayar insanlar tarafından hazırlanıp yüklenen programlar yardımıyla bilgileri belirli bir düzende saklamak, işleyerek yeni sonuçlar üretmek, üretilen verileri başka yerlere iletmek, başka yerlerdeki verilere ulaşmak gibi amaçlarla kullanılan makinelerdir.” Akbulut, s. 10-11.

özelliklerini belirtmekle yetineceğiz. Her ne kadar birçok çalışmada bilgisayara ve unsurlarına detaylı bir şekilde değinilmiş olsa da çalışma konusu olan bilişim sistemleri bilgisayarı da içine alan daha kapsamlı bir terim olduğundan ayrıca bilgisayarın ve unsurlarının açıklanmasının gereksiz olduğu kanaatindeyiz. Kaldı ki doktrinde bilgisayarın tüm işlevlerini ve özelliklerini içeren bir tanımın yapılmasının zorluğu yanında böyle bir tanımın ancak mevcut bilgisayarların özelliklerini içermesi gelecekte geliştirilen bilgisayarları tanımlamak için yetersiz kalacağı belirtilmiştir.³⁸

Bilgisayarları diğer bilişim sistemlerinden ayıran özellik, bilgisayarın genel amaçlı kullanılabilir olmasıdır.³⁹ Diğer otomatik, elektronik, manyetik cihazların tek yönde veya belirli şekillerde işlem yapmasına karşın bilgisayardan genel amaçlı faydalanılabilmektedir.⁴⁰ Bilgisayarlar verileri depolama, işleme, yeniden değerlendirme fonksiyonlarını başka bir ifadeyle veri işlemi gerçekleştirebilirken; bilişim sistemleri hem veri işlemi hem de verilerin aktarılmasını yani veri-iletişimi gerçekleştirebilmektedir. Yani bilişim sistemleri veri işlem ve veri iletişim özelliklerine birlikte sahiptir.⁴¹

Doktrinde bir görüşe göre bilişim sistemi ifadesiyle asıl kastedilen genel amaçlı/ çok yönlü kullanılabilen bilgisayarlardır.⁴² Tek yönlü çalışan başka bir deyişle belirli bir kullanım amacına özgülenen bilgisayar destekli cihazlar bilişim sistemi değildir.⁴³ Bilişim sistemlerini diğer otomatik, manyetik cihazlardan ayıran en temel özellik de genel amaçlı kullanımdır.⁴⁴ Yani bilgisayar temelli çalışan verileri otomatik işleyebilen ve

³⁸ Yenidünya/ Değirmenci, s. 17.

³⁹ Temelde bilgisayar “*bilgi işleyen, programlama yeteneğine sahip elektronik*” bir araçtır. Ancak bu özellikler bilgisayarı diğer sistemlerden ayıran özellikleriyle ortaya koymamıza yetmemektedir. Bilgisayarı diğer sistemlerden ayıran genel amaçlı çalışabiliyor olması yani bilgisayarın “*yeterince kavramsallaştırılmış ve iyi tanımlanabilmiş her türlü problem üzerine çalışabilen bir aygıt*” olmasıdır. Yazıcıoğlu, s. 26-27.

⁴⁰ Yazıcıoğlu, s. 216-217.

⁴¹ Koca, Mahmut/ Üzülmöz, İlhan, **Türk Ceza Hukuku Özel Hükümler**, Ankara, Seçkin Yayıncılık, s. 898; Değirmenci, s. 199.

⁴² Yazıcıoğlu, s. 404

⁴³ Yazıcıoğlu, s. 405.

⁴⁴ Kurt, s. 141.

belirli bir amaca özgülenmeksizin genel amaçlı çalışan sistemler bilişim sistemleridir.⁴⁵ Ancak bu tanımlamayı doğru bulmayan yazarlar, bilişim sistemlerinin zorunlu olarak genel amaçlı kullanılma özelliğine sahip olmasına gerek olmadığını; veriyi işleyebilen, depolayabilen ve veri iletişimi yapılan her türlü sistemin genel amaçlı kullanılıp kullanılmadığına bakılmaksızın bilişim sistemi sayılması gerektiğini savunmaktadır.⁴⁶ Biz de bu görüşe iştirak etmekteyiz zira örneğin POS cihazları, navigasyon cihazları belli bir kullanım amacına özgülenmiş araçlar olsa da veri işlem ve veri iletişimi yapabildiklerinden bu araçlar da bilişim sistemidir.

Burada üzerinde durulması gereken bir konu da bilgisayar ve bilişim kavramlarının her ne kadar birbirleri yerine kullanılıyor olsalar da farklı şeyleri ifade ettiğidir. Bilgisayar bir araç iken bilişim “*bilginin saklanması, iletilmesi ve işlenerek kullanılır hale gelmesini konu alan*” alandır.⁴⁷

Yukarıda açıklandığı üzere teknolojik gelişmelerin hızının tersine, kanunların yapılmasının zaman alan bir faaliyet olması dolayısıyla gerek kanun koyucular gerek de yazarlar bilişim sistemi tanımını vermekten kaçınmaktadır. Burada somut olayın özelliğine göre değerlendirme yapılarak mevcut gelişmelere paralel ancak biçimsel kanunilik ilkesini ihlal etmeden, bilişim sistemi kavramının yorumlanması gerekir.⁴⁸ Biçimsel kanunilik ilkesinin gereği olarak tipikliği oluşturan suçun unsurlarının açıkça tanımlanması gerekir. Buna karşın hızlı gelişim gösteren bir alan olan bilişim alanında ortaya çıkan buluşların yapılacak tanımlamaların dışında kalması ihtimali vardır. Dolayısıyla burada sınırın hassas bir şekilde çizilmesi gereklidir.⁴⁹ Her türlü haksızlık teşkil eden fiilleri kapsamı ve gelişen teknolojiye yenik düşmemesi için kanunlarda

⁴⁵ Ersoy, s. 151; Taşkın, Şaban Cankat, Bilişim Hukuku Uluslararası Uyuşmazlıklar, s. 333-334. Yazıcıoğlu, s. 403.

⁴⁶ Genel amaçlı çalışan sistemlerden ne anlaşılması gerektiği oldukça muğlak olduğundan yazar bu görüşü eleştirmektedir. Erdoğan, s. 12-13

⁴⁷ Yazıcıoğlu, s. 130-131

⁴⁸ Erdoğan, s. 18.

⁴⁹ Yazıcıoğlu, s. 134-135.

daha kapsayıcı ve geniş tanımlara yer verilse de tipik fiillerin açık ve belirli olması elzemdir.⁵⁰

Bir sistemin bilişim sistemi olup olmadığının tespiti teknik bir konu olup, ceza hukuku bilgisiyle çözülebilecek bir sorun değildir. Dolayısıyla muhakeme sürecinde bilirkişilere başvurulması maddi gerçeğin ortaya çıkarılması bakımından sağlıklı sonuçlar verecektir.

C. BİLİŞİM SİSTEM AĞLARI

Bilişim sistemlerinin bazı protokoller çerçevesinde birbirine bağlanarak insanlar arası iletişimi mümkün hale getirmesi fikri, zaman ve mekân sınırı olmaksızın bilişim sistemleri arasında veri alışverişini mümkün kılan bilişim ağlarının ortaya çıkmasını sağlamıştır.⁵¹ Bilişim sistem ağları ifadesi bilgisayar ağları⁵² ifadesine göre daha isabetlidir. Çünkü bilgisayar dışındaki bilişim sistemleriyle de ağa bağlanılabilmektedir.⁵³

Dünyadaki bilişim sistemleri ve bilişim sistemleri ağlarının TCP/IP denilen protokol çevresinde birbirine bağlanmasıyla oluşturulmuş en büyük iletişim ağı İnternettir.⁵⁴ Ağların ağı olarak da nitelendirilen internetin temel işlevi gerek bilişim sistemleri gerek bilişim sistem ağlarını bağlayarak küresel düzeyde her türlü bilginin paylaşılmasını ve iletişimin gerçekleştirilmesini kısacası veri iletişimini mümkün kılmaktadır.⁵⁵ ABD Savunma Bakanlığının bir savaş halinde askeri ve idari kurumların iletişiminin kesintiye uğrama tehlikesini bertaraf etmek amacıyla⁵⁶ bir iletişim sistemi

⁵⁰ Yazıcıoğlu, s. 141.

⁵¹ Ketizmen, s. 19-20; Yendünya/ Değirmenci, s. 34.

⁵² Özen/ Baştürk bilgisayar ağı ifadesini kullanmaktadır.

⁵³ Erdoğan, s. 25; Yenidünya/ Değirmenci, s. 33.

⁵⁴ Akbulut, s. 18.

⁵⁵ Ketizmen, s. 21; Taşkın, s. 13; Kurt, s. 41; Özen/ Baştürk, s. 13.

⁵⁶ Burada amaç -geleneksel ağ sisteminde ana bilgisayarın devre dışı bırakılması durumunda ağın işlevsiz kaldığı için- herhangi bir saldırıda bir bilgisayarın devre dışı kalması halinde dahi diğer bilgisayarların çalışmaya devam etmesini sağlamaktır. Akbulut, s. 19.

kurma fikri, internetin icadında temel taşı oluşturmaktadır.⁵⁷ ABD Savunma Bakanlığındaki çalışmalar sonucu kurulan ARPANET adındaki internetin atası sayılabilecek ağ, askeri amaçların ötesinde kullanılmaya başlanmış ancak daha sonra geniş kitlelere açılmasıyla yerini internete bırakmıştır.⁵⁸

Bilgisayar ve bilgisayar ağlarını TCP/IP adındaki protokolle birbirine bağlayan bir ağ olan⁵⁹ internet, yaratmış olduğu sınırsız özgürlük alanı ve anonim kalma özellikleriyle suç işlemek isteyenler için bulunmaz bir mecra niteliği taşımaktadır.⁶⁰ Bu durumsa iletişim ve bilgi paylaşımı amaçlarıyla kurulan ancak bu amacı aşarak hayatın her alanında kullanılan internetin hukuk tarafından düzenlenmesi zorunluluğunu ortaya çıkarmıştır. Zira internet bazı suçların işlenmesini daha da kolay hale getirirken yeni bazı suç tiplerinin de ortaya çıkmasına neden olmuştur.⁶¹ Ancak bu mecraya ilişkin mevzuat çalışmalarında, her şeyden önce getirilen düzenlemeler ifade özgürlüğü, iletişim özgürlüğü gibi temel hak ve özgürlükleri güvence altına almak amacına hizmet etmelidir.⁶² İnternet üzerinden gerçekleştirilen fiillerin düzenlenmesiyle ilgili olarak AİHS 10. maddesi ve Anayasa 22 ve 26. maddesindeki sınırlamalara riayet edilmesi zorunludur.⁶³

D. VERİ

TCK madde 243'ün gerekçesinde veri, “*sistem içindeki bütün soyut unsurlar, fıkra*da geçen veri tanımının kapsamındadır.” şeklinde tanımlanmıştır. 5651 S. İnternet

⁵⁷ Nükleer saldırı durumunda dahi çalışabilmesi için tasarlanmış bu ağın merkezi bir yapısının olmaması tercih edilmesindeki temel sebeptir. Zira ABD Savunma Bakanlığı mevcut iletişim ağlarının merkezi yapısı dolayısıyla yani ana bilgisayara saldırı durumunda tüm sistemin işlevsiz hale gelmesini engellemek için ARPANET'i kurmuştur. Bkz. Ketizmen, s. 20; Yenidünya/ Değirmenci, s. 37.

⁵⁸ Yenidünya/ Değirmenci, s. 38-39; Özen/ Baştürk, s. 7-8.

⁵⁹ TCP/IP protokolü internet aracılığıyla yapılan veri iletişimde uyulması gerekli kuralları belirleyen protokoldür. Karagülmez, s. 40.

⁶⁰ MAHMUTOĞLU, Fatih Selami, “Karşılaştırmalı Hukuk Bakımından İnternet Süjelerinin Ceza Sorumluluğu”, *İÜHF*M, C. 59, S. 1-2, s. 39.

⁶¹ ÖZEN/ BAŞTÜRK, s. 87-88. Özbek, Veli Özer, “İnternet Kullanımında Ortaya Çıkabilecek Bazı Ceza Hukuk Sorunları”, *DEÜHFD*, C. 4, S. 1, İzmir 2002 s. 105.

⁶² Özen/ Baştürk, s. 89.

⁶³ Ketizmen, s. 23-24.

Ortamında Yapılan Yayınların Düzenlenmesi Ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun'un 2-(1) k maddesinde ve 5651 S. Kanuna dayanarak çıkarılan İnternet Ortamında Yapılan Yayınların Düzenlenmesine Dair Usul Ve Esaslar Hakkında Yönetmelik 3-(1) p maddesinde ayrıca 11.04.2017 tarihli İnternet Toplu Kullanım Sağlayıcıları Hakkında Yönetmelik 3-(1) m maddesinde veri “*bilgisayar tarafından üzerinde işlem yapılabilen her türlü değer*” olarak ifade edilmiştir.

Veriler, bilişim sistemlerinin üzerinde çalışabilmesi için bilgilerin belirli bir formata dönüştürülmüş şeklidir.⁶⁴ Bilişim sistemlerinin sakladığı, işlediği ve kendilerinden sonuç çıkardığı her şey veridir ve bu veriler sistemin temel unsurlarıdır.⁶⁵ Veriler aynı zamanda bilişim sistemlerinin kendisinden beklenen doğrultuda çalışmasını sağlayan programları da oluşturur.⁶⁶ Bilişim sisteminin veri işleyebilmesi, işlediği verilerden sonuç çıkarabilmesi yani işlev gösterebilmesi için gereken komut dizinlerine program denir.⁶⁷ Yani veriler hem bilişim sisteminin işlevini yerine getirmesine yarayan programların temel birimi hem de veri işlemek ve aktarmak için kullanılan bilişim sistemlerinin varoluş sebebidir.⁶⁸

ETCK'da “*verileri, programları veya diğer herhangi bir unsuru*” ifadesi kullanılmış ancak bu ifade yerinde değildir zira bahsedilen her bir unsuru veri ifadesi karşılamaktadır. Dolayısıyla bu ifade kendisinin tekrarından ibarettir. Veri kavramı bilişim sistemlerinde yer alan programları da kapsadığından 5237 S TCK'da sadece veri ifadesine yer verilmesi yerinde bir tercih olmuştur.⁶⁹

⁶⁴ Yazıcıoğlu, s. 229; Yenidünya/ Değirmenci, s. 47-48.

⁶⁵ Yenidünya/ Değirmenci, s. 47.

⁶⁶ Yazıcıoğlu, s. 225.

⁶⁷ Yenidünya/ Değirmenci, s. 47.

⁶⁸ Yazıcıoğlu, s. 227.

⁶⁹ Ayrıca Avrupa Siber Suç Sözleşmesinde de bilgisayar verisi “bilgisayar sisteminin bir işlevi yerine getirmesini mümkün kılan bir programı da kapsayan, olguların, bilginin veya kavramların bir bilgisayar sisteminde işlenmeye uygun haldeki her türlü temsilini ifade eder” şeklinde tanımlanmıştır ve bu tanım da bu görüşü destekler niteliktedir. Değirmenci, s. 199/200.

E. BİLİŞİM SUÇLARI

a. TERİM SORUNU

Bilişim teknolojilerinin gelişimiyle ortaya çıkan bilişim alanındaki suçlar için en başta kanunlarda değişiklik yapma yoluna gidilmemiş; bu suçlar klasik suçlar altında değerlendirilmeye çalışılmış ancak geleneksel suç tiplerine uymayan yeni suç tiplerinin ortaya çıkmasıyla yeni düzenlemelerin yapılması zorunluluk haline gelmiştir.⁷⁰ Bilişim alanındaki suçlar ilk işlenmeye başladığında bu suçların nasıl adlandırılacağı ve nasıl tanımlanacağı konusunda sorunlar ortaya çıkmıştır. Hala bu suçların isimlendirilmesi ve tanımlanması konusunda bir görüş birliği olduğu söylenemez. Gerek Türk hukuku doktrininde gerek diğer ülke hukuku doktrinlerinde bu suçları ifade etmek için üzerinde uzlaşılmış bir terim ve tanımın bulunduğunu söylemek mümkün değildir.⁷¹

Bilişim suçlarının 1960'lı yıllarda Amerika'da ortaya çıkması ve bu suçlara ilişkin ilk tartışmalar ve yasal düzenlemelerin Amerika'da bilgisayar suçları⁷² adı altında yapılması diğer ülke hukukçularını da etkilemiştir.⁷³ Bilgisayar suçları ifadesi, bilişim alanındaki suçların tam olarak karşılığı değildir. Bilişim alanındaki suçlar denildiğinde sadece bilgisayarlara karşı veya onlar marifetiyle işlenen suçlar anlaşılmamaktadır. Zira bilişim sistemi kavramı bilgisayar kavramına göre üst bir kavram olup, onu da kapsamına

⁷⁰ Karagülmez, s. 42.

⁷¹ Almanya'da bu suçları karşılamak için Computer Kriminalität (bilgisayar suçluluğu) terimi kullanılmakta ancak bu ifade bir makinenin suç işleyemeyeceğinden bahisle eleştirilmektedir. İtalya'da bu suçları karşılamak için I reati elettronici (elektronik suçlar), I reati commessi con l'uso del computer (bilgisayar kullanımı vasıtasıyla işlenen suçlar) gibi ifadeler kullanılmış ancak doktrinde daha sonra I reati informatici (bilişim suçları) ve la criminalita informatica (bilişim suçluluğu) kavramları kabul görmüştür. İtalyan kanun koyucusu doktrinindeki gelişmelere paralel bilişim suçluluğu tabirini kanunda kullanmayı tercih etmiştir. Fransa'da bu suçlar için la fraude informatique (bilişim ihlali) ifadesi kanun koyucu tarafından tercih edilmiştir. Yazıcıoğlu, s. 126-129.

⁷² Amerika'da bilişim suçları için computer crime (bilgisayar suçu), computer-assisted crime (bilgisayar yardımcı suçu) computer related crime (bilgisayar bağlantılı suçu) ya da crime against computer (bilgisayara karşı suçu) ifadeleri kullanılmaktadır. Ayrıca high-tech crime (ileri teknoloji suçu) veya techno-crime (teknoloji suçu) gibi ifadeler de yer verilmektedir. Yenidünya/ Değirmenci, s. 30; Karagülmez, s. 91; Ö. Umut Eker, s. 104.

⁷³ Dülger, s. 70; Erdoğan, s. 44.

almaktadır.⁷⁴ Bilgisayar veri işlemi yani verilerin saklanması, işlenmesi ve yeniden değerlendirilmesini yapabilmekteyken; bilişim sistemleri hem veri işlem hem de veri iletişimi yani verilerin aktarılmasını yapabilmektedir.⁷⁵ Kısacası bilgisayar sayılmayan ancak bilişim sistemi sayılan bir sistem (örneğin bilişim sistemi ağları) vasıtasıyla veya bu sisteme karşı da bu suçlar işlenebileceğinden, bilgisayar suçları ifadesi bu suçları karşılamak için yetersiz kalmaktadır.⁷⁶ Bilgisayar suçluluğu ifadesi de bilgisayarlar suç işleyemeyeceğinden yanlış bir tercihtir.⁷⁷

Doktrindeki bazı yazarlar bilişim alanındaki suçlara, internet suçları ismini vermektedir.⁷⁸ Fakat internet her ne kadar bilişim suçlarının işlenmesi bakımından ortam yaratsa da internet suçları kavramı tüm bilişim suçlarını kapsama konusunda yetersiz kalmaktadır.⁷⁹ Kaldı ki bilişim suçları kavramı diğer bilişim sistem ağları aracılığıyla işlenen suçları (örneğin intranet, ekstranet gibi bilişim ağ sistemleri) ve ileride geliştirilebilecek farklı ağ sistemleri aracılığıyla işlenecek suçları da kapsamaktadır.⁸⁰

Siber suç kavramı da bilişim alanında işlenen suçları ifade etmek için kullanılan terimlerden biridir.⁸¹ Fakat siber suç kavramı sadece bilişim sistemi ağları vasıtasıyla (özellikle internet) işlenen eylemleri ifade etmek için kullanıldığından, tüm bilişim

⁷⁴ Yenidünya/ Değirmenci, s. 31; Yılmaz, Sacit, “5237 Sayılı TCK’nın 244. Maddesinde Düzenlenen Bilişim Alanındaki Suçlar”, **TBBD**, S. 92, Ankara, 2011 s. 63; Erdağ, s. 279.

⁷⁵ Yenidünya/ Değirmenci, s. 31; Erdoğan, s. 44-45.

⁷⁶ Yazıcıoğlu, s. 131; Ersoy, s. 151.

⁷⁷ Tiedemann (Yenisey Çeviri), s. 321.

⁷⁸ Doktrinde bir görüşe göre internet suçları ile bilgisayar suçları birbirinden tamamen farklı kavramlardır. Her ne kadar internet suçları bilgisayarlar aracılığıyla işlense de bu suçlar internet ortamında işlenen suçlardır. İnternet ortamında işlenmiş olma niteliği bu suçlara ayırıcı özelliğin veren unsurdur. Dolayısıyla internet ortamında işlenmiş tüm bilgisayar suçları aslında internet suçudur. Yazara göre internet suçları ikiye ayrılır. İlk grubu internet aracılığıyla işlenen ceza kanunlarında yer alan klasik suç tipleri oluşturur. İkinci grubu ise internetin ortaya çıkmasıyla işlenmeye başlamış, daha önce var olmayan, ceza kanunlarında düzenlenmemiş internete özgü suçlar oluşturur (internetteki bir web sitesini kırmak, tahrif etmek). Özbek, Veli Özer, İnternet Kullanımında Ortaya Çıkabilecek Bazı Ceza Hukuku Sorunları, s. 106-109

⁷⁹ Erdoğan, s. 48.

⁸⁰ Erdoğan, s. 48.

⁸¹ Gerek Avrupa Konseyinin gerek diğer uluslararası örgütlerin çalışmalarında bu kavramı tercih etmeleri dolayısıyla yazar siber suç ifadesini kullanmaktadır. Ergün, s. 14.

suçlarını kapsamamaktadır.⁸² Dolayısıyla bilişim suçları terimi siber suçlara göre daha geniş bir kavramdır ve siber suçları da kapsamına alır.⁸³

Doktrinde birçok yazar bilişim alanında yaşanan teknolojik gelişmeleri ve hızını göz önünde tutarak hem mevcut teknolojiyi hem de olası herhangi bir yeniliği kapsamına alabilecek bir terimin tercih edilmesini savunmaktadır. Bu yüzden bilişim sistemi ve bilişim suçları ifadelerinin kullanılması, bilişim suçlarının hem bilgisayar suçlarını ve siber suçları hem de bugünkü teknoloji yanında gelecekte ortaya çıkabilecek yeni teknolojilerle işlenebilecek suçları kapsayan üst bir kavram olması dolayısıyla daha doğru bir tercih olduğu vurgulanmaktadır.⁸⁴ Nihayetinde Türk Kanun Koyucusu da 3756 S. Kanunla bilişim alanında suçlar tabirini kullanmayı tercih etmiştir. Biz de bu tercihin daha isabetli olduğu görüşündeyiz.

b. TANIM SORUNU

Terim olarak bilişim suçu kabul edildikten sonra bu suçun nasıl tanımlanacağı sorunu ortaya çıkmaktadır. Ulusal mevzuatlara bakıldığında bu kavramın tanımına kanun metinlerinde yer verilmediği görülmektedir. Milletlerarası yapılan çalışmalarda da tanım vermek yerine, bilişim suçu teşkil eden hareketlerin tek tek sayılması yoluna gidilmektedir.⁸⁵ Doktrinimizde bilişim suçlarına ilişkin çok çeşitli tanımlar verilmiş ancak üzerinde uzlaşılan bir tanım ortaya konamamıştır. Ortak bir tanım vermenin zorluğu bu suçların çok çeşitli işlenme şekillerinin olması ve bu suçlarla çok farklı hukuki değerlerin ihlal edilmesinden kaynaklanmaktadır. Bunun yanında çok kısa bir sürede büyük bir değişim geçiren bilişim teknolojilerine ilişkin yapılacak suç tanımı, yeni bir

⁸² Yenidünya/ Değirmenci, s. 33.

⁸³ Erdoğan, s. 45.

⁸⁴ Akbulut, s. 59; Ketizmen, s. 34; Yaşar, Osman/ Gökcan, Hasan Tahsin/ Artuç, Mustafa: **Yorumlu Uygulamalı Türk Ceza Kanunu**, C. 5, Ankara, 2014, s. 7286; Soyaslan, Doğan, **Ceza Hukuku Özel Hükümler**, Ankara, Yetkin Yayınevi, 2014, s. 691; Orta, s. 110; Açıkgöz, s. 34; Erdoğan, s. 47; Erdağ, s. 279; Kurt, s. 139.

⁸⁵ Akbulut, s. 55

gelişmeyle ortaya çıkabilecek bilişim sistemlerinin tanımın kapsamı dışında kalması tehlikesini de içinde barındırmaktadır. Böyle olunca da kanun koyucular bilişim suçlarına ilişkin net bir tanım vermekten kaçınmakta, doktrindeki yazarlarsa yaptıkları tanımlarda genel ve kapsayıcı ifadelerle yer vererek gelecekte ortaya çıkabilecek bilişim sistemlerini suçların kapsam dışında bırakmamaya çalışmaktadır.⁸⁶

Doktrinde bilişim suçlarını tanımlamaya çalışan yazarlar çeşitli kriterleri esas almış ve bu doğrultuda tanım vermeye çalışmışlardır. Ancak bu tanımlama çalışmaları, bilişim suçlarına niteliğini veren özellikleri içermekte ve bu suçların klasik suçlardan ayırımını sağlamakta başarılı olamamıştır.⁸⁷ Bilişim suçları bilişim sistemine karşı veya bilişim sistemlerinin araç olarak kullanıldığı suçlardır.⁸⁸ Ancak klasik suçlardan bazıları da bilişim sistemleri aracılığıyla veya bilişim sistemlerine karşı işlenebildiğinden, bilişim suçlarını belirleyici özellikleriyle ortaya koyan tanım verilememesi kapsam sorununu da beraberinde getirmiştir.⁸⁹

Bilişim suçlarının maddi konu ve kullanılan araç ölçütüyle tanımlanarak kapsamının belirlenmeye çalışılması, hukuki konu gözetilmeksizin çok farklı suçların bir arada değerlendirilmesine neden olacaktır.⁹⁰ Öyle bir tanım yapılmalı ki hem bilişim suçlarını klasik suçlardan ayırsın hem de bütün bilişim suçlarını kapsasın. Bu noktada

⁸⁶ Eker, s. 103.

⁸⁷ Bilgisayar veya bilişimin amaç veya araç olmasını arayan kriter; çok geniş kapsamlı olduğundan örneğin bir bilgisayarın çalınmasının dahi bu tanıma göre bilişim suçu kabul edilmesinden ve klasik suç tiplerden bilişim suçlarını ayıramadığından dolayı eleştirilmektedir. Suçları malvarlığı ihlalleriyle sınırlayan kriter bu suçların malvarlığı değerleri dışında farklı hukuki değerleri de ihlal etmesi ve bu sistemler aracılığıyla gerçekleştirilen her türlü malvarlığına karşı suçun bilişim suçu sayılmış olması dolayısıyla eleştirilmektedir. Bilişim sistemleriyle herhangi bir şekilde bağlantılı olan suçları esas alan kriter; bu kriter de herhangi bir şekilde bilişim sistemlerinin yer aldığı her suçu kapsadığından, klasik suç tiplerinden bilişim suçlarının farkını ortaya koymadığı için eleştirilmiştir. Suçu işleyen faili esas alan kriter bilişim suçları ancak bilişim sistemlerine dair bilgisi olan kişiler tarafından bu sistemlere karşı veya bu sistemler aracılığıyla işlenen suçlar olduğu savunduğundan failin bilişim sistemlerine dair teknik bir bilgisi olmadan sisteme zarar vermesi durumu bu suça vücut vermemiş olacaktır ve durum sağlıklı bir netice doğurmamaktadır. Veri iletişim ağlarını esas alan kriter; suçların bu ağlar aracılığıyla işlenmesini esas almaktadır. Ancak bu suçlar sadece veri iletişim ağları aracılığıyla işlenmemektedir. Akbulut, s 59-67.

⁸⁸ Yenidünya/ Değirmenci, s. 31.

⁸⁹ Ketizmen, s. 32.

⁹⁰ Ketizmen, s. 38.

bilişim suçlarında, bilişim sisteminin kullanılması ya da bilişim sistemi aleyhine bu suçun işlenmesi zorunlu unsurdur. Ancak bu nitelendirme bilişim suçlarını klasik suç tiplerinden ayırmaya yetmemektedir. Zira bir bilgisayarın başkasını yaralamak üzere diğerine atılması durumunda, bilgisayarın araç olarak kullanıldığı bir yaralama suçu vardır. Ancak bu suç her ne kadar bilgisayar araç olarak kullanılsa da bilişim suçu değildir. O halde tanımın sınırlandırılması gerekir ki bilişim sistemi aracılığıyla veya ona karşı işlenen her hareket bilişim suçu sayılsın. Bu noktada bilişim suçlarına özelliğini veren unsurun ortaya çıkarılması gerekir. Bu unsur bilişim sistemlerinin varlık sebebi olan ve ayrıca çalışmasını sağlayan verilerdir. Buradan hareketle bilişim suçları “*verilerle veya veri işleme konu bağlantısı olan ve bilişim sistemleriyle veya bilişim sistemine karşı işlenen suçlar bilişim suçlarıdır. Burada önemli olan fiilin verilerle ilgili olması ve bilişim sistemi kullanılarak gerçekleştirilebilmesinin söz konusu olmasıdır.*”⁹¹

c. BİLİŞİM SUÇLARININ TASNİFİ

Doktrinde bilişim suçlarına dair çok farklı tasnifler yapılmıştır. Bir görüş bilişim suçlarını, bilgisayarın fiziki yapısına zarar verme, bilgisayarın işleyişine ilişkin fiiller, bilgisayar ağları aracılığıyla işlenen suçlar şeklinde sınıflandırmaktadır.⁹² Başka bir görüş bilişim suçlarını dar anlamda bilişim suçları, geniş anlamda bilişim suçları olarak kategorize etmektedir.⁹³ Dar anlamda bilişim suçu “*bilişim sisteminin kendisinin ya da bilişim sistemi içerisinde bulunan verilerin hedef alındığı ve bilişim teknolojilerinin kullanılması suretiyle ya da bilişim araçlarına doğrudan fiziki müdahaleyle işlenen suçlardır.*”; geniş anlamda bilişim suçları ise “*herhangi bir şekilde suçun icrasında bilişim sistem ya da araçlarının kullanıldığı ya da bilişim sistemlerinin veya içindeki verilerin hedef alındığı suçlardır.*”⁹⁴

⁹¹ Akbulut, s. 70.

⁹² Karagülmez, s. 59.

⁹³ Akbulut, s. 57-58.

⁹⁴ Erdoğan, s. 52.

Doktrinde bir yazar bilişim suçlarını; “*sadece bilişim sisteminin kullanılmasıyla işlenebilen suçlar (doğrudan ya da dar anlamda veyahut gerçek bilişim suçları TCK 243, 244, 245), bilişim sisteminin kullanılmasının suçun işlenmesinde zorunlu olmadığı ancak suçun nitelikli halini oluşturduğu suçlar (TCK 142/2-e, 158/1-f) ve kullanılması zorunlu olmamakla birlikte bilişim sisteminin suçun işlenmesinde araç olarak kullanılabildiği suçlar (TCK 132, 124, 113, 112, 125, 226, 228, 214, 105 gibi)*” şeklinde tasnif etmektedir.⁹⁵

Bir başka yazar bilişim suçlarını üç kategori altında değerlendirmektedir. Bunlar; bilişim sisteminin suçun maddi konusu olduğu yani bilişim sistemlerine karşı suçlar (bu suçlarda fiziki zarar söz konusu olduğundan bu suçların ceza kanunundaki mevcut mala zarar verme suçlarıyla karşılanması mümkündür.), bilişim sistemlerinin araç olarak kullanıldığı suçlar ve bilişim sistemlerine karşı bilişim sistemi ortamında gerçekleştirilen suçlar (asıl bilişim suçları)⁹⁶

Yargıtay kararlarında da ise bilişim suçları doğrudan bilişim suçları ve dolayısıyla bilişim suçları olarak ikiye ayrılmaktadır. TCK’da Bilişim Alanında Suçlar (TCK 243, 244, 245, 245/A, 246) bölümünde düzenlenen suçlar doğrudan bilişim suçlarıyken; bilişim sistemlerinin suçun işlenmesinde araç olarak kullanılabildiği suçlar dolayısıyla bilişim suçlarıdır.⁹⁷ Doğrudan bilişim suçlarından kasıt, bilişim sistemlerinin kendine özgü yapısından kaynaklanan ve yeni hukuki menfaatleri koruyan suçlardır. Dolayısıyla bilişim suçlarından kasıtsa geleneksel suçların bilişim sistemleri aracılığıyla işlenmesidir.⁹⁸

⁹⁵ Mahmutoglu, s. 856.

⁹⁶ Ersoy, s. 160-161.

⁹⁷ Bu suçlar: TCK 112, 113, 125, 132, 133, 134, 135, 136, 138, 142/2-e, 158/1-f, 213, 218, 226, 228 Özsoy, Nevzat, “Yargıtay Kararları Işığında Doğrudan Bilişim Suçları (TCK 243 ve 244)”, **Yaşar Hukuk Dergisi** C.1, S. 2, s. 295.

⁹⁸ Yazicioğlu, s. 397.

Bilişim suçlarını doktrinde ekonomik suç ya da beyaz yaka suçları olarak nitelendiren görüşler olmuş ancak bu suçlar bilişim sistemi uzmanı olmayan herkes tarafından işlenebilecek suçlar olmaları dolayısıyla beyaz yaka suçlarından değildir. Bu suçlar ekonomik suçlar kategorisinde de değerlendirilmemeli zira bu suçlarla sadece ekonomik değerler ihlal edilememekte; verilerin hukuka aykırı ele geçirilmesi, sisteme yetkisiz giriş veya sistemde izinsiz kalma, kişilik haklarının ihlali gibi durumlarda farklı hukuki değerlerin ihlali söz konusu olup, ekonomik bir değer ihlali söz konusu değildir.⁹⁹

F. BİLİŞİM ALANINDAKİ SUÇLARA İLİŞKİN DÜZENLEMELER

a. AVRUPA KONSEYİ SİBER SUÇ SÖZLEŞMESİ

Klasik suç tanımlarında fiil belli bir coğrafi alanla sınırlıyken, bilişim teknolojileriyle dünyanın her yeri kolayca bir suç mahalli haline gelebilmektedir. Bu durum ise iç hukuk düzenlemelerinin işlenen fiiller karşısında yetersiz kalmasına neden olmaktadır. Bilişim sistemi ağlarının yaratmış olduğu coğrafi anlamda engel tanımayan ortam sayesinde, bilişim suçlarıyla mücadele konusunda ülkeler arası işbirliği olmaksızın başarı mümkün görünmemektedir.¹⁰⁰ Bilişim suçlarıyla mücadeleyle ilgili uluslararası alanda gerek Avrupa Birliği, Avrupa Konseyi, BM, OECD gibi hükümetler arası gerek de hükümet dışı uluslararası örgütler tarafından birçok çalışma yapılmıştır.¹⁰¹ Bunlardan en önemlilerinden biri de bilişim suçlarına dair ilk uluslararası sözleşme olan Avrupa Konseyi Siber Suç Sözleşmesidir (AKSSS).¹⁰² Sözleşme Avrupa Bakanlar Komitesi

⁹⁹ Akbulut, s. 26.

¹⁰⁰ Tezcan, Durmuş, “Bilişim Suçlarında Uluslararası Adli Yardımlaşma”, **Yaşar Hukuk Dergisi**, C. 1, S. 2, İstanbul 2019, s. 287-288.

¹⁰¹ Çalışmalara dair daha detaylı bilgi için bkz. Önok, Murat, “Avrupa Konseyi Siber Suç Sözleşmesi Işığında Siber Suçlarla Mücadelede Uluslararası İşbirliği”, Prof. Dr. Nur Centel’e Armağan, s. 1239-1241.

¹⁰² Açığöz, s. 40; Önok, s. 1241.

tarafından 8.11.2001 tarihinde kabul edilmiş, Budapeşte’de devletlerin imzasına 23.11.2001 tarihinde açılmış ve 1.07.2004 tarihinde yürürlüğe girmiştir.¹⁰³

AKSSS’nin gerekçesi niteliğindeki memorandumda sözleşmenin amaçlarının ulusal düzeydeki maddi ceza hukuku düzenlenmelerinin uyumlu hale getirilmesi, bilişim suçlarının muhakemesiyle ilgili gerekli yetkilerin sağlanması ve son olarak bilişim suçları alanında uluslararası işbirliğinin sağlanması olduğu belirtilmiştir.¹⁰⁴ Bu amaçların gerçekleştirilebilmesi için Sözleşme’de, maddi ceza hukukuna ilişkin suç olarak öngörülecek tipik fiillerin belirlenmesi konusunda asgari düzenlemeler öngörülmeyle çalışılmış ve bilişim suçları öngörülürken takip edilmesi gereken bazı ilkeler getirilmiştir. Bu ilkeler; bilişim suçları öngörülürken temel hak ve özgürlüklere bilhassa da düşünce ve ifade özgürlüğü, iletişim özgürlüğünün sınırlandırılmasında uyulması gereken ölçütlere dikkat edilmesi, hangi fiillerin suç olarak öngörülmesi gerektiği hususunda asgari standarda uygun düzenleme yapılması¹⁰⁵, fiillerin hukuka aykırı olması ve fiillerin kasten işlenmiş olmasıdır.¹⁰⁶

Türkiye bu sözleşmeyi 10.11.2010 tarihinde imzalamış, 22.04.2014 tarihinde uygun bulma kanunu Meclisten geçmiştir. Bakanlar Kurulu Sözleşmeyi 08.07.2014 onaylamış ve bu karar Resmî Gazetede 09.08.2014 tarihinde yayımlanmıştır.¹⁰⁷ Türkiye için bağlayıcı hale gelen bu sözleşmeyle devletlere hangi fiillerin suç haline getirilmesi gerektiği hususunda bazı yükümlülükler getirildiğinden, Türk kanun koyucusu da mevzuatını Sözleşmeye uyumlu hale getirmek için bazı çalışmalar yapmıştır. Bu doğrultuda TCK’da “*Bilişim Alanında Suçlar*” bölümünde, 6698 S Kanunla Sözleşmeye

¹⁰³ Önok, s. 1241; Mahmutoglu, s. 40; Ketizmen, s. 49; Karagülmez, s. 88.

¹⁰⁴ İçel, Kayıhan, “Avrupa Konseyi Siber Suç Sözleşmesi Bağlamında Avrupa Siber Suç politikasının Ana İlkeleri”, s. 6.

¹⁰⁵ Bu konuda sözleşmenin gerekçesinde devletlerin mevzuatlarını sözleşmeyle uyumlu hale getirirken bu asgari standartlara uymak koşuluyla başka fiilleri de suç olarak öngörebileceği belirtilmiştir. İçel s. 7.

¹⁰⁶ İçel, s. 6-8.

¹⁰⁷ Koca/ Üzülmüş, s. 892.

paralel olarak bazı deęişiklikler yapılmıştır. Söz konusu deęişikliklere ilgili oldukları yerlerde değinilecektir.¹⁰⁸

Bilişim suçlarıyla uluslararası mücadelede iş birliğinin etkili bir şekilde sağlanabilmesi için öncelikle maddi ceza hukuku kurallarının yeknesaklaştırılması elzemdir.¹⁰⁹ Ancak bilişim suçlarının tanımı ve ismi konusunda dahi ülkelerin ceza kanunlarında ortak düzenlenmelerin yer almaması adli yardımlaşmayı olumsuz etkilediğinden, ülke mevzuatlarının maddi ceza hukuku düzenlemelerinin bilişim suçları konusunda uyumlu hale getirilmesi adli yardımlaşmanın etkin bir şekilde işletilebilmesi için gereklidir.¹¹⁰ Ulusal mevzuatların uyumlu hale getirilmesinde amaç, adli yardımlaşmayı kolaylaştırmaktan ibaret olmayıp; bu suçlar için daha düşük standartta koruma getirmiş ülkelerde suçların yaygın şekilde işlenmesinin engellenmesi de hedeflenmektedir.¹¹¹

b. TÜRK HUKUKUNDA BİLİŞİM ALANINDA SUÇLAR

1. Tarihsel Gelişim

Bilişim terimi mevzuatımızda ilk defa 1989 tarihli TCK ön tasarısında kullanılmıştır. Tasarının “*Özel Hükümler*” başlıklı ikinci kitabının “*Topluma Karşı Suçlar*” kısmının 9. bölümü “*Bilişim Alanında Suçlar*” olarak düzenlenmiş¹¹² ve Tasarının 342. maddesinin gerekçesinde bilişim alanı “*bilgileri depo ettikten sonra bunları otomatik işleme tabi tutma sistemlerinden oluşan alan*” olarak tanımlanmıştır. Bu tanım 765 S TCK’ya “*Bilişim Alanında Suçlar*” başlıklı 11. bölümü ekleyen 14.06.1991

¹⁰⁸ Sözleşmenin 2. maddesine uygun olarak TCK 243. maddesinde ve, veya yapılmıştır. Sözleşmenin 3. maddesine uygun olarak TCK 243. maddesine 4. fıkra eklenmiştir. Sözleşmenin 6. maddesine uygun olarak 245/A maddesi kanuna eklenmiştir.

¹⁰⁹ Önok, s. 1233; Sokullu-Akıncı, s. 12.

¹¹⁰ Önok, s. 1234-1235.

¹¹¹ Sokullu-Akıncı, s. 12.

¹¹² Yılmaz, s. 207.

tarhli, 3756 sayılı yasanın gerekçesinde de korunmuştur.¹¹³ 1989 Tasarısı küçük deęişiklikler dışında 14.06.1991 tarihli 3756 sayılı TCK deęişiklięinin esasını oluşturmış¹¹⁴ ve bu deęişiklikle 765 S TCK’ya eklenen on birinci bab ile bilişim alanında suçlar mal aleyhine cürümler babında düzenleme altına alınmıştır.¹¹⁵ Söz konusu düzenleme bilişim suçlarına ilişkin mevzuatımızdaki ilk düzenlemedir.¹¹⁶

Godfrain Yasası olarak da geçen Fransa’da 1988 tarihinde yürürlüğe giren Bilişim Sahtekarlığına İlişkin Kanun, Türkiye’de bilişim alanında suçlara ilişkin ilk düzenlemelerin kaynağını teşkil etmektedir.¹¹⁷ 5237 S TCK’nın esasını oluşturan tasarılarıdaki bilişim suçlarına ilişkin düzenlemelerse, 1994’de yürürlüğe giren Fransız Ceza Kanunu örnek alınarak hazırlanmıştır.¹¹⁸

1997 tarihli TCK ön tasarısında bilişim “*verileri toplayıp, yerleştirdikten sonra bunları otomatik işlemlere tabi tutma imkânı veren manyetik sistemler*” şeklinde tanımlanmış, 2000 tarihli TCK ön tasarısında bilişim alanı “*verileri toplayıp yerleştirdikten sonra bunları otomatik olarak işleme tabi tutma imkânı veren manyetik sistemlerin oluşturduğu alan*” olarak tanımlanmıştır. 2003 tarihli TCK ön tasarısında bilişim kavramı yerine bilişim sistemi kavramına yer verilmiş ve bilişim sistemi “*verileri toplayıp yerleştirdikten sonra bunları otomatik olarak işleme tabi tutma olanağı veren manyetik sistemler*” olarak tanımlanmıştır. Bu tanıma 1 Haziran 2005’te yürürlüğe giren 5237 S. TCK’nın 243. maddesinin gerekçesine de deęiştirilmeden aktarılmıştır.¹¹⁹

¹¹³ Dülger, s. 69; Erem, Faruk, Bilgisayar Suçları ve Türk Ceza Kanunu, **TBB**, Ankara 1993, s. 178. Yenidünya/ Deęirmenci, s. 28; Erdoğan, s. 75.

¹¹⁴ Bu düzenleme sonrası 1995’te 4110 S Kanun ile FSEK’de deęişiklik yapılmış; bilgisayar programlarının da eser sayılacağı hüküm altına alınmış, ayrıca bunlara karşı gerçekleştirilen bazı eylemler yaptırım altına alınmıştır. Bilişim sistemlerinin ticarete kullanılmasıyla e-ticaret kavramı ortaya çıkmış; işlemler elektronik imza aracılığıyla yapılmaya başlanmış. Bu gelişmelere paralel olarak 2004’te Elektronik İmza Kanunu kabul edilmiştir. Karakehya, s. 5.

¹¹⁵ Deęirmenci, s. 197; Ketizmen, s. 54.

¹¹⁶ “Bilişim Alanında Suçlar” adıyla bir bab eklenmiş ve 525/a, 525/b, 525/c, 525/d maddelerinde suçlara yer verilmiştir. Karagölmez, s. 129; Soyaslan, s. 691.

¹¹⁷ Yazıcıoğlu, s. 207; Ketizmen, s. 59; Erem, s. 182; Tezcan/ Erdem/ Önok, s. 1146.

¹¹⁸ Yazıcıoğlu, s. 394.

¹¹⁹ Kurt, s. 25.

5237 S. TCK’da bilişim suçları “*Bilişim Alanında Suçlar*” başlığıyla “*Topluma Karşı Suçlar*” adını taşıyan üçüncü kısmın onuncu bölümünde 243 ila 246. maddelerinde hükme bağlanmıştır. Sırasıyla TCK 243. maddesinde “Bilişim Sistemine Girme”, TCK 244. maddesinde “Sistemi engelleme, bozma, verileri yok etme veya değiştirme”, TCK 245. maddesinde “Banka veya kredi kartlarının kötüye kullanılması”, TCK 245/A. maddesinde “Yasak cihaz veya programlar” ve TCK 246. maddesinde “Tüzel kişiler hakkında güvenlik tedbiri uygulanması” düzenlenmiştir. Ayrıca bilişim sistemlerinin kullanılması suretiyle bazı klasik suç tiplerinin işlenmesi de nitelikli hal olarak düzenlenmiştir.¹²⁰

2. Düzenleniş Biçimi

Bilişim suçlarının düzenlenmesi konusunda karşılaştırmalı hukukta temelde iki farklı sistem benimsenmiştir. Bazı ülkeler bilişim suçlarına ilişkin ayrı, yeni bir kanun çıkarırken (ABD- Anglo-Sakson Hukuk sistemleri); bazı ülkelerse ayrı düzenleme yapmaksızın mevcut ceza kanunlarına bu suçları ekleme yoluna gitmiştir. İkinci sistemi benimseyen ülkelere bazıları bilişim suçlarına kanunlarında ayrı bir bölüm içinde yer verirken (Fransa, Lüksemburg); diğerleri hukuki konularına göre ilgili suç tipinin altında bilişim suçlarına yer vermiştir (Almanya, İtalya).¹²¹ 5237 S TCK’da karma bir sistem benimsenerek, hem “Bilişim Alanında Suçlar” başlığı altında ayrı bir bölüme yer verilmiş hem de hukuki konularına göre bazı klasik suç tiplerinin bilişim sistemleri aracılığıyla işlenmesi nitelikli hal olarak öngörülmüştür.¹²²

5237 S. TCK’nın Adalet Komisyonu tarafından kabul edilen tasarısında, bölüm başlığı olarak “*Bilişim Sistemine Karşı Suçlar*” tercih edilmişti ancak yerinde bir tercih

¹²⁰ TCK 142/2-e, TCK 158/1-f

¹²¹ Kurt, s. 92; Erdoğan, s. 92-93.

¹²² Koca, s. 89-90; Değirmenci, s. 200-201; Yazıcıoğlu, s. 396.

değildi. Zira bilişim suçları sadece bu sistemlere karşı işlenmemekte; ayrıca bu sistemler aracılığıyla da işlenebilmekteydi.¹²³ TBMM Genel kurulunda verilen bir önergeyle bölüm başlığı hükümet tasarısında olduğu gibi “*Bilişim Alanında Suçlar*” olarak değiştirilmiş ve tasarı bu şekilde yasalaşmıştır.¹²⁴ Bu bakımdan kanunun tercihi yerindedir.

Bilişim suçlarının, TCK’nın “Topluma Karşı Suçlar” bölümünde düzenlenmesi doktrinde bazı tartışmaları tetiklemiş ve bu suçların “Topluma Karşı Suçlar” bölümünde düzenlenmesinin yerinde bir tercih olup olmadığı tartışılmıştır.¹²⁵ TCK sistematüğinde suçlar öncelikle mağdura göre tasnif edildiğinden bilişim suçlarının ihdas edilmesiyle korunmaya çalışılan hukuki değer veya menfaatin sahibi toplum mudur sorunu ve toplum olduğu kabulüne bağlı olarak genel hukuka uygunluk nedenlerinden rızanın bu suçlara uygulanabilirliği ve kimin rıza göstereceğı sorunu ortaya çıkmaktadır.¹²⁶

Bilişim suçlarının düzenlendiğı yeri isabetli bulan yazarlara göre bilişim sistemlerinin ve içerdığı verilerin güvenliğinin sağlanması, bu sistemlerin hayatın her alanında insanlar tarafında yaygın bir şekilde kullanılması dolayısıyla toplumsal bir önem taşımaktadır.¹²⁷ Her ne kadar kişilerin malvarlığı değerlerine dahil olan bu sistemlerin işleyişinin veya bu sistemlerin içerisindeki verilerin bütünlüğünün korunmaya çalışılması, bu suçların kişilere karşı suçlar bölümünde düzenlenmesi gerektiğı düşüncesini desteklese de günümüz teknolojisi ve bu teknolojinin hayatımızda edindiğı yer, bilişim sistemlerine ve içerisindeki verilere ilişkin korumanın kişilerin menfaatlerinin ötesinde olmasını zorunlu kılmıştır.¹²⁸ Kanun koyucu da bilişim sistemlerine; kişilere ait değerlerin ötesinde bir koruma sağlamak amacıyla, yani bilişim sistemlerinin ve içerisindeki verilerin güvenliğine daha büyük bir önem atfettiğinden, bu sistemlere

¹²³ Değirmenci, s. 198.

¹²⁴ Erdoğan, s. 16; Koca/ Üzülmmez, s. 889.

¹²⁵ Bilişim alanında suçların neden topluma karşı suçlar arasında düzenlendiğine dair kanun gerekçesinde bir açıklamaya yer verilmemiştir.

¹²⁶ Ketizmen, s. 62.

¹²⁷ Koca/ Üzülmmez, s. 889.

¹²⁸ Koca, s. 91.

toplum nezdinde duyulan güven ve sistemlerin işleyişine ilişkin toplumsal faydayı korumak istemiştir.¹²⁹ Bu nedenle bu suçlar Topluma Karşı Suçlar başlığı altında düzenlenmiştir.¹³⁰

Bilişim suçlarının düzenlendiği yeri isabetsiz bulan yazarlarsa TCK'nın benimsediği sistematigi, bilişim suçlarıyla asıl kişilerin bireysel menfaatlerinin ihlal edildiği¹³¹ ve suçların mağdurunun kişiler olduğu bu sebeple suçların kişilere karşı suçlar bölümünde düzenlemesi gerektiği gerekçesiyle eleştirmiştir.¹³²

Biz de bu suçların kişilere karşı suçlar bölümünde düzenlenmesi gerektiği kanaatindeyiz. Bu çerçevede çalışmamızın ikinci ve üçüncü bölümünde anlatılacağı üzere bilişim alanındaki suçlar farklı mağdurlara yönelik, farklı hukuki konulara sahip suçlardır. Bilişim alanındaki suçlar kategorisi, suçun bilişim alanında işlenmesine göre yapılmış bir ayırım olup, hukuki değer ya da mağdur ölçüt alınmadan farklı hukuki değerlere sahip suçlar aynı bölüm altında yaptırıma bağlanmıştır.¹³³ Dolayısıyla bilişim alanındaki suçlarda, hukuki konu ve mağdurun tespiti konusunda kanun koyucunun getirdiği sistematik yerine her norm, topluma karşı suçlar başlığı altında düzenlenmesinden bağımsız değerlendirilmelidir.¹³⁴ Buna paralel olarak suçun mağdurunun toplum olmadığının kabulüyle ileride anlatılacağı üzere bu suçlarla rıza hukuka uygunluk nedeninin bağdaştığı görüşündeyiz.

¹²⁹ Bir kimsenin kişisel bilgisayarına giren failin fiiliyle trafik sinyalizasyon sistemi veya havaalanı kontrol bilgisayarlarını işlev dışı bırakan failin fiili aynı düzeyde değildir. DEĞİRMENCİ, s. 198.

¹³⁰ Koca/ Üzülmüş, s. 889; Parlar, s. 25; Yaşar/ Gökcan/ Artuç, s. 7307.

¹³¹ TCK 245. maddesinin gerekçesinde “hırsızlık, dolandırıcılık, güveni kötüye kullanma ve sahtecilik suçlarının ratio legis’lerinin tümünü de içeren bu fiillerin, duraksamaları ve içtihat farklılıklarını önlemek amacıyla bağımsız suç haline getirilmeleri uygun görülmüştür.” demek suretiyle aslında bu suçların bireylerin kişisel menfaatlerini koruma amacını ortaya koymaktadır ki bu durum suçun hukuki konusunun kişilere ait olduğunu göstermektedir. Aynı şekilde TCK 244. maddesinin gerekçesinde de bu suçun ızzar suçunun özel bir halinin düzenlendiğinin belirtilmesi suçlarla kişilere ait menfaatlerin korunmaya çalışıldığını ortaya koymaktadır. Ketizmen, s. 64-65.

¹³² Soyaslan, s. 689.

¹³³ Koca/ Üzülmüş, s. 890.

¹³⁴ Böylelikle ilgilinin rızası hukuka uygunluk sebebi suçla bağdaşır. Ketizmen, s. 67.

İKİNCİ BÖLÜM

BİLİŞİM SİSTEMİNE GİRME SUÇU

I. GENEL OLARAK

Günümüzde bilişim sistemlerine yönelik haksızlık teşkil eden fiillerin cezalandırılması, bu sistemlere karşı gerçekleştirilen ve her geçen gün artış gösteren müdahaleleri engellemeye yöneliktir. Zira nasıl ki gerçek hayatta kişinin korunmaya değer menfaatlerinin ceza normuyla güvence altına alınması bir gereklilikse, sanal alanda bilişim sistemleri ve bu sistemler içerisindeki verilere ilişkin menfaatlerin korunması da bir gerekliliktir. Bilişim sistemlerinin haksız müdahalelerden korunması için cezai yaptırıma bağlanması gereken ilk fiillerden biri bilişim sistemine yetkisiz erişimdir.¹³⁵

765 S. TCK döneminde bilişim sistemine hukuka aykırı olarak girmek tek başına suç sayılmamakta; verilerin ele geçirilmesi aranmaktaydı.¹³⁶ Bilişim sisteminin ve içerdiği verilerin güvenliğini, gizliliğini sağlamak amacıyla AKSSS'nin 2. maddesine¹³⁷ uygun olarak bu eksiklik giderilmiş; sisteme izinsiz girmek veya sistemde izinsiz kalmak cezai müeyyideye bağlanmıştır.¹³⁸ Dolayısıyla bilişim sistemine girme fiili, verilerin ele geçirilmesi aranmaksızın 5237 S. TCK ile bağımsız bir suç haline getirilmiştir.¹³⁹

¹³⁵ Doktrinde bilişim sistemine girme suçu, geleneksel suçlardan konut dokunulmazlığını ihlal suçuna benzetilmektedir. Karagülmez, s. 175.

¹³⁶ 765 S TCK 525/a maddesinde verilerin ele geçirilmesi suç olarak düzenlenmekteydi ve sisteme girmek suç sayılmamaktaydı. 1997, 2000 ve 2003 TCK tasarılarında bilişim sistemine hukuka aykırı girmenin bağımsız bir suç olarak düzenlenmesi öngörülmüştür. Değirmenci, s. 204; Parlar, s. 15; Yazıcıoğlu, s. 237-238.

¹³⁷ Madde 2 Yasadışı Erişim: “Taraflardan her biri, bir bilgisayar sisteminin tamamına veya bir kısmına haksız yere gerçekleştirilen erişimi, kasten yapıldığı zaman, kendi iç hukuku kapsamında cezai bir suç olarak tanımlaması için gerekli olabilecek yasama tedbirlerini ve diğer tedbirleri kabul edecektir. Taraflardan biri, söz konusu suçun, bilgisayar verilerini elde etmek veya başka sahtekâr niyetle veya bir bilgisayar sistemine bağlı başka bir bilgisayar sistemiyle ilişkili olarak güvenlik tedbirlerinin ihlal edilmesi suretiyle işlenmiş olmasını şart koşabilir.”

¹³⁸ Avrupa Siber Suç Sözleşmesiyle getirilen yükümlülüğe uygun davranılmış, Sözleşmenin “Yasadışı Erişim” başlıklı 2. maddesi uyarınca bilişim sistemine girme suç haline getirilmiştir. Parlar, s. 15. Parlar, Ali / Hatipoğlu, Muzaffer: **Türk Ceza Kanunu Yorumu**, Ankara, Seçkin Yayınevi, 2010, s. 3467-3468.

¹³⁹ Karagülmez, s. 177; Yazıcıoğlu, s. 406; Parlar/ Hatipoğlu, s. 3467; Soyaslan, s. 692.

Bilişim suçlarının birçoğunun işlenebilmesi için bilişim sistemine girme veya sistemde kalma suçu, araç suç niteliğindedir.¹⁴⁰ Bilişim sistemine girme suçu, birçok başka suçun işlenmesini mümkün kıldığından; başlı başına sisteme girme veya kalmanın cezalandırılması bu suretle işlenebilecek başka suçlar açısından da önleyici bir etkiye sahip olacaktır.¹⁴¹ Bu nedenle TCK 243. maddesi isabetli bir düzenleme olmuştur.¹⁴²

Her ne kadar sisteme girilmesinin müstakil bir suç haline getirilmesi olumlu bir değişiklik olarak nitelendirilse de kanun koyucu, 765 S. TCK’da yer alan verilerin ele geçirilmesi suçunu 5237 S. TCK’da düzenlememiştir. Ele geçirilen veriler kişisel veri niteliğindeyse, verilerin TCK 136. maddesi bağlamında korunduğu; verilerin sistemden ortadan kaldırılarak ele geçirilmesi durumunda, verilerin TCK 244/2. maddesi bağlamında koruma altında olduğu söylenebilir.¹⁴³ Fakat bu suçlar açısından tipikliğin gerçekleşmediği durumlarda veriler korumasız kalmaktadır.¹⁴⁴ Bu eksikliğin giderilmesi gerekir.¹⁴⁵

TCK 243. maddesinde¹⁴⁶ bilişim sistemine girme suçu üç fıkra halinde düzenlenmiş; ilk fıkra suçun temel şekline, ikinci fıkra cezayı hafifletici nedene ve

¹⁴⁰ Karagülmez, s. 176.

¹⁴¹ Erdoğan, s. 117.

¹⁴² İhtiyaroğlu, s. 409.

¹⁴³ Yazıcıoğlu, s. 406.

¹⁴⁴ Bilişim Ağı Hizmetlerinin Düzenlenmesi ve Bilişim Suçları Hakkında Kanun Tasarısı’nda bu eksikliğe ilişkin bir maddeye yer verilmiş ve “bir bilişim sistemindeki veri veya programları hukuka aykırı olarak elde etme” fiili için Tasarının 15. Maddesinde cezai müeyyide öngörülmüş ancak Tasarı yasalaşmamıştır.

¹⁴⁵ Değirmenci, s. 208.

¹⁴⁶ Madde gerekçesinde “Bilişim sistemlerine karşı suçların düzenlendiği bölümde yer alan bu maddede bilişim sistemine girme fiili suç olarak tanımlanmıştır. Bilişim sisteminden maksat, verileri toplayıp yerleştirdikten sonra bunları otomatik işlemlere tâbi tutma olanağını veren manyetik sistemlerdir. Maddenin birinci fıkrasında bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak girmek veya orada kalmaya devam etmek fiili suç hâline getirilmiştir. Sisteme, hukuka aykırı olarak giren kişinin belirli verileri elde etmek amacıyla hareket etmiş bulunmasının önemi yoktur. Sisteme, doğal olarak, haksız ve kasten girilmiş olması suçun oluşması için yeterlidir. İkinci fıkraya göre, birinci fıkra tanımlanan fiillerin bedeli karşılığı yararlanılabilen sistemler hakkında işlenmesi, bu suç açısından daha az ceza ile cezalandırılmayı gerektirmektedir. Üçüncü fıkra, bu suçun neticesi sebebiyle ağırlaşmış hâli düzenlenmiştir. Birinci fıkra tanımlanan suçun işlenmesi nedeniyle sistemin içerdiği verilerin yok olması veya değişmesi hâlinde failin, suçun temel şekline nazaran daha ağır ceza ile cezalandırılması öngörülmüştür. Dikkat edilmelidir ki, bu hükmün uygulanabilmesi için, failin verileri yok etmek veya

üçüncü fıkradaysa neticesi sebebiyle ağırlaştırılmış suça yer verilmiştir.¹⁴⁷ 6698 S. Kanunla maddeye dördüncü bir fıkra eklenmiş ve bilişim sistemine girme tipik fiiliyle hiçbir ilgisi olmayan hatta sisteme girmeksizin işlenen teknik araçlarla veri naklinin izlenmesi suçuna yer verilmiştir. Söz konusu fıkra bağımsız, farklı bir suç düzenlendiğinden bu suç çalışmamızda ayrı bir başlık altında incelenecektir.

Mukayeseli hukukta bilişim sistemine girme suçu “*hukuka aykırı erişim*”¹⁴⁸, “*yetkisiz erişim*”, “*zorla erişim*”, “*hileyle erişim*” adlarına sahiptir.¹⁴⁹ Türk Ceza Kanunu Koyucusunun, takdirini AKSSS’den farklı olarak “erişim” ifadesi yerine “bilişim sistemine girme” ifadesinden yana kullanması doktrinde eleştirilmiştir. Zira “girme” kelimesinin fiziken bir yere girmeyi çağrıştırdığı ileri sürülmüş; bu ifade yerine erişim ifadesinin kullanılmasının daha yerinde bir tercih olacağı ifade edilmiştir.¹⁵⁰ “Girme” kelimesinin yerinde bir tercih olduğunu savunan yazarlara göre bu iki kavram aynı şeyi ifade etmemektedir. Bir sisteme giren kişi herhangi başka bir sistem ile bu sisteme erişen kişi olabileceği gibi; doğrudan, başka bir sistem kullanmadan bu bilişim sistemine giren kişi de olabilir. Dolayısıyla erişim ifadesinin uzaktan bir yere erişmeyi içerip, doğrudan sisteme girmeyi ifade etmemesine karşılık, “girme” kelimesinin hem uzaktan sisteme erişimi hem de doğrudan müdahale ederek sisteme girilmesini kapsamaması nedeniyle girmek fiili daha yerinde bir tercih olmuştur.¹⁵¹

Burada ister “girme” kelimesinin ister “erişim” kelimesinin doğru tercih olduğu savunulsun, TCK 243. maddesi kanun yapma tekniği açısından sorunlu bir maddedir.

değiştirmek kastıyla hareket etmemesi gerekir. Sistem içindeki bütün soyut unsurlar, fıkra da geçen “veri” teriminin kapsamındadır.” olduğu ifade edilmiştir.

¹⁴⁷ Hafizoğulları, Zeki/ Özen, Muharrem: **Türk Ceza Hukuku Özel Hükümler Topluma Karşı Suçlar**, Ankara, 2017, s. 445.

¹⁴⁸ Değirmenci, s. 209.

¹⁴⁹ Karagülmez, s. 175; Ketizmen, s. 100.

¹⁵⁰ Özbek, Veli Özer/ Doğan, Koray / Bacaksız, Pınar: **Türk Ceza Hukuku Özel Hükümler**, Ankara 2021, s. 960; Karagülmez, s. 182; Erdoğan, s. 1366.

¹⁵¹ Koca/ Üzülmüş, s. 900; Ekici/ Koruculu, s. 597-598.

Madde başlığı, “*Bilişim Sistemine Girme*” olarak isimlendirilse de maddede hem bilişim sistemine girme hem bilişim sisteminde kalma hem de sisteme girmeksizin veri nakillerinin teknik araçlarla izlenmesi suçları düzenlenmiştir. Hem birçok farklı suçun tek maddede hüküm altına alınması hem de madde başlığının madde metniyle uyuşmaması dolayısıyla TCK 243. maddesi kanun yapma tekniği bakımından yerinde bir düzenleme değildir.¹⁵²

6698 S. KVKK ile 24.03.2016 tarihinde maddenin ilk fıkrasında değişiklik yapılmış, “*hukuka aykırı olarak giren ve orada kalmaya devam eden*” ifadesindeki “ve” bağlacı “veya” olarak değiştirilmiştir.¹⁵³ Dolayısıyla eski haliyle bu suçun gerçekleşmesi için sadece sisteme girmek yetmemekte, ayrıca sistemde belli bir süre kalınması şartı aranmaktaydı.¹⁵⁴ Suçun varlığı için girmek ve kalmak şeklindeki hareketlerin birlikte aranması dolayısıyla bu suç çok hareketli bir suçtu¹⁵⁵ ve sisteme girmek ancak sistemde kalmamak suç teşkil etmediği gibi hukuka uygun olarak bilişim sisteme giren kişinin, bilişim sisteminde hukuka aykırı olarak bulunmaya devam etmesi halinde de suç oluşmuyordu.¹⁵⁶ Sisteme girmenin müstakil suç sayılmasıyla hem AKSSS 2. maddesiyle uyum sağlanmış hem de suç ileride daha detaylı anlatılacağı üzere seçimlik hareketli bir suç haline getirilmiştir.¹⁵⁷

6698 S, kanunla yapılan bir diğer değişiklik de TCK 243. maddesine dördüncü fıkra olarak “*Bir bilişim sisteminin kendi içinde veya bilişim sistemleri arasında gerçekleşen veri nakillerini, sisteme girmeksizin teknik araçlarla hukuka aykırı olarak izleyen kişi, bir*

¹⁵² Benzer yönde eleştiriler için bkz. Özbek/ Doğan/ Bacaksız, s. 959.

¹⁵³ TBMM Adalet Komisyonunda kabul edilen metnin ilk halinde madde 243/1’de veya bağlacı kullanılmış ancak TBMM Genel Kurulu’nda metnin görüşmeleri sırasında verilen önergeyle madde ve bağlacı haliyle yasalaşmıştır. Koca/ Üzülmüş, s. 894; Parlar, s. 16.

¹⁵⁴ Bu haliyle madde doktrinde eleştirilmiş, sisteme girmenin müstakil bir suç olarak düzenleme altına alınması gerektiği ifade edilmiştir. Parlar, s. 16; Taşkın, s. 20; Karagülmez, s. 179.

¹⁵⁵ Orta, s. 114.

¹⁵⁶ Mahmutoğlu, s. 860; Meran, s. 565; Ketizmen, s. 106-107.

¹⁵⁷ Avrupa Siber Suç Sözleşmesi madde 2 taraf devletlere “*bir bilgisayar sisteminin tamamına veya bir kısmına kasten ve haksız olarak erişilmesini suç haline getirmek için gerekli görülen yasal tedbirleri alma*” yükümlülüğü getirmiştir. Bahse konu maddeye göre sisteme erişilmesi yani girilmesi tek başına suç olarak belirtilmekte; ayrıca sistemde kalma aranmamaktadır. Koca/ Üzülmüş, s. 894.

yıldan üç yıla kadar hapis cezası ile cezalandırılır.” ibaresinin eklenmesidir. Söz konusu fıkra sisteme girme veya sistemde kalma suçundan tamamen farklı, yeni bir suç olan “veri nakillerini sisteme girmeksizin teknik araçlarla izleme suçu” düzenlenmiştir. Bu ekleme TCK’yı AKSSS’ye uyumlu hale getirmek için yapılmıştır.¹⁵⁸

A. HUKUKİ KONU

Suçun hukuki konusu suç ile ihlal edilen; ceza normuyla korunmaya çalışılan değer veya menfaattir.¹⁵⁹ Bilişim alanında suçlar kanunda düzenlenirken kanunun sistematigi dikkate alınmaksızın, ihlal edilen değerlere göre suçların ilgili bölümde düzenlenmesi yerine tek bir bölüm altında düzenleme yapılması yoluna gidilmiştir. Bu durum suçların hukuki konularını tespit konusunda farklı fikirlerin ortaya atılmasına neden olmuştur. TCK 243. maddesinde de bu sebeple korunmaya çalışılan hukuki değer ne olduğu konusunda doktrinde çok farklı fikirler ortaya atılmıştır.

Doktrinde birçok yazar burada korunmaya çalışılan hukuki değer in karma nitelikte olduğunu yani birden fazla hukuki değerin bu normla korunmaya çalışıldığını ileri sürmektedir.¹⁶⁰ Suçun hukuki konusunun karma nitelikte olduğunu savunan bu

¹⁵⁸ Dülger, s. 312.

¹⁵⁹ Toroslu Nevzat / Toroslu Haluk, **Ceza Hukuku Genel Kısım**, s. 109.

¹⁶⁰ Kişisel verilerin ve özel hayatın gizliliğinin korunması- Haberleşmenin gizliliğinin sağlanması hukuki konu diyen görüş: Mahmutoglu s. 859; Bu suçla ihlal edilen değerlerin bilişim sisteminin güvenliği ve güvenilirliği olduğunu ileri süren görüş, Tezcan/ Erdem/ Önok s. 1148-1149; “*Bilişim teknolojisindeki gelişmelere paralel olarak günümüzde bireyler birçok işlemi başta internet olmak üzere farklı bilişim sistemlerini kullanmak suretiyle yerine getirmektedir. Bu açıdan toplumda bu sistemlere karşı bir güven duygusu oluşmaktadır. Ayrıca kişisel kullanıma özgülenmiş bilgisayar gibi bilişim sistemlerinde kişiler, kendilerine özgü ve sadece kendilerinin yönetmek isteyecekleri bir alan oluşturmaktadırlar. Dolayısıyla bu alanın kişiliklerini rahatlıkla geliştirebilecekleri güvenli bir alan olmasını isteme ve bu güvenliğ in korunmasını bekleme hakkına sahiptirler. Şayet kişinin serbestçe üzerinde tasarrufla bulunabileceği verileri kapsayan ve dış etkilere karşı korumaya alınan bir bilişim sistemine, sistem sahibinin rızası hilafla ve hukuk aykırı bir şekilde yetkisiz erişim sağlanırsa, o sisteme karşı güven de ortadan kalkacaktır. Bir ölçüde bilişim alanında işlenen suçların topluma karşı işlenen suçlar kapsamında düzenlenmiş olmasının bir gereğesi olarak bu bilişim sistemlerine karşı toplumda ortaya çıkan güven duygusunun korunması ihtiyacı gösterilebilir. Bu nedenle TCK m. 243 ile bilişim sistemlerinin güvenliği ve güvenilirliğinin korunduğunu kabul etmek yerinde olacaktır.*” Özbek/Doğan/ Bacaksız, s. 956-957; Bilişim sisteminin güvenliği yanında verilerin gizliliğinin korunması, özel hayatı dokunulmazlığı ve kişi ve kurumların duyduğu güvenlik duygusunun korunmaya çalışılması hukuki konu diyen görüş Meran, s. 563; Bilişim sistemlerinin güvenilirliği, özel hayatın gizliliği, bilişim sistemi kullananların çıkarları hukuki konu diyen görüş: Taşkın, s. 23; Özel hayatın gizliliği ve sırların masuniyeti hukui konu diyen görüş için bkz. Kurt, s. 148; bilişim sistemlerinin güvenliği, güvenilirliği, özel hayatın gizliliği, haberleşme özgürlüğü hukuki konu diyen görüş için bkz. Meral Ekici Şahin/ Irmak Koruculu, s. 591; Toplum düzeni, özel hayatın gizliliği,

yazarlar farklı değer ihlallerinden bahsetseler de nihayetinde korunmaya çalışılan esas değer; sistemin güvenliği yanında özel hayatın gizliliği, hak sahibinin sistem üzerindeki tasarruf hakkı, sırların masuniyeti, haberleşmenin gizliliği, verilerin gizliliği, malvarlığı değerleri olduğunu iddia etmektedir. Ancak bu suçun gerçekleştirilebilmesi için haksız bir şekilde bilişim sistemine girmek ya da bilişim sisteminde kalmak yeterli görülmüştür. Bilişim sistemi üzerinde hak sahibi kimsenin bu sistemi kullanmasının engellenmesi, bu sistemdeki verilerin ele geçirilmesi veya başka herhangi bir değeri zarar veya tehlikeye sokma aranmamıştır. Kısacası suçun öngörülmesiyle asıl engellenmeye çalışılan sisteme yetkisiz erişimlerdir. Buradan yola çıkarak suçun ihdas edilmesiyle bilişim sistemlerinin güvenliğinin korunması amaçlandığından, suçun hukuki konusu da bilişim sistemlerinin güvenliğine ilişkin menfaattir.¹⁶¹

Kanun koyucu hayatın her alanında yaygın bir şekilde kullanılan bu sistemlere yönelik insanlarda oluşmuş güven duygusunun sisteme haksız müdahaleler durumunda zedeleneyeceğinden hem insanlardaki bu güven duygusunun kırılmaması hem de sistemin güvenliğini sağlamak için böyle bir düzenleme yoluna gitmiştir. Sonuç olarak TCK 243. maddesinde düzenlenen bilişim sistemine girme suçunun hukuki konusu bilişim

haberleşmenin gizliliği, kullanıcı ve sistem sahibinin menfaatleri, olası başka suçların önlenmesi, bilişim sisteminin güvenliği hukuki konu diyen görüş için bkz. Erdoğan, s. 1369-1373; özel hayatın gizliliği, sırların masuniyeti, haberleşme özgürlüğü, bilişim sisteminin güvenliği ve güvenilirliği, mülkiyet hakkı için bkz. Yaşar/ Gökcan/ Artuç, s. 7286; özel hayatın gizliliği ihlal, sistemin güvenliği hukuki konu diyen görüş için bkz. Soyaslan, s. 692; sistemin güvenliği, özel hayatın gizliliği, sırların masuniyeti, konut dokunulmazlığı, haberleşme özgürlüğü, verilerin gizliliği, mameleki değerler hukuki konu diyen görüş için bkz. Kayaer, s. 88-89; özel hayatın gizliliği, sırların masuniyeti ve bilişim sisteminin güvenliğidir hukuki konu diyen görüş için bkz. Orta, s. 111-112; Bireyin dijital ortamdaki özel alanı koruma altına alınmaya çalışılmakta, bu özel alanın korunma gerekçeleri farklı nedenlere dayanabilir ancak bu nitelikli hal ile özel alanın korunmasındaki amaç kişinin özel bir takım verilerini veya ona ait başkaca değerleri korumak değil; salt özel alanın sahibine ait ekonomik değerleri korumak şeklinde ortaya çıkmaktadır. Çünkü söz konusu sisteme girilmesi ve birtakım içeriklerin öğrenilmesi, içerik sahibi kimsenin gizli alanına ilişkin değildir; aksi takdirde bu içeriklerin ücret karşılığı herkesçe görülebilmesi içerik sahibi tarafından mümkün kılınmazdı. Karakehya s. 12; Ketizmen'e göre hem sistem üzerinde hak sahibi kimsenin tasarruf hakkı hem de malvarlığı değerleri bu suçun hukuki konusunu teşkil etmektedir. Ketizmen, s. 82 ve 99; Hukuki konu bilişim sistemlerinin “*geliştirilmesine, sağlıklı, güvenli, güvenilir işlemesine ilişkin ferdi- kamusal yarardır*” diyen görüş için bkz. Hafızoğulları/ Özen, s. 445.

¹⁶¹ Koca/Üzülmez, s. 895; Çetin, s. 4.

sistemlerinin güvenliğine ve toplumda bu sistemlere duyulan güvenin korunmasına ilişkin menfaattir.

B. MADDİ KONU

Suçun maddi konusu, “*suçun üzerinde işlendiği kişi veya şeydir*”.¹⁶² Bu suçun maddi konusu, hukuka aykırı olarak bir kısmına veya tamamına girilen ya da kalmaya devam edilen bilişim sistemleridir.¹⁶³ Burada bilişim sisteminin maddi/fiziki varlığı değil soyut varlığı suçun maddi konusunu teşkil etmektedir.¹⁶⁴ Cezayı hafifletici nedenin düzenlendiği ikinci fıkra da maddi konu, bedeli karşılığı yararlanılabilen bilişim sistemleridir. Neticesi sebebiyle ağırlanmış halin düzenlendiği üçüncü fıkra da maddi konu ise sistemdeki yok olan veya değişen verilerdir.¹⁶⁵ Veri taşıma araçlarındaki veriler de neticesi sebebiyle ağırlanmış halin konusu olabilecektir.¹⁶⁶

Suçun maddi konusu bilişim sistemlerinin bir kısmı da olabilir. Burada bilişim sisteminin bir kısmı ifadesiyle bilişim sisteminin tamamına değil de bir kısmına girişlere izin verildiği durumlarda, izin dahilinde olmayan bölümler açısından da koruma sağlanmak istenmiştir.

C. FAİL

Kanunda yazılı tipik fiili gerçekleştiren kimse faildir.¹⁶⁷ Kanun koyucunun ancak belirli hukuki veya fiili durumda olan kimsenin kanuni tipik fiili gerçekleştirebileceğini öngördüğü suçlara özgü suç denmektedir.¹⁶⁸ Bilişim sistemine girme suçunun

¹⁶² Yalçın Türkan / Köprülü Timuçin, **Ceza Hukuku Genel Hükümler Uygulamalı Çalışmaları**, Ankara, Savaş Yayınevi, 2019, s. 157.

¹⁶³ Tezcan/ Erdem/ Önok, s. 1150; Koca/ Üzülmüş, s. 897; Meran, s. 564; Parlar, s. 16; Taşkın, s. 24; Kurt, s. 150; Ekici/ Koruculu, s. 592; Soyaslan, s. 693.

¹⁶⁴ Yaşar/ Gökcan/ Artuç, s. 7289.

¹⁶⁵ Meran, s. 564; Yaşar/ Gökcan/ Artuç, s. 7288.

¹⁶⁶ Kayaer, s. 96.

¹⁶⁷ Hafizoğulları, Zeki/ Özen, Muharrem, **Türk Ceza Hukuku Genel Hükümler**, Ankara, US-A Yayıncılık, 2015, s. 373.

¹⁶⁸ Yalçın/ Köprülü, s. 156.

işlenebilmesi için özel bir faillik sıfatı veya niteliği aranmamıştır.¹⁶⁹ Yani bu suç, özgü suç değildir¹⁷⁰; herhangi bir kimse tarafından işlenebilir.¹⁷¹ Bir bilişim sistemine yetkisi olmaksızın, haksız bir şekilde giren ve/veya kalan kimse bu suçun failidir. Birinci bölümde de ifade edildiği üzere suçun faili olabilmek için bilişim sistemlerine dair yüksek derecede teknik bilgi sahibi olmak aranmamış; hukuka aykırı olarak kasten sisteme girebilen veya sistemde kalabilen herkes bu suçun faili olabilir.¹⁷² Ancak temel bilişim sistemi bilgisi bu suçun işlenmesi için yeterli olmayabilir. Yine de bu durum bilişim sistemine girme suçunu, özgü suç haline getirmemektedir.¹⁷³

Failin sıfatı bakımından nitelikli hal de öngörülmüş değildir.¹⁷⁴ Gerçekten de sahip oldukları yetki gereğince rahatça sisteme erişme imkânı olan kimselerin bu yetkileri aşkın kullanması durumu (örn: kamu görevlisi, banka çalışanı gibi) TCK'da cezanın ağırlaştırılması sebebi olarak kabul edilmediğinden, bu durum bir eksikliktir.

5237 S. TCK ile cezai sorumluluğun şahsiliği ve tüzel kişilerin ceza sorumluluğunun olmadığı kabul edildiğinden tüzel kişiler herhangi bir suçun faili olamaz¹⁷⁵; bilişim sistemine girme veya kalma suçunun da faili olamaz. Ancak TCK 246. maddesi gereği bu suçla “*yararına haksız menfaat sağlanan tüzel kişiler hakkında bunlara özgü güvenlik tedbirlerine hükmolunur.*”

D. MAĞDUR

Suçun mağduru, “*suçla zarara uğratılan veya tehlikeye maruz bırakılan hak veya yararın sahibidir.*”¹⁷⁶ Suçun mağduru suç teşkil eden fiille ihlal edilen; ceza normuyla

¹⁶⁹ Tezcan/Erdem/Önok, s. 1149; Koca/ Üzülmez, s. 896; Yaşar/ Gökcan/ Artuç, s. 7287.

¹⁷⁰ Erdoğan, s. 143.

¹⁷¹ Özbek/ Doğan/ Bacaksız, s. 958; Meran, s. 563; Taşkın, s. 23; Kurt, s. 241; Ekici/ Koruculu, s. 595; Karagülmez, s. 183; Hafizoğulları/ Özen, s. 445.

¹⁷² Kurt, s. 241.

¹⁷³ Erdoğan, s. 144.

¹⁷⁴ Ekici/ Koruculu, s. 595.

¹⁷⁵ Özgenç, İzzet, **Türk Ceza Hukuku Genel Hükümler**, s. 213-214.

¹⁷⁶ Dönmezer Sulhi / Erman Sahir: **Nazari ve Tatbiki Ceza Hukuku**, s, 726.

korunan menfaat veya değerin sahibi olduğundan suçun mağdurunun tespiti, suçun hukuki konusundan yola çıkarak yapılmalıdır.¹⁷⁷ Öncelikle biz tüzel kişilerin suçun mağduru olabileceğini kabul ettiğimizden bu suçun mağduru tüzel kişiler de olabilecektir.¹⁷⁸ Suçun mağduru olabilmek açısından herhangi bir hukuki veya fiili durumda olmak aranmadığından herhangi bir gerçek veya tüzel kişi suçun mağduru olabilecektir.

Yukarıda da ifade edildiği üzere suçun hukuki konusuna ilişkin doktrinde çok farklı fikirler ortaya atıldığından, mağdur konusunda da farklı görüşler ileri sürülmüştür. Bir görüş burada korunmaya çalışılan hukuki değerin bilişim sisteminin güvenliği olması nedeniyle mağdurun belirli bir kimse olmadığını iddia etmiştir.¹⁷⁹ Bir başka görüş suçun düzenlendiği yerin “Topluma Karşı Suçlar” olması ve güvenli bilişim ortamı sağlanmasında toplumsal menfaat olmasından hareketle mağdurun kamu idaresi olduğunu; kişilerinse ancak suçtan zarar gören sıfatını haiz olabileceklerini savunmuştur.¹⁸⁰

Doktrinde genel kanı TCK 243. maddesinde düzenlenen suçun mağdurunun, bir kısmına veya tamamına hukuka aykırı olarak girilen ya da kalınan bilişim sistemi üzerinde hak sahibi kimse/kimseler olduğu yönündedir.¹⁸¹ Sistem üzerinde hak sahibi kimse, bu sisteme girme ve/veya sistemde kalma hususunda yetkili olduğundan bu kimsenin zorunlu olarak sistem sahibi olması gerekmez. Hak sahipliği ifadesi çok geniş bir ifade olduğundan, sistem üzerinde hak sahibi ifadesinin suçun mağdurunun belirlenmesi açısından daraltılması gerekir. Zira sistem sahibi, sistem üzerinde hak sahibi olmaya devam ettiği gibi bu sistemi kullanma hakkı verilen kimseler de sistem üzerinde

¹⁷⁷ Katoğlu Tuğrul, Ceza Hukukunda Suçun Mağduru Kavramının Sınırları, *AÜHFD*, C. 61, S. 2, 2012, s. 660-661.

¹⁷⁸ Aynı yönde bkz. Ekici/ Koruculu, s. 596; İhtiyaroğlu, s. 415; Erdoğan, s. 145.

¹⁷⁹ Tezcan/ Erdem/ Önok, s. 1149.

¹⁸⁰ Hafizoğulları/ Özen, s. 445.

¹⁸¹ Mahmutoglu, s. 859; Özbek /Doğan/ Bacaksız, s. 958; Koca/ Üzülmez, s. 897; Kurt, s. 242; Ekici/ Koruculu, s. 596; Yaşar/ Gökcan/ Artuç, s. 7288.

hak sahibidir. Gerçekten de sistem üzerinde her hak sahibi bu suçun mağduru olarak değerlendirilmemelidir. Ancak sistem üzerindeki yetkisini doğrudan kullanabilen kişiler mağdur sıfatını haiz sayılmalıdır.¹⁸² Örneğin mülkiyet hakkı sahibi de sistem üzerinde hak sahibidir ancak bilişim sistemini kullanma yetkisinin kira sözleşmesi gibi bir hukuki ilişkiye dayalı başkasına devredildiği durumda artık sistemi kullanma yetkisi kiralayanda olacağından mağdur da o kişi olacaktır. Bu suçun hukuki konusu olan sistem güvenliği/güvenilirliğine ilişkin menfaat de sistem kullanıcısına ait menfaattir dolayısıyla mağdur sistemi kullanım yetkisini haiz kimsedir.

*“Bilişim sistemi üzerinde birden fazla hak sahibi varsa tüm hak sahipleri suçun mağduru olacaktır.”*¹⁸³ Ancak burada her bir hak sahibinin mağdur olduğu, sistem üzerindeki yetkilerini doğrudan kullanabilenler açısından kabul edilmelidir. Dolayısıyla sistem üzerinde hak sahibi kimse suçtan zarar görendir meğerki sistemi doğrudan kullanma yetkisi olmasın.

Hukuka aykırı olarak girilen bilişim sisteminde başkalarına ait verilerin bulunması durumunda, bazı yazarlar hem sistem sahibinin hem veri sahibinin suçun mağduru olacağını ileri sürmüştür.¹⁸⁴ Ancak TCK 243. maddesinde verilerin elde edilmesi değil; sisteme girilmesi veya sistemde kalınması cezai yaptırıma bağlanmıştır. Bu nedenle sistemde bulunan verilerin başkasına ait olup olmaması, TCK 243. maddesi özelinde önem taşımamaktadır. Dolayısıyla bilişim sistemindeki verilerin kime ait olduğuna bakılmaksızın suçun mağduru sadece sistem üzerinde hak sahibi kimsedir.¹⁸⁵

Doktrinde bir başka görüş hukuka aykırı olarak girilen bilişim sisteminin bankaya ait olması ve banka müşterilerinin bilgilerinin incelenmesi durumunda, bilişim sistemine girme suçunun mağdurunun banka müşterileri olduğunu; bankanın ise suçtan zarar gören

¹⁸² Özbek/ Doğan/ Bacaksız, s. 959.

¹⁸³ Koca/ Üzülmüş, s. 897.

¹⁸⁴ Erdoğan, s. 146.

¹⁸⁵ İhtiyaroğlu, s. 415.

olduğunu savunmaktadır.¹⁸⁶ Ancak bu görüşe katılmak mümkün değildir. Nitekim sistem üzerinde her ne kadar müşterilere ait veriler olsa da bilişim sistemi ve sistem içerisindeki veriler üzerinde tasarruf yetkilisi banka olduğundan, suçla doğrudan menfaati ihlal edilen kimse bankadır. Kısacası suçun mağduru girilen bilişim sisteminin sahibi bankadır.

E. SUÇUN UNSURLARI

a. MADDİ UNSUR

1. Genel Olarak

Suçun maddi unsuru fiildir. Fiilsiz suç olmaz ilkesi gereğince bir suçtan bahsedilebilmesi için ortada insana izafe edilebilen bir fiil olması gerekir.¹⁸⁷ Fiil de neticeli suçlar bakımından “*hareket, netice ve bu ikisi arasındaki nedensellik bağı*” olmak üzere üç alt unsura sahiptir. Ancak bütün suçlar neticeli olmadığından, netice ve nedensellik bağı fiilin zorunlu unsuru olmayıp sırf hareket suçları da denilen neticesiz suçlar bakımından hareket, suçun maddi unsurunu teşkil etmektedir.¹⁸⁸

TCK 243. maddesinin ilk fıkrasında suçun temel haline yer verilmiştir. İkinci fıkarda cezayı hafifletici neden, üçüncü fıkarda neticesi sebebiyle ağırlaştırılmış suçta yer verilmiştir. Tipik fiile bakıldığında, “*bir bilişim sisteminin bütününe veya bir kısmına hukuka aykırı olarak girilmesi veya orada kalmaya devam edilmesi*” suç olarak öngörülmüştür. Dolayısıyla suçun gerçekleşmesi için sistemin içerdiği verilerin öğrenilmesi, sisteme veya verilere zarar verilmesi ya da verilerin başka yere aktarılması bu madde kapsamında aranmamaktadır.¹⁸⁹ Bu yönüyle herhangi bir zarar veya somut bir tehlike aranmadığından başka bir deyişle suçun kanuni tanımındaki tipik fiilin icrasıyla

¹⁸⁶ Yaşar/ Gökcan/ Artuç, s. 7288.

¹⁸⁷ Hafizoğulları/ Özen, s. 167.

¹⁸⁸ Hafizoğulları/ Özen, s. 168.

¹⁸⁹ Koca/Üzülmez, s. 901; Meran, s. 564; Yaşar/ Gökcan/ Artuç, s. 7293.

suç tamamlandığından, bu suç neticesiz bir suçtur¹⁹⁰ ve soyut tehlike suçudur.¹⁹¹ TCK 243. maddesinin üçüncü fıkrasında düzenlenen, suçun neticesi sebebiyle ağırlaşmış hali bakımından bir zarar suçu söz konusudur.¹⁹² Nitekim hareket neticesinde verilerin değişmesi ya da yok olması aranmaktadır.

Bilişim sistemine girme suçunun gerçekleşmesi için zorunlu olarak sistemdeki güvenlik mekanizmalarının aşılması gerekli değildir. Şifresini bildiği bir sisteme ya da şifresi olmayan bilişim sistemine giren kimse, sistem sahibinin rızası hilafında hareket ettiğinden bu suç gerçekleşmiş olacaktır.¹⁹³

Bilişim sistemine girme suçu girme seçimlik hareketi bakımından sistemin soyut alanına erişildiği an; sistemde kalma seçimlik hareketi bakımından sistemin soyut alanında belirli bir süre kaldıktan sonra tamamlanır. Burada kalma seçimlik hareketi yeri geldiğinde anlatılacağı üzere temadi teşkil ettiğinden suçun tamamlanma anıyla suçun bitme anı farklı olabilir. Suç tamamlanmakla birlikte sona ermemiş olabilir. Kalma seçimlik hareketi bakımından suç sistemden çıkıldığı zaman sona ermektedir.

Failin sisteme hukuka aykırı olarak girmesi veya sistemde kalması başka bir ifadeyle doğrudan sistemin güvenliğini ihlal etmesi engellenmek istendiğinden, failin sisteme girip hiçbir dosyaya girmemesi durumu dahi bu suça vücut verecektir zira tipik hareket başlı başına sisteme girme fiilidir.¹⁹⁴ Ancak bilişim sistemine hukuka aykırı olarak giren kimse kişisel verileri elde ederse gerçek içtima hükümleri gereği fail hem TCK 243. maddesinden hem de TCK 136. maddesinden sorumlu olacaktır.¹⁹⁵

¹⁹⁰ Koca/ Üzülmmez, s. 901; Ekici/ Koruculu, s. 600; Ketizmen, s. 80; Yaşar/ Gökcan/ Artuç, s. 7294; Çetin, s. 5; Parlar, s. 16; Tezcan/ Erdem/ Önok, s. 1153.

¹⁹¹ Parlar, s. 16; Kurt, s. 152; Özsoy, s. 307; Mahmutoglu, s. 862; Tezcan/ Erdem/ Önok, s. 1159.

¹⁹² Tezcan/ Erdem/ Önok, s. 1153.

¹⁹³ İhtiyaroğlu, s. 420/421.

¹⁹⁴ Soyaslan, s. 693-694.

¹⁹⁵ Özsoy, s. 306.

TCK 243. maddesinde sistemin bütününe veya bir kısmına girme ya da sistemin bütününe veya bir kısmında kalma hareketleri cezalandırılmaktadır. Sistemin bir kısmına veya tamamına girilmesi suçun oluşumu bakımından fark yaratmayacak¹⁹⁶, sistemin bir kısmına girilmesi veya bir kısmında kalınması suretiyle de suçun kanuni tanımındaki tipik hareketler gerçekleştirilmiş olacaktır.¹⁹⁷ Dolayısıyla burada sistemin bir kısmının neyi ifade ettiği öncelikle açıklığa kavuşturulmalıdır. Bazı durumlarda sistemin ancak bir bölümüne girilmesine müsaade edilmiş olabilir. Bilişim sistemine girme yetkisi olan kimsenin kendisine yasaklanmış olan bir bölüme erişmesi durumunda bilişim sisteminin bir kısmına girme suçu oluşmuş olacaktır.¹⁹⁸ Örneğin hak sahibinin belirli bir amaç doğrultusunda kullanılması için ödünç verdiği sistemin, kişisel dosyalara bakılmak için kullanılması durumunda sistemin bir kısmına girme tipik hareketi oluşmuş olacaktır. Kanun koyucu da bunu öngörerek sistemin bütününe girilmesine izin verilmediği durumlarda, sistemin izin verilmeyen kısımlarına hukuka aykırı girmenin herhangi bir tartışmaya yol açmadan bu suça vücut vereceğini belirtmek için böyle bir düzenleme yoluna gitmiştir.

Bilişim sisteminin işlevini yerine getirmesi için sisteme bağlı olarak çalışan bütün donanım parçaları (hardware) bilişim sisteminin kısmıdır.¹⁹⁹ Bu çerçevede yedek depolama araçları, CD ve DVD okuyucu cihazlar bilişim sisteminin bir parçası olduğundan, bilişim sisteminin kısmı ifadesi altında değerlendirilmelidir.²⁰⁰ Veri taşıma araçları da bilişim sisteminin bir kısmı olduğundan, bu araçlara hakkı olmaksızın girilmesi halinde de bilişim sisteminin bir kısmına girme suçu açısından tipik hareket gerçekleşmektedir.²⁰¹

¹⁹⁶ Ketizmen, s. 103.

¹⁹⁷ Tezcan/ Erdem/ Önok, s. 1153.

¹⁹⁸ Ketizmen, s. 106.

¹⁹⁹ Örneğin tek başına bilişim sistemi sayılmamakla birlikte bankanın ana bilgisayarına bağlı işlev gören ATM'ler bilişim sisteminin kısmıdır. Kurt, s. 156.

²⁰⁰ Kurt, s. 156.

²⁰¹ Karakehya, s. 15; Kayaer, s. 101; Açıkgöz, s. 26.

Doktrinde bazı yazarlar madde metninde “*hukuka aykırı olarak*”, “*hukuka aykırı şekilde*” gibi ifadelerin geçmesi haline yani suçun kanuni tanımında hukuka aykırılığın vurgulanması durumuna hukuka özel aykırılık hali demektedir.²⁰² Hukuka aykırılık unsuruna tipiklikte yer verildiğinden, failin işlediği fiilin haksızlık teşkil ettiği bilincine sahip olması aranmaktadır.²⁰³ Yani failin kastının hukuka aykırılığı, işlediği fiilin haksızlık teşkil ettiğini (haksızlık bilinci) de kapsamı gerektiği savunulmaktadır. TCK 243. madde metninde suç tanımında “*hukuka aykırı olarak*” ifadesine yer verilmiştir. Dolayısıyla failin haksızlık bilinciyle yani işlediği fiilin hukuka aykırı olduğunu bilerek ve isteyerek hareket etmesi gerekir.²⁰⁴ Yargıtay da bu doğrultuda bazı kararlarında failde hukuka aykırılık bilinci olmadığından bahisle kastın oluşmadığına hükmetmiştir.²⁰⁵

Bilişim sistemine girme suçu bakımından hukuka özel aykırılık hali söz konusu olduğundan²⁰⁶, rıza gibi bir hukuka uygunluk nedeninin var olduğunu sanarak sisteme girilmesi halinde haksızlık bilinci kast kapsamında değerlendirildiğinden, hata suçun kanuni tanımında yer alan bir unsura ilişkin olduğundan TCK 30/1. maddesi kapsamında değerlendirilmelidir.²⁰⁷

2016’da 6698 S KVKK ile “ve” bağlacının “veya” bağlacı olarak değiştirilmesi sonrası, TCK 243/1. maddesi seçimlik hareketli bir suç haline gelmiştir²⁰⁸ Bilişim sistemine hukuka aykırı bir şekilde girmek ya da bilişim sisteminde hukuka aykırı bir

²⁰² Koca/ Üzülmüş, Genel Hükümler, s. 267.

²⁰³ Koca/ Üzülmüş, s. 903.

²⁰⁴ Yazar düzenlemeyi yerinde görmektedir zira eylemin suç teşkil ettiğini bilmeyenler cezalandırılmayacaktır. Yazıcıoğlu s. 407; Ekici Şahin/ Koruculu, s. 608; Soyaslan, s. 695.

²⁰⁵ Yargıtay uygulamaları incelendiğinde boşanma davalarında eşlerin delil elde edebilmek amacıyla diğer eşin bilişim sistemine girmesi durumunda haksızlık bilincinin var olmadığını dolayısıyla suçun oluşmadığına hükmedilmiştir. Bkz. Yargıtay 12. CD E. 2015/439, K. 2015/10716. T. 15.06.2015 Ancak bu karara katılmak mümkün değildir zira sanığın delil elde etme amacı sanıkta haksızlık bilincinin bulunmadığı anlamına gelmez. Bu durumda mağdurun boşanma sürecinde olduğu eşe bu konuda rıza göstermeyeceği açık olduğundan haksızlık bilincinin varlığı kabul edilmelidir. Ancak boşanma sürecinde olmayan eşlerin izinsiz böyle bir fiili işlemleri durumunda TCK 30/4. maddesinde yer alan hukuki hata durumu uygulama alanı bulabilecektir. Ekici Şahin/ Koruculu, s. 609-610; Tezcan/ Erdem/ Önok, s. 1156.

²⁰⁶ Bir görüş burada bilişim sistemine girmenin az da olsa teknik bilgi gerektirmesinden dolayı failin fiilinin hukuka aykırılığını bilmemesinin mümkün olmadığını ve bu sebeple hukuka özel aykırılık halinin bu suç için geçerli olmadığını ifade etmiştir. Kurt, s. 158.

²⁰⁷ Ekici Şahin/ Koruculu, s. 613-614; Tezcan/ Erdem/ Önok, s. 1155.

²⁰⁸ Tezcan/ Erdem/ Önok, s. 1151; Özbek/ Doğan/ Bacaksız, s. 960; Koca/ Üzülmüş, s. 899.

şekilde kalmak suretiyle bu suç işlenebilecektir.²⁰⁹ Seçimlik hareketli suçlarda hareketlerden birden fazlasını yapmak birden fazla suça değil, tek suça vücut vermektedir.²¹⁰ Yani sisteme girip, sistemde kalmaya devam eden kişi tek bir bilişim sistemine girme suçunu işlemiş sayılır.²¹¹

Maddede yapılan değişiklik öncesi sadece sisteme girmek bu suça vücut vermiyor, sistemde belli bir süre kalınması da aranıyordu. Bu sebeple sisteme girme suçu bazı yazarlara göre mütemadi²¹² bazı yazarlara göre çok hareketli²¹³ bazı yazarlara göreyse karma hareketli bir suçtu.²¹⁴ Yapılan değişiklik sonrası müstakil olarak sisteme girme de suç haline getirilmiş ve artık sisteme girdikten sonra sistemde kalmadan, sistemden hemen çıkılması fiili de cezalandırılabilir.²¹⁵ Dolayısıyla sisteme hukuka aykırı olarak erişen kimsenin sistemde kalıp kalmadığı, kaldıysa ne kadar süre kaldığı suçun gerçekleşmesi bakımından önem arz etmez zira suç zaten gerçekleşmiştir.²¹⁶

2. Bilişim Sistemine Girme

Kanuni tanımdaki tipik hareketin gerçekleştirilmesiyle tamamlanan suçlar ani hareketli olduğundan,²¹⁷ “*bilişim sistemine girme*” seçimlik hareketi bakımından TCK 243. maddesi ani hareketli bir suçtur. Yani suçun işlenmesi için sisteme girmek uzun bir vakti alsa da suç, sisteme girildiği an gerçekleşmiş olacağından ani hareketli bir suçtur.

²⁰⁹ Doktrinde bu suçun serbest hareketli suç olduğunu iddia eden yazarlar olmuştur. Fakat serbest hareketli suçlarda kanuni tanımda suçun işlenebileceği hareketlere yer verilmemekte; sadece hangi durumun ihlal teşkil ettiği ifade edilmektedir. TCK 243. maddesinde ise bu suçun sisteme girmek ya da sistemde kalmak şeklinde işlenebileceği açık bir şekilde ifade edilmiştir.

²¹⁰ Artuk/ Gökçen, **Ceza Hukuku Genel Hükümler**, s. 319.

²¹¹ Özbek/ Doğan/ Bacaksız, s. 961; Koca/ Üzülmüş, s. 900.

²¹² Kurt, s. 153; Ketizmen, s. 106-107.

²¹³ Karakehya, s. 13; Mahmutoglu, s. 860; Taşkın, s. 25; Yaşar/ Gökcan/ Artuç, s. 7292.

²¹⁴ Sisteme girmek için icrai bir hareket gerekir ve kalma hareketiyle ihmali olarak suça devam edilir. Ancak bu durum suçu kesintisiz suç haline getirmez, suç karma hareketli ani bir suçtur. Hafizoğulları/ Özen, s. 447.

²¹⁵ Tezcan/ Erdem/ Önok, s. 1153.

²¹⁶ Tezcan/ Erdem/ Önok, s. 1152.

²¹⁷ Koca/ Üzülmüş: Genel Hükümler, s. 124.

Ayrıca sisteme girme seçimlik hareketi bakımından bu suç icrai hareketle gerçekleştirilebilir.²¹⁸

“Bilişim sistemine girmek” ifadesi bilişim sisteminin fiziki parçalarının açılarak içine girilmesinden ziyade sistemin soyut alanına hukuka aykırı olarak erişmeyi ifade etmektedir.²¹⁹ “Sisteme girme” hareketi açısından herhangi bir yöntem belirlemesi yapılmamıştır dolayısıyla sisteme girmeyi sağlayacak elverişli her türlü hareketle bu suç işlenebilir.²²⁰ Bu fiil doğrudan bilişim sisteminin fiziki parçalarına temas etmek suretiyle işlenebileceği gibi bir ağ üzerinden sisteme girmek şeklinde de işlenebilir.²²¹ Aynı şekilde fail sisteme giriş şifresini ele geçirerek, sistemdeki güvenlik açıklarından faydalanarak veya güvenlik açığı oluşturularak bu suçu işleyebilir.²²² Dolayısıyla suçun oluşması için fiziken sistemin yakınında veya uzağında olmak önem arz etmez.²²³

Hak sahibi kimse tarafından açılan bilişim sistemini veya içindeki dosyayı başkasının görmesi halinde, bilişim sistemine herhangi bir müdahale söz konusu olmadığından ortada suç yoktur. Ancak açık bulunan bir bilişim sisteminin, hak sahibinden izin alınmaksızın kullanılarak, sistem içeriğine nüfuz edilmesi durumunda artık kanuni tipe uygun eylemin gerçekleştiği kabul edilmelidir.²²⁴

Bilişim sistemine e-posta gönderilmesi tek başına bu suça vücut vermeyecektir meğerki sisteme gönderilen e-postada yer alan bir programın açılması suretiyle sisteme girme mümkün olsun. E-posta ile gönderilen programın açılması aracılığıyla bilişim sistemine girilmesinin mümkün olduğu örneklerde, gönderilen e-postanın açılmaması

²¹⁸ Tezcan/ Erdem/ Önok, s. 1152; Koca/ Üzülmöz, s. 900; Ekici/ Koruculu, s. 600.

²¹⁹ Parlar, s. 16; Taşkın, s. 25; Parlar/ Hatipoğlu, s. 3469; Erdoğan, s. 126.

²²⁰ Koca/ Üzülmöz, s. 901; Parlar, s. 16.

²²¹ Kurt, s. 156; Ketizmen, s. 103.

²²² Hafizoğulları/ Özen, s. 446; Ekici/ Koruculu, s. 598.

²²³ Erdoğan, s. 126.

²²⁴ Erdoğan, s. 132.

durumunda suçun icrasına elverişli hareketlerle doğrudan doğruya başlandığından teşebbüsten sorumluluk doğacaktır.²²⁵

Failin sisteme kimin için girdiğinin diğer bir ifadeyle kendisi için veya başkası için sisteme girmiş olması suçun gerçekleşmesi bakımından bir fark yaratmamaktadır.²²⁶ Doktrinde bir görüş bilişim sistemine girme suçunun oluşabilmesi için sisteme erişimi sınırlayan tedbir veya uygulamaların varlığı şart koşmaktadır.²²⁷ Bu görüşe göre yeterli veya hiç güvenlik tedbirinin olmamasından faydalanılarak sisteme girildiği örneklerde suç oluşmamaktadır. Ancak “bilişim sistemine girme” suçunun oluşması için bilişim sisteminde şifre benzeri güvenlik mekanizmalarının varlığı şart değildir.²²⁸ Hak sahibi kimsenin iradesine aykırı olarak sisteme girilmiş olması yeterlidir.²²⁹ Suçun kanuni tanımında da tipik hareketin gerçekleştirilebilmesi için bilişim sisteminde güvenlik tedbirlerinin varlığı aranmadığından, böyle bir şartın aranması kanunilik ilkesiyle bağdaşmayacağı gibi güvenlik tedbirlerinin olmadığı sistemleri maddenin koruma alanı dışında bırakacaktır.

Birden fazla kullanıcısı bulunan bir bilişim sisteminde, genel kullanıcı hesabı üzerinden başka bir deyişle başkasının şifreli hesabına müdahale etmeden o sistemin kullanılması bu suça vücut vermeyecektir.²³⁰ Ancak belirli bir amaç doğrultusunda sistemin kullanılmasına izin verildiği durumda, sisteme bu amaç dışında girilmesi bu suça vücut verecektir.²³¹

Kamu görevlilerine ve özel sektör çalışanlarına görevleriyle bağlantılı olarak tahsis edilmiş bilişim sistemleri, bu kişilerce amaç dışı örneğin kişisel işlerin görülmesi

²²⁵ Mahmutoglu, s. 861.

²²⁶ Taşkın, s. 26.

²²⁷ Özbek/ Doğan/ Bacaksız, s. 960; Kayaer, s. 99.

²²⁸ Tezcan/ Erdem/ Önok, s. 1151; Koca/ Üzülmüş, s. 900; Taşkın, s. 27; İhtiyaroğlu, s. 428.

²²⁹ Şifresiz bir bilgisayarın sahibinin rızası olmaksızın açılması halinde dahi bu suç oluşur. Ekici Şahin/ Koruculu, s. 601.

²³⁰ Ekici Şahin/ Koruculu, s. 605.

²³¹ Tezcan/ Erdem/ Önok, s. 1152.

için kullanılamaz.²³² Kamu kurum ve kuruluşlarında belirli kimseye tahsis edilmiş ve/veya zimmetlenmiş bilişim sistemine başkası tarafından işlerin yürütülmesi amacıyla sistemin kendisine zimmetlendiği kişinin hesabına müdahale edilmeden girilmesi, TCK 243. maddesi kapsamında değerlendirilemeyecektir.²³³

Kamu görevlileri veya özel sektör çalışanlarına görevleriyle ilgili tahsis edilmiş bilişim sistemlerine yetkili amir veya görevli kimse tarafından teftiş amacıyla incelenmek üzere girilmesi TCK 243. maddedeki suçu oluşturmayacaktır.²³⁴ Ancak burada yapılacak inceleme, çalışanların özel hayatının gizliliği ve haberleşme özgürlüğü göz önünde bulundurularak yapılmalıdır. Zira söz konusu inceleme özgürlükleri kısıtlayacak bir müdahale olduğundan işverenin sınırsız inceleme yetkisi söz konusu olmayacak ve bu müdahale için açık bir yasal düzenlemenin varlığı gerekecektir.²³⁵ Az önce de ifade edildiği üzere inceleme yetkisi söz konusu olabilecek ancak bu inceleme yetkisi belirli koşullar altında kullanılabilir. Bu koşullar, inceleme yetkisini gösteren bir yasal düzenlemenin varlığı ve incelemenin işverenin haklarını korumak gibi meşru bir amaca dayanmasıdır.²³⁶

AYM, başvuru numarası 2013/4825 olan 24.03.2016 tarihli kararında inceleme şeklindeki müdahale, özel hayata saygı ve haberleşmenin gizliliğine müdahale niteliğinde olduğundan meşru bir amaca dayalı olarak, sınırsız ve keyfi olmadan ölçülü bir şekilde bilişim sistemlerinin incelenebileceğini belirtmiştir.²³⁷ İşletmenin ticari gerekleri ve iç disiplinini sağlamak için denetim yapılabilmesine dair düzenlemenin olduğu ve

²³² Ekici Şahin/ Koruculu, s. 603-604.

²³³ Ekici Şahin/ Koruculu, s. 605.

²³⁴ Ekici Şahin/ Koruculu, s. 605.

²³⁵ AİHM Amann v. İsviçre ve Halford v. Birleşik Krallık kararlarında çalışanın e-posta ve internet kullanımının özel hayatın gizliliği ve haberleşme özgürlüğü kapsamında korunması gerektiğini, çalışana bu konuda inceleme yapılacağına dair hiçbir uyarı yapılmadan yürütülen denetiminse özel yaşama ve haberleşme hakkına saygı ilkesine aykırı olacağına hükmetmiştir. Tezcan/ Erdem/ Önok, s. 1156-1157.

²³⁶ Söz konusu kriterler AİHM'in Libert v. Fransa kararında tespit edilen ölçütlerdir. Bkz. Tezcan/ Erdem/ Önok, s. 1157.

²³⁷ Tezcan/ Erdem/ Önok, s. 1157.

alıřanların nceden byle bir dzenleme erevesinde inceleme yapılacađına dair uyarılması gerektiđini ifade etmiřtir. Yani alıřanlara grevleriyle ilgili tahsis edilen biliřim sistemlerinin veya kurumsal e-postaların incelenmesi amacıyla sistemlerine girilmesi ancak bu konuda aık bir dzenleme olduđunda ve bu dzenlemeye dair alıřanlar nceden bilgilendirildiđinde hukuka uygun nitelikte olacaktır.²³⁸

Bu su zelinde ok kullanıcılı sistemlerin ayrıca incelenmesinde fayda vardır. Zira sisteme birden fazla kiřinin eriřim yetkisi olmakla birlikte, bu yetkilerin sistemin belli kısımları zelinde sınırlandırılmış olması mmkndr. Bu noktada her bir kullanıcının sisteme eriřim yetkisi gz nnde bulundurularak suun oluřup oluřmadıđı hususunda belirleme yapılacaktır.

ok kullanıcılı bir sisteme girme yetkisi olan kimsenin bařka bir kullanıcı hesabından sisteme girmesi durumunda kural olarak bu su gerekleřir.²³⁹ Doktrinde bir grře gre st dzey iřlem yapma yetkisine sahip sistem kullanıcısının, alt dzey iřlem yapma yetkisine sahip sistem kullanıcısının hesabına girmesi kural olarak su teřkil etmeyecektir nitekim ortada bir yetki ařımı yoktur. Fakat bu durumun tersi iin sisteme yetkisiz giriř gerekleřmiř olacaktır. Aynı dzeyde yetkiye sahip kullanıcılar sz konusu olduđundaysa kullanıcıların yetkilerine bakılarak sisteme giriřin hukuka aykırı olup olmadıđı tespit edilecektir.²⁴⁰ Ayrıca bu grře gre biliřim sistemini kullanma yetkisinin belli bazı blmler ya da verilerle kısıtlanmış olduđu durumda, yetkisi kısıtlanmış kimsenin kendisi iin yasaklı kısımlara girmesi ya da verilere bakması veya kendisinden daha geniř yetkilere sahip bir kullanıcı hesabından sisteme giriř yapması bu sua vcut verecektir. Biliřim sisteminde aynı dzeyde kullanım yetkisine sahip kullanıcıların sisteme veya verilere eriřim konusunda aralarında bir fark yaratılmamıřsa bu kiřilerden

²³⁸ Tezcan/ Erdem/ nok, s. 1158; Ekici řahin/ Koruculu, s. 607.

²³⁹ Ketizmen, s. 104.

²⁴⁰ Ketizmen, s. 104.

birinin diğzerinin hesabından sisteme giriş yapması durumunda bu suç oluşmayacak; ancak sistemin bölümü veya erişilebilecek veriler konusunda bir farklılık yaratılmışsa bu durumda aynı düzeyde yetkiye sahip bir kullanıcının diğzerinin kullanıcı hesabından sisteme girmesi durumunda TCK 243. maddesi gerçekleşmiş olacaktır.²⁴¹

Ancak çok kullanıcılı bir bilişim sisteminde ayrı kullanıcı hesaplarının açılmasının nedeni, her bir kullanıcı açısından bireysel kullanım alanı yaratmak ve bu çerçevede iş alanında da olsa belirli düzeyde gizliliği sağlamak olduğundan, aynı düzeyde yetkiye sahip kullanıcıların ve hatta üst düzey yetkili kullanıcıların özel olarak yetkilendirilmediği veya hesap sahibinin rızası bulunmadığı takdirde başkasının kullanıcı hesabı üzerinden sisteme giriş yapılması durumunda bilişim sistemine girme suçunun işlendiği kanaatindeyiz.

3. Bilişim Sisteminde Kalma

Failin suç teşkil eden ihlali, iradesiyle devam ettirdiği suçlar mütemadi (kesintisiz) suçlardır.²⁴² Bilişim sisteminde kalma seçimlik hareketi bakımından ihlalin yani bilişim sisteminde kalmanın belli bir süre devam etmesi gerektiğinden kalma seçimlik hareketi bakımından bu suç mütemadi (kesintisiz) bir suçtur.²⁴³

Doktrinde bir görüş sistemde kalma seçimlik hareketi bakımından bu suçun hem ihmali hem icrai hareketle işlenebileceğini savunmaktadır.²⁴⁴ Ancak bu görüşe katılmak mümkün değildir. Zira sistemde kalma seçimlik hareketi, sisteme hukuka uygun veya aykırı girdikten sonra sistemde bulunmaya devam etmek şeklinde gerçekleştirilmektedir.²⁴⁵ Dolayısıyla fail aslında çıkması gereken bir sistemden

²⁴¹ Ketizmen, s. 105.

²⁴² Yalçın/ Köprülü, s. 181.

²⁴³ Tezcan/ Erdem/ Önok, s. 1152; Ekici/ Koruculu, s. 601; Kayaer, s. 105.

²⁴⁴ Tezcan/ Erdem/ Önok, s. 1152

²⁴⁵ Hukuka aykırı şekilde sisteme girilmiş olması durumunda suçun zaten girme seçimlik hareketi bakımından gerçekleşmesi dolayısıyla kalma seçimlik hareketi bakımından suçun ancak hukuka uygun bir şekilde veya kast olmaksızın sisteme girilmesi fakat hukuka aykırı olarak sistemde bulunmaya devam edilmesi suretiyle işlenebileceğini savunan görüş için bkz. Koca/Üzölmez s. 900.

çıkımayarak yani hukuken yapması gereken bir hareketi yapmayarak bu suçu işlediğinden; sistemde kalma seçimlik hareketi bakımından bu suç ihmalî hareketle işlenmektedir.²⁴⁶

TCK 243. maddesinin kalma seçimlik hareketiyle işlenmesi için farklı ihtimaller söz konusu olabilir. Öncelikle kalma seçimlik hareketiyle bu suçun işlenebilmesi için sisteme girmek gerekir. Burada hukuka aykırı olarak sisteme girilmiş olması, sistemde kalma suçu açısından zorunlu bir unsur değildir.²⁴⁷ Zira sisteme hukuka aykırı olarak girilmesiyle zaten TCK 243. maddesi ihlal edilmiş olmakta, failin ayrıca sistemde kalması aranmamaktadır.²⁴⁸ Fail hukuka uygun olarak sisteme girmiş ancak çıkması gereken sistemde kalmaya devam etmiş, zaten açık olan sistemde hak sahibinin rızası olmadan kalmaya devam etmiş²⁴⁹, kastı olmaksızın yanlışlıkla girdiği sistemde bu durumu fark etmesine rağmen kalmaya devam etmiş²⁵⁰ veya hukuka aykırı olarak bir başkasının erişmiş olduğu sistemde kalmaya²⁵¹ devam etmiş olabilir. Son ihtimalde sisteme hakkı olmaksızın giren kişi ve sistemde kalmaya devam eden kişi ayrı ayrı TCK 243. maddesinden sorumlu olacaktır çünkü suçun kanuni tanımındaki farklı tipik hareketleri gerçekleştirmektedirler.

Bilişim sisteminde kalma seçimlik hareketi bakımından bu suç kesintisiz bir suç olduğundan, suçun gerçekleşmesi için failin ne kadar süre sistemde kalması gerektiğinin kanunda belirtilmemesi sorun olarak karşımıza çıkmaktadır. Bu soru karşısında 5 dakika gibi net bir süre söylemek herhangi bir mantığa dayanmadığından, somut olayın özellikleri değerlendirilerek belirleme yapılması en sağlıklı çözüm olacaktır. Doktrinde bazı yazarlar sistemde kalma seçimlik hareketi bakımından, ne kadar süre sistemde

²⁴⁶ Koca/ Üzülmüş, s. 900.

²⁴⁷ Tezcan/ Erdem/ Önok, s. 1152; Özbek/ Doğan/ Bacaksız, s. 961.

²⁴⁸ Koca/ Üzülmüş, s. 902.

²⁴⁹ Örneğin başkasının bilgisayarından sosyal medya hesabına girdikten sonra hesabını kapatmayı unutan kimsenin sosyal medya hesabından çıkımayarak sistemde kalmaya devam eden bilgisayar sahibi bu suçu işlemiş olacaktır. Tezcan/ Erdem/ Önok, s. 1152.

²⁵⁰ Koca/ Üzülmüş, s. 902.

²⁵¹ Tezcan/ Erdem/Önok, s. 1152.

kalındığının suçun oluşumu bakımından önemli olmadığını savunmaktadır. Bu yazarlara göre ne kadar sistemde kalındığı cezanın belirlenmesi bakımından önem taşımaktadır.²⁵² Ancak bu görüşe katılmak mümkün değildir. Nitekim kalma eylemi temadi teşkil ettiğinden belirli bir süre sistemde kalınması şarttır. Bu sürenin belirli bir uzunlukta olması aranmalıdır ki suçun gerçekleşip gerçekleşmediği somut olayda belirlenebilsin.²⁵³

Doktrinde bizim de katıldığımız görüşe göre kalma için yeterli sürenin belirlenmesinde, failin girmesinin hukuka aykırı olduğu bir sisteme girdiğini fark etmesi ve bu ihlal hareketini sonlandırması için yeterli sürede sistemden çıkıp çıkmadığı esas alınmalıdır. Fail sistemden ayrılabilmesi için yeterli sürede sistemden çıkmamışsa artık kalma seçimlik hareketi bakımından TCK 243. maddesi gerçekleşmiş sayılmalıdır.²⁵⁴

b. MANEVİ UNSUR

TCK 21. maddesine göre kast “*suçun kanuni tanımındaki unsurlarının bilerek ve istenerek gerçekleştirilmesidir.*” Bilişim sistemine girme suçu, kasten işlenebilen bir suçtur; suçun özel bir saikle işlenmesi aranmadığından genel kastla işlenebilir.²⁵⁵ Dolayısıyla amacı gözetilmeksizin kasten sisteme giren ya da sistemde kalan kişi bu suçun faili olacaktır.²⁵⁶ Failin kastı, bilişim sisteminin üzerinde başkasının hak sahibi olduğunu ve bu sisteminin bir kısmına veya tamamına izinsiz girdiğini bilmesini ve istemesini kapsamalıdır.²⁵⁷ Failin bilişim sistemindeki verileri öğrenme, elde etme, verilere müdahale etme veya sisteme müdahale etme, kendisine ya da başkasına haksız

²⁵² Tezcan/ Erdem/ Önok, s. 1159.

²⁵³ Aksi görüşe göre bilişim sisteminde ne kadar süre kalındığı önemli değildir. Önemli olan kişinin sistemde hukuka aykırı olarak kaldığını bilmesi ve buna rağmen kalmaya devam etmesidir. Sistemde ne kadar süre kalındığıysa cezanın belirlenmesinde dikkate alınmalıdır. Özbek/ Doğan/ Bacaksız, s. 961.

²⁵⁴ Yaşar/ Gökcan/ Artuç, s. 7293; Mahmutoğlu, s. 861.

²⁵⁵ Tezcan/ Erdem/ Önok, s. 1155; Özbek/ Doğan/ Bacaksız, s. 964; Koca/ Üzülmmez, s. 902; Parlar, s. 17; Taşkın, s. 28; Kurt, s. 159; Karagülmez, s. 186; Soyaslan, s. 695.

²⁵⁶ Karakehya, s. 15; Parlar/ Hatipoğlu, s. 3469.

²⁵⁷ Yaşar/ Gökcan/ Artuç, s. 7294; Erdoğan, s. 156.

çıkar sağlama, eğlenme, merak giderme amaçlarıyla hareket etmesi önemli olmaksızın; TCK 243. maddesindeki suç oluşacaktır.²⁵⁸

Taksirli sorumluluk istisnai olduğundan, suçun taksirli hali kanunda öngörülmemişse cezalandırılmayacaktır.²⁵⁹ Bilişim sistemine girme suçunun, taksirle işlenebileceği kanunda öngörülmediğinden taksirle bu suç işlenemez.²⁶⁰ Yani bir kimse dikkat ve özen yükümlülüğüne aykırı davranarak bir bilişim sistemine girerse veya hukuka uygun olarak girdiği sistemde kalmaya devam ederse bu suç oluşmayacaktır. Ancak kişi girmemesi veya kalmaması gereken sisteme girdiğini veya sistemde kaldığını fark ettiği an sistemden çıkmazsa sistemde kalma seçimlik hareketi bakımından suç gerçekleşmiş olacaktır.²⁶¹

Doktrinde bir yazar, bilişim sistemine girme suçunun olası kastla da işlenebileceğini ileri sürmüştür.²⁶² Ancak “*hukuka aykırı olarak*” ifadesi suçun kanuni tanımında geçtiğinden bu suç ancak doğrudan kastla işlenebilir.²⁶³

TCK 243/3. maddesinde suçun neticesi sebebiyle ağırlaşmış hali öngörülmüştür. Buna göre failin bilişim sistemine girme veya sistemde kalma fiili “*nedeniyle sistemin içerdiği veriler yok olur veya değişirse*” daha ağır cezaya hükmedilir. TCK 23. maddesi gereği failin ağır neticeden “*sorumlu tutulabilmesi için bu netice bakımından en azından taksirle hareket etmesi gerekir*”. Yani failin kastı sisteme girmeye veya sistemde kalmaya yönelik olmalı ancak bu fiil neticesinde verilerin yok olması veya değişmesi bakımından

²⁵⁸ Failin amacı sadece sisteme girmek de olabilir. Burada önemli olan amaç değil; amaçtan bağımsız olarak bilişim sistemine girme veya kalma hareketlerinin işlenmiş olmasıdır. Parlar, s. 16.

²⁵⁹ Hafizoğulları/ Özen, Genel Hükümler, s. 263.

²⁶⁰ Özbek/ Doğan/ Bacaksız, s. 964; Koca/ Üzülmmez, s. 902; Taşkın, s. 28; Kurt, s. 159; Ekici Şahin/ Koruculu, s. 608; Karagülmez, s. 186; Parlar/ Hatipoğlu, s. 3470; Tezcan/ Erdem/ Önok, s. 1155.

²⁶¹ Meran, s. 567.

²⁶² Özbek/ Doğan/ Bacaksız, s. 964; Yaşar/ Gökcan/ Artuç, s. 7295; Tezcan/ Erdem/ Önok, s. 1156; Mahmutoğlu, s. 862.

²⁶³ Koca/ Üzülmmez, s. 903; Meran s. 567; Ekici Şahin/ Koruculu, s. 608.

failin kastının söz konusu olmaması gerekir. Failin kastını aşan ya da kastından farklı netice bakımından sorumlu olması için en azından taksirinin olması gerekir.²⁶⁴

TCK 244/2. maddesinde bilişim sistemindeki “*verileri yok etme veya değiştirme*” fiilleri suç haline getirilmiştir. Dikkat edildiğinde burada sayılan hareketler TCK 243/3. maddesinde, neticesi sebebiyle ağırlaşmış suç olarak düzenlenmiştir. Ancak bu iki madde arasında manevi unsur yönünden fark vardır. Failin kastı sadece sisteme girmeye veya kalmaya yönelik değil de doğrudan sistemdeki verileri yok etme veya değiştirmeye yönelikse TCK 243/3. maddesi değil; TCK 244/2. maddesi gerçekleşmiş olacaktır.²⁶⁵ Nitekim neticesi sebebiyle ağırlaşmış suçtan sorumluluk için failin kasten hareket etmemiş olması gerekir. Aksi halde fail neticesi sebebiyle ağırlaşan suçtan değil; gerçekleştirdiği ihlalden sorumlu olur.²⁶⁶

c. HUKUKA AYKIRILIK

Suç ceza hukuku normuyla çatışan, normu ihlal eden fiildir. İhlalsiz suç olmaz ilkesi gereğince fiilin hukuka aykırı olması gerekir.²⁶⁷ Fiilin kanuni tipe uygun olması durumunda, fiil karine olarak hukuka aykırıdır. Ancak bu karine, fiili hukuka uygun hale getiren sebeplerin gerçekleşmesi halinde çürütülmekte ve fiil suç olmaktan, hukuk düzeniyle çatışma halinde olmaktan çıkmaktadır. Kanuni tipe uygun fiili, suç olmaktan çıkaran sebeplere hukuka uygunluk sebepleri denilmektedir.²⁶⁸ Hukuka aykırılığı tespit ederken de kanuni tipe uygun fiil bakımından hukuka uygunluk sebeplerinin olayda bulunup bulunmadığına göre belirleme yapılır. Fiil bakımından herhangi bir hukuka uygunluk nedeninin olayda gerçekleşmemesi durumunda fiil suç teşkil etmektedir. Yani

²⁶⁴ Doktrindeki bir görüşe göre, TCK 243/3. maddesinde suçun taksirle işlenebileceği açıkça öngörülmediğinden, bu fıkra bakımından da fiil kastla veya olası kastla işlenebilecek ancak taksirle işlenemeyecektir. Özbek/ Doğan/ Bacaksız, s. 965.

²⁶⁵ Tezcan/ Erdem/ Önok, s. 1156; Kurt, s. 159.

²⁶⁶ Tezcan/Erdem/Önok, s. 1155.

²⁶⁷ Hafızoğulları/ Özen: Genel Hükümler, s. 193.

²⁶⁸ Koca/ Üzülmüş: Genel Hükümler, s. 265.

bir fiilin hukuka aykırı olarak nitelendirilebilmesi için fiilin tipik olması ve hukuka uygunluk sebeplerinin bulunmaması gerekir.²⁶⁹

TCK 24. maddesinde düzenlenen kanun hükmü ve yetkili amirin emrinin icrası, TCK 25. maddesinde düzenlenen meşru müdafaa²⁷⁰ ve TCK 26. maddesinde düzenlenen ilgilini rızası bu suç açısından geçerli hukuka uygunluk nedenlerindendir.²⁷¹ Yani bilişim sistemine girilmesi veya sistemde kalınması kanun hükmünün veya amirin emrinin icrası çerçevesinde ya da ilgili kimsenin rızasına dayalı gerçekleştiriyorsa ortada suç teşkil eden bir fiil söz konusu değildir.

Kanun hükmünün icrası dolayısıyla suç teşkil etmeyen bilişim sistemine girme veya sistemde kalma örneği olarak CMK 134. (“*Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma*”) ve 135. (“*İletişimin tespiti, dinlenmesi ve kayda alınması*”) maddeleri gösterilebilir. CMK 134, 135. maddeleri gereği sisteme girilmesi veya sistemde kalınması suç değildir.²⁷²

Çalışanlarına, kurumlarca belirli bir amaçta kullanılması için sağlanmış bilişim sistemlerinin amaca uygun kullanılıp kullanılmadığının denetlenmesi için sistemlere girilmesi veya sistemde kalınması hukuka uygunluk nedeni sayılmalıdır.²⁷³ Kamu görevlilerine tahsis edilen bilişim sistemleri kişisel amaçlarla kullanılamayacağından ve bu sistemlerde kişisel veriler bulunamayacağından, kamu görevlisinin rızası

²⁶⁹ Özen/ Hafizoğulları: Genel Hükümler, s. 195.

²⁷⁰ Ekici Şahin/Koruculu, s. 610.

²⁷¹ Koca/ Üzülmmez, s. 903; Parlar, s. 18; Taşkın, s. 27; Yaşar/ Gökcan/ Artuç, s. 7295; Parlar/ Hatipoğlu, s. 3470; Tezcan/ Erdem/ Önok, s. 1156.

²⁷² Parlar, s. 18.

²⁷³ Ekici Şahin/ Koruculu s. 610; Yaşar/ Gökcan/Artuç, s. 7295. Aksi görüş için bkz. yazarlar kişinin hem özel yaşamının hem de haberleşme özgürlüğünün korunduğu bu alana müdahale için kanuni bir hükmün bulunması gerekliliğinden bu görüşe mutlak bir şekilde katılmamaktadır. “İşveren tarafından denetim yapılabileceğine dair açık bir düzenlenmenin bulunması ve çalışanın bu düzenlemeler hususunda açıkça bilgilendirilmiş olması ön koşullarına bağla olarak işveren tarafından çalışanların kullandığı kuruma ait bilişim sistemlerinin incelenmesi mümkündür”, Tezcan/ Erdem/ Önok, s. 1158.

aranmaksızın yetkili amir veya onun yetkilendirdiği kimsenin sisteme denetim amacıyla girmesi hukuka uygundur.²⁷⁴

Doktrinde bir görüş, TCK'nın sistematüğini göz önünde bulundurarak bilişim sistemine girme suçunun “*Topluma Karşı Suçlar*” bölümünde düzenlenmesi ve kanun koyucunun burada toplumsal bir menfaate öncelik verdiği düşüncesinden hareketle ilgilinin rızası hukuka uygunluk nedeninin bilişim alanında suçlar açısından geçerli olmadığını savunmaktadır. Ancak bu görüşe katılmak mümkün değildir. İlgilinin bilişim sistemi üzerindeki hakkı mutlak surette tasarrufta bulunabileceği bir hak olduğundan rıza bu suç bakımından hukuka uygunluk sebebi sayılmazdır.²⁷⁵ TCK'nın sistematüğinden hareketle yapılan yorumlar, suçların hukuki konusunu ve buradan hareketle mağdurun ve suçun unsurlarının belirlenmesinde yol gösterici olsa da kanunun sistematüğü sadece bir yorum aracıdır. Bilişim alanında suçların, “*Topluma Karşı Suçlar*” bölümünde düzenlenmesi bu suçlar açısından kanun koyucunun kamu menfaatini de ön plana çıkarmaya çalışılıyor şeklinde yorumlanmaya müsait olduğundan bu suçlar açısından bilhassa kişilerin mutlak surette üzerinde tasarrufta bulunabileceği haklarına ilişkin rıza gösteremeyeceğini söylemek hukuk pratiğiyle bağdaşmayacaktır. Zira bu yorum bir bilgisayar sahibinin arkadaşına bilgisayarını kullanma konusunda rıza açıklayamayacağı gibi mantıksız bir sonuca ulaştıracaktır.

Bu açıklamalar çerçevesinde ilgilinin rızası (TCK 26/2) bu suçla bağdaşan bir diğer hukuka uygunluk nedenidir. Burada kişinin bilişim sistemi üzerindeki hakkı üzerinde mutlak surette tasarruf edebileceği bir hak olduğundan, sisteme başkasının girmesi veya kalması için göstermiş olduğu rıza fiili hukuka uygun kılacaktır. Rızayı göstermesi gereken kimse, tipik fiille ihlal edilen hukuki konunun sahibidir.²⁷⁶ Bu suçla

²⁷⁴ Erdoğan, s. 161.

²⁷⁵ Erdoğan, s. 109-110.

²⁷⁶ Artuk/ Gökçen, s. 550.

korunmak istenen değer sistemin güvenliği olduğundan, sistemde her ne kadar başkalarına ait veriler bulunsada bu suçun mağduru sistem üzerinde hak sahibi kişi veya kişilerdir. Dolayısıyla rızayı göstermesi gereken kişi sistem üzerinde hak sahibi olan yani sisteme girme yetkisini haiz kimsedir.²⁷⁷ Bir bilişim sistemindeki güvenlik zafiyetlerini ortaya çıkarmak üzere anlaşılmış kimsenin, sisteme girme eylemi hukuka uygundur zira görevi gereği kendisine gösterilen rıza kapsamında bu eylemi gerçekleştirmiştir.²⁷⁸

Bilişim sistemini kullanma yetkisinin başkasına devredildiği durumlarda, sisteme girme açısından rıza göstermeye yetkili kişinin tespit edilmesi TCK 243. maddesinin ihlal edilip edilmediğinin tespiti bakımından önemlidir. Doktrinde bir görüşe göre sistemi kullanma yetkisinin başkasına verildiği durumlarda, bu yetkinin verildiği kişiler rıza göstermeye yetkili değildir. Nitekim bilişim sistemini kullanma hakkı olan kişinin sistem üzerinde tasarruf yetkisi kısıtlı olduğundan, onun rızası geçerli bir rıza olmayacaktır. Örneğin bir banka çalışanına banka bilişim sistemlerini kullanma yetkisinin ve şifrelerin verilmesi banka personelinin bu şifreyi başkalarına verme yetkisi vermediğinden bu şifreyi kullanarak sisteme giren kimse TCK 243. maddesinden sorumlu olacaktır.²⁷⁹ Ancak böyle bir tespitin, bizi her zaman doğru sonuçlara götürmeyeceği kanaatindeyiz. Zira bilişim sisteminin kullanımının devredildiği bazı durumlarda bilişim sistemi üzerinde kullanım hakkına sahip olan kimse, başkasının bu sistemi kullanması konusunda rıza gösterme yetkisini haiz olabilir. Kısacası burada rızayı göstermeye ehil olan kimsenin, hukuki ilişkiye göre tespit edilmesi gerektiği kanaatindeyiz.

Rızanın dayandığı iradenin hata, hile, cebir gibi sebeplerle sakatlanmamış olması, özgür bir iradeye dayanması gerekir.²⁸⁰ Rıza tipik fiilin işlenmesinden önce veya en geç

²⁷⁷ Tezcan/ Erdem/ Önok, s. 1159; Bir kamu kuruluşunda çalışan memurun göreviyle bağlantılı olarak kendisine verilen bilişim sistemine giriş şifresini başkasına vermesi durumunda rızadan bahsedilemez. Zira memur sisteme girme hak ve yetkisini başkasına devredemeyecektir. Kurt, s. 157.

²⁷⁸ Taşkın, s. 336.

²⁷⁹ Yaşar/ Gökcan/ Artuç, s. 7296.

²⁸⁰ Kurt, s. 157; Ekici Şahin/ Koruculu, s. 611; Erdoğan, s. 159.

işlenirken verilmelidir. Aksi halde tipik fiil gerçekleştirdikten sonra verilen rıza geçerli bir rıza olmadığından fiili hukuka uygun hale getirmez.²⁸¹ Doktrinde bir görüşe göre izin almaksızın girdiği sistemde kalmaya devam ederken, sistem sahibi tarafından sistemde kalmasına rıza gösterilen kimse açısından fiil hukuka uygundu. Çünkü suç mütemadi bir suç olduğundan ve kalma hareketi kesilmeden, henüz suç tamamlanmadan verilen rıza fiili hukuk uygun hale getirecektir.²⁸² Ancak sonradan gösterilen rıza işlenen fiili hukuka uygun hale getirmez.²⁸³ Rıza örtülü veya açık olarak verilebilir.²⁸⁴ Herkesin kullanımına açık bilişim sistemlerine girme durumunda bu suç oluşmayacaktır.²⁸⁵ Ancak bir bilişim sisteminin saldırılara karşı korunması için sistemde herhangi güvenlik mekanizmasının örneğin şifrenin bulunmaması örtülü rıza olarak değerlendirilmemelidir.²⁸⁶ Güvenlik önlemlerinin alınmadığı bir bilişim sistemine hukuka aykırı girişi ispatlamak sorun yaratacağından Alman Ceza Kanununda olduğu gibi “yetkisiz girişlere karşı özellikle korunmuş olma” şartının suçun oluşumu açısından aranması gerekir.²⁸⁷

Sistem üzerinde hak sahibi kimsenin başlangıçta açıkladığı rızayı geri alması durumunda sistemde kalmaya devam edilmesi²⁸⁸ veya bilişim sistemine bir kereye mahsus girilmesi için açıklanmış şifrenin daha sonra tekrar kullanılması²⁸⁹ durumlarında ilgilinin rızası söz konusu olmadığından hukuka uygunluk sebebinden bahsedilemez.

²⁸¹ Hafizoğulları/ Özen, Genel Hükümler, s. 228.

²⁸² Özbek/ Doğan/ Bacaksız, s. 964; Erdoğan, s. 1409.

²⁸³ Hafizoğulları/ Özen, s. 448.

²⁸⁴ Artuk/ Gökçen, s. 558.

²⁸⁵ Koca/Üzülmez, s. 903.

²⁸⁶ Tezcan/ Erdem/ Önok, s. 1158; Yaşar/ Gökcan/ Artuç, s. 7296; Erdoğan, s. 160.

²⁸⁷ Soyaslan, s. 695.

²⁸⁸ Parlar, s. 18. Benzer yönde Yargıtay kararı için bkz. “Müşteki Sibel ile birlikte olduğu dönemde müştekinin rızasıyla kendi facebook şifresini verdiğini beyan ettiği dikkate alındığında, sanığın, müştekiye ait facebook giriş şifresini hukuka aykırı olarak ele geçirdiğine dair hiçbir delil bulunmadığı gibi, müşteki Sibel'in bu yönde bir iddiasının da bulunmadığı anlaşılmakla, sanığın, müşteki Sibel'in bilgisi ve rızası dışında müştekiye ait facebook sayfasına girme eyleminin, TCK'nın 136.maddesinde düzenlenen verileri hukuka aykırı olarak verme veya ele geçirme suçunu değil, TCK'nın 243/1.maddesinde düzenlenen bilişim sistemine girme suçunu oluşturduğu göz önünde bulundurularak bu suçtan ceza verilmesi gerektiği gözetilmeden suçun vafında yanılğıya düşülerek yazılı şekilde hüküm kurulması” dolayısıyla hüküm bozulmuştur. Yargıtay 12. CD. E. 2015/2309 K. 2015/15364 T. 14.10.2015

²⁸⁹ YARGITAY 12. CD E. 2015/2309 K. 2015/ 15364 KT. 14.10.2015 Tezcan/ Erdem/ Önok, s. 1159.

Aynı şekilde bilişim sisteminin şifresinin paylaşıldığı kişi bu şifreyi üçüncü bir kimseyle paylaşırsa, üçüncü kişinin sisteme girmesi ilgilinin rızası söz konusu olmadığından TCK 243. maddesindeki suç oluşturacaktır.²⁹⁰ Ayrıca verilen rızanın sınırlarının aşılaraq bilişim sistemine girilmesi veya sistemde kalınması durumunda da TCK 243. maddesindeki suç oluşmaktadır. Örneğin bilişim sisteminin bir kısmına girilmesi için açıklanmış rızada, sistemin izin verilemeyen bölümlerine girilmesi durumunda rızanın sınırı aşıldığından bilişim sistemine girme suçu oluşmuştur.

Şüpheli/sanık rızaya dayalı sisteme girdiğini iddia ediyor ancak müşteki rıza olmadığını söylüyorsa, şüpheli/sanık bilişim sistemine rızaya dayalı girildiğini ispatlamalıdır.²⁹¹

Bu suçla bağdaşan bir diğer hukuka uygunluk nedeni meşru müdafaadır. Meşru müdafaada kişi, kendisine veya bir başkasına yönelen haksız bir saldırıyı defetmek amacıyla saldırıyla orantılı, kanuni tipe uygun bir fiili gerçekleştirmektedir.²⁹² Ancak bu tipik fiili kendisine veya başkasına ait bir hakkı korumak için işlediğinden, kanundaki diğer şartların da gerçekleşmesi halinde fiili suç teşkil etmemektedir.²⁹³ Bilişim sistemine girme fiilinin meşru müdafaada durumunda işlenmesi halinde, bu fiil suç teşkil etmeyecektir. Örneğin sosyal medya hesabından başkasının uygun olmayan görüntülerini izinsiz paylaşan ve uyarılmasına rağmen hesabından söz konusu fotoğrafları kaldırmayan kimsenin bilişim sistemine, şifresi kırılarak girilmesi ve fotoğrafların silinmesi durumu meşru müdafaada kapsamında değerlendirilebilir.²⁹⁴ Bu örnekte mevcut haksız saldırıyı defetmek amacıyla saldırıyla orantılı savunma fiilinin icra edilmesi kaçınılmaz niteliktedir. Zira savunmanın kaçınılmaz olup olmadığının belirlenmesi konusunda, suç

²⁹⁰ Tezcan/ Erdem/ Önok, s. 1159; Ekici Şahin/ Koruculu, s. 612.

²⁹¹ Kurt, s. 157; Zira bilişim sistemine başkası tarafından girilmesi hayatın olağan akışına uygun olmadığından şüpheli/sanık bunun ispatlamalıdır. Parlar/ Hatipoğlu, s. 3470; Erdoğan, s.159.

²⁹² Dönmezer/ Erman, s. 333.

²⁹³ Koca/ Üzülmüş, Genel Hükümler, s. 278.

²⁹⁴ Ekici Şahin/Koruculu, s. 610.

soruşturmak ve kovuşturmakla görevli mercilere başvurulması düşünülebilirse de devam eden bir saldırıda böyle bir yolun izlenmesi çok uzun süreceğinden meşru müdafaanın şartlarının gerçekleştiği kabul edilmelidir. Ancak savunmayı gerçekleştiren kimsenin, fotoğrafları silmesinin yanında diğer verilere veya sisteme zarar vermesi durumunda ya da sistemden fotoğrafları silmesine rağmen sistemde kalmaya devam etmesi durumunda artık meşru müdafaada sınırın kasten aşılması söz konusudur. Bu halde sisteme meşru müdafa kapsamında giren kimsenin, meşru müdafaada sınırı aşması dolayısıyla gerçekleştirdiği suçtan kasten sorumluluğu doğacaktır.²⁹⁵

F. SUÇA ETKİ EDEN HALLER

a. DAHA AZ CEZAYI GEREKTİREN HAL

Suçun varlığını etkilemeyip, suç karşılığı öngörülen cezanın ağırlığını etkileyen haller suça etki eden hallerdir.²⁹⁶ TCK 243/2. maddesinde cezayı hafifletici bir nitelikli hal öngörülmüştür. Fıkra göre “*fiillerin bedeli karşılığı yararlanılabilen sistemler hakkında işlenmesi halinde, verilecek ceza yarı oranına kadar indirilir.*” Bu nitelikli halin uygulanabilmesi için bedel karşılığı yararlanılabilen bir sistemin bulunması ve failin bu sisteme bedel ödemeksizin girmesi gerekir.

Cezayı hafifletici bu neden doktrini ikiye bölmüş ve bazı yazarlar “*bilişim sistemine girme veya sistemde kalma*” hareketlerinin bedeli karşılığı yararlanılabilen bir sisteme karşı işlenmesinin daha fazla cezayı gerektirdiğini savunmuştur.²⁹⁷ Bu görüşe göre sisteme girme ya da sistemde kalma hareketleri, bedeli karşılığı yararlanılabilen bir sisteme karşı işlendiğinde hem sistemin güvenliği hem de sistem üzerinde hak sahibi kimsenin ekonomik menfaatleri ihlal edilecektir.²⁹⁸ Aksi görüşü savunanlara, yani

²⁹⁵ Ekici Şahin/ Koruculu, s. 610.

²⁹⁶ Yalçın/ Köprülü, s. 387.

²⁹⁷ Tezcan/ Erdem/ Önok, s. 1155; Özbek/ Doğan/ Bacaksız, s. 963; Taşkın, s. 36; Erdoğan, s. 151.

²⁹⁸ Özbek/ Doğan/ Bacaksız, s. 963; Taşkın, s. 36.

maddenin kaleme alınış şeklini doğru bulan yazarlara göre bedeli karşılığı başkalarının kullanımına açılan bilişim sistemlerine girme veya kalma hareketleriyle; hiçbir şekilde başkasının kullanımına açılmamış bilişim sistemlerine girme veya kalma hareketleriyle ihlal edilen hukuki değerler aynı değildir.²⁹⁹ Çünkü bedel karşılığı yararlanılabilen bir sistemde korunmaya çalışılan hukuki değerde mahremiyetten ziyade “ekonomik menfaat” öne çıkarılmaktadır. Dolayısıyla bedel ödenerek yararlanılan bir sisteme girilmesi fiilinin haksızlık içeriği daha az bulunduğundan bu düzenleme yerindedir.³⁰⁰

Kanaatimizce bir sistem bedeli karşılığında başkasının kullanımına açılsın ya da açılmasın, her sistemin güvenliği ve mahremiyeti aynı derecede önemlidir. Bedeli karşılığı yararlanılabilen bir sistem söz konusu olduğunda, sunulan bir hizmet söz konusu olduğundan bu hizmetten bedeli ödenmeksizin faydalanılması hem sistem güvenliğine ilişkin menfaati hem de sistem sahiplerinin ekonomik menfaatini zedelemektedir. Bu sebeple söz konusu sebebin hafifletici değil ağırlaştırıcı neden olması düşüncesini paylaşmaktayız.

Doktrinde bir görüş, ikinci fıkranın bilişim sistemine girme suçu altında değil; karşılıksız yararlanma suçu altında değerlendirilmesinin daha isabetli bir düzenleme olacağını ileri sürmüştür.³⁰¹ Ancak TCK 243. maddesinin ikinci fıkrasından sorumluluğun doğması için, bilişim sistemine girme zorunlu olarak sistemin sunduğu hizmetten yararlanılmasını içermemektedir. TCK 163. maddesindeyse yaptırıma bağlanmaya çalışılan tipik hareket, bedel ödenmeksizin bir hizmetten faydalanılmasıdır. Dolayısıyla karşılıksız yararlanma suçunda bedel ödenmeksizin hizmetten faydalanma tipik hareketken; bilişim sistemine girme suçunda hizmetten faydalanılıp faydalanılmadığı önemsenmeksizin bedel ödenmeden sisteme girilmesi tipik harekettir.

²⁹⁹ Mahmutoglu, s. 863; Ekici Şahin/ Koruculu, s. 615; Yazıcıoğlu, s. 406-407.

³⁰⁰ Koca/ Üzülmüş, s. 904; Karagülmez, s. 189.

³⁰¹ Ekici Şahin/ Koruculu, s. 616.

Bu sebeple bedel karşılığı faydalanılan bir bilişim sistemine girme hareketine TCK 243. maddesi altında yer verilmesi bize göre isabetli olan düzenlemedir.

Bedeli karşılığı yararlanılabilen sistemden ne anlaşılması gerektiği ne kanun metninde ne de gerekçede ifade edilmiştir. Dolayısıyla ifadenin anlamı ve kapsamı oldukça muğlak³⁰² ayrıca geniş yorumlanmaya müsaittir.³⁰³ Bedeli karşılığında yararlanılan bilişim sistemlerinden, sistemle sunulan hizmetin herkesin kullanımına açık olmadığı ancak öngörülen bedelin ödenmesi durumunda insanların faydalanabildiği sistemler anlaşılmalıdır. Örneğin dijital kütüphaneler, içtihat bilgi bankaları, elektronik dergi ve gazeteler.³⁰⁴

İkinci fıkrada geçen bedel kavramı dar yorumlanarak, sadece para şeklinde anlaşılmalıdır.³⁰⁵ Sistemden faydalanılması için verilen her türlü karşılık bedeldir.³⁰⁶ Bu bedel para gibi maddi bir değer olabileceği gibi başka şeyler örneğin siteye belli sayıda kimsenin abone edilmesi bedel olarak kararlaştırılabilir.³⁰⁷

Bedeli karşılığında yararlanılabilecek sistemlerle kastedilen internet kafe³⁰⁸ gibi bir mekân içindeki bilişim sistemlerinden kullanılan süre için ücreti karşılığı faydalanılması veya internet bağlantı servisinin sağlanması³⁰⁹ değil de ancak ücreti karşılığında bilişim sistemi aracılığıyla sunulan bir hizmetin olmasıdır.³¹⁰ TCK'daki diğer şartların gerçekleşmesi halinde, internet kafedeki ya da internet bağlantı servisi sağlayan

³⁰² Hafizoğulları/ Özen, s. 449.

³⁰³ Ketizmen, s. 110.

³⁰⁴ Parlar, s. 19.

³⁰⁵ Karagülmez, s. 188

³⁰⁶ Koca/ Üzülmüş, s. 904; Çetin, s. 8.

³⁰⁷ Parlar, s. 19.

³⁰⁸ İnternet kafelerin bu fıkraya girdiğini savunan görüş için bkz. Yaşar/ Gökcan/ Artuç, s. 7299.

³⁰⁹ İnternet bağlantı servisinin sağlanması da bedeli karşılığında yararlanılan bilişim sistemi ifadesine dahil değildir. Karagülmez, s. 188; Parlar/ Hatipoğlu, s. 3472. Aksi görüş için bkz. Yaşar/ Gökcan/ Artuç, s. 7299.

³¹⁰ Tezcan/ Erdem/ Önok, s. 1154-1155; Özbek/ Doğan/ Bacaksız, s. 963; Parlar, s. 19; Karagülmez, s. 188; Parlar/ Hatipoğlu, s. 3472.

sistemlerden bedel ödenmeksizin yararlanılması durumunda karşılıksız yararlanma suçundan (TCK 163/2) hüküm kurulacaktır.³¹¹

Doktrinde TCK 243/2. maddesinin TCK 163. maddesi (karşılıksız yararlanma suçu) ile karıştırılabileceği ifade edilmiştir.³¹² Ancak TCK 163. maddede sayılan unsurlar³¹³ bilişim sistemi olmadığında zaten 243/2. maddesinde düzenlenen suça vücut vermezler. Otomatların bilişim sistemi olduğu durumlarda bu sisteme girilerek sistemden bedel ödenmeksizin faydalanılması durumunda TCK 163. maddesi gereğince “*otomatlar aracılığı ile sunulan ve bedeli ödendiği takdirde yararlanılabilen bir hizmetten ödeme yapmadan*” yararlanma karşılıksız yararlanma suçuna vücut vereceğinden otomatlar bilişim sistemi olsa da 243. maddenin uygulama alanına girmemektedir.³¹⁴ Otomatlar aracılığıyla sunulan bir hizmetten bedeli ödenmeksizin yararlanılması TCK 243. maddesi kapsamına değil TCK 163 (karşılıksız yararlanma) kapsamına girmektedir, zira 163. madde özel olarak otomatlar için öngörülmüştür.³¹⁵ Ayrıca TCK 163. maddesinde bedel ödenmeksizin otomatlar aracılığıyla sunulan hizmetten faydalanılması ceza yaptırımına bağlanmışken; TCK 243. maddesinin ikinci fıkrasında bedel ödenerek faydalanılan bir bilişim sistemine bu bedel ödenmeksizin girme hareketi başlı başına ceza yaptırımına bağlanmıştır.

TCK 243. maddesinde kamu kurumlarıyla özel hukuk tüzel kişilerinin bilişim sistemlerine girilmesi veya sistemlerinde kalınması hareketleri, cezayı ağırlaştırıcı nitelikli hal olarak öngörülmemiştir. Bu kurumlara karşı gerçekleştirilen haksız fiillerin ortaya çıkardığı zarar veya zarar tehlikesi, kişisel bilişim sistemlerine girilmesi durumunda ortaya çıkan tehlikeye nazaran çok daha büyük olduğundan böyle bir cezayı

³¹¹ Erdoğan, s. 149-150.

³¹² Hafizoğulları/ Özen, s. 449.

³¹³ Otomatlar; telefon hatları, frekanslar veya elektromanyetik dalgalarla yapılan şifreli veya şifresiz yayınlar.

³¹⁴ Karagülmez, s. 187.

³¹⁵ Parlar, s. 19; Soyaslan, s. 697.

ağırlaştırıcı nedene yer verilmesi isabetli bir düzenleme olacaktır.³¹⁶ Ayrıca doktrinde bir yazar, bilişim sistemine haksız bir şekilde erişilmesi sonucu sistemde oluşan bir açık dolayısıyla başkalarının sisteme girmesi veya sistemden veri elde etmesi durumunun suça etki eden hal olarak düzenlenmesi gerektiğini savunmaktadır.³¹⁷

b. NETİCESİ SEBEBİYLE AĞIRLAŞMIŞ HAL

Üçüncü fıkranın nitelikli hal mi neticesi sebebiyle ağırlaştırılmış suç mu olduğu hususunda doktrinde tartışma vardır. Bir görüş üçüncü fıkranın, ikinci fıkra gibi nitelikli hal olduğunu ileri sürmektedir.³¹⁸ Bu görüşe göre ikinci fıkra cezayı hafifletici nitelikli halken; üçüncü fıkra cezayı ağırlaştırıcı nitelikli haldir.³¹⁹ Diğer görüşse üçüncü fıkra düzenlenmiş durumun, suçun neticesi sebebiyle ağırlaştırılmış hali olduğunu ileri sürmektedir.³²⁰

Cezayı ağırlaştırıcı nitelikli haller bakımından failin sorumluluğunun doğması için failin kastının bu durumu da kapsamı gerekir.³²¹ Yani eğer fail olayda cezayı ağırlaştırıcı nitelikli halin var olduğunu bilmiyorsa, onu bilmediği ve istemediği bu nedenden sorumlu tutmak mümkün değildir. Neticesi sebebiyle ağırlaştırılmış suçta fail, fiiliyle kastettiğinden daha ağır veya başka bir neticenin meydana gelmesine sebep olmaktadır.³²² Burada tipik fiilin işlenmesi aslında daha ağır veya başka neticenin meydana gelme ihtimalini de bünyesinde taşır. Ancak fail gerçekleşen daha ağır veya başka netice bakımından kasten hareket etmemiştir.³²³

³¹⁶ Ketizmen, s. 110; Erdoğan, s. 151; Karagülmez, s. 206.

³¹⁷ Karagülmez, s. 207.

³¹⁸ Tezcan/ Erdem/ Önok, s. 1154; Kurt, s. 152.

³¹⁹ Karakehya, s. 204

³²⁰ Özbek/ Doğan/ Bacaksız, s. 959; Koca/ Üzülmüş, s. 895.

³²¹ Yalçın/ Köprülü, s. 389.

³²² Yazara göre başka netice ifadesi yanında daha ağır netice ifadesine yer verilmesi gereksizdir. Zira başka netice ifadesi, daha ağır netice ifadesini de içermektedir. Doğan, Koray: **Neticesi Sebebiyle Ağırlaştırılmış Suçlar**, Ankara, Adalet Yayınevi, 2015 s. 27.

³²³ Koca/ Üzülmüş, Genel Hükümler, s. 243.

TCK 243. maddesinin üçüncü fıkrasının lafzı incelendiğinde, verilerin yok olması veya değişmesi bakımından failin kastı aranmamış; failin sadece sisteme girme veya sistemde kalma amacıyla hareket etmesi aranmıştır. Ancak maddeye göre failin, sisteme girmek ve/veya sistemde kalmak isterken gerçekleştirdiği hareket neticesinde kastı olmaksızın veriler yok olmakta veya değişmektedir.³²⁴ Dolayısıyla TCK 243/3. maddesinde neticesi sebebiyle ağırlaşmış suç ihdas edilmiştir.³²⁵ Bu fıkradaki suç, gerçek neticesi sebebiyle ağırlaşmış suç niteliğinde olduğundan ağır neticeye sadece taksirle sebep olunabilir.³²⁶ Failin verilerin değişmesi ya da yok olması hususunda kastının söz konusu olduğu durumda, ileride anlatılacağı üzere TCK 244. maddesinde düzenlenen suç gerçekleşmiş olacaktır.³²⁷

Neticesi sebebiyle ağırlaşmış suçtan sorumluluk için failin sisteme girme veya sistemde kalma hareketiyle gerçekleşen ağır netice arasında nedensellik bağı olmalıdır.³²⁸ Nedensellik bağının kurulamadığı durumda fiil artık faile izafe edilemeyeceğinden fail birinci fıkradan sorumlu tutulacaktır.³²⁹

Üçüncü fıkradan sorumluluğun doğması için seçimlik sonuçlardan verinin yok olması veya değişmesinden birinin ya da her ikisinin gerçekleşmesi önem taşımaz. Ortada yine tek neticesi sebebiyle ağırlaşmış bilişim sistemine girme suçu olur ancak bu durum cezanın belirlenmesinde göz önünde bulundurulur.³³⁰

Verilerin yok edilmesi ve değişmesi hareketlerine bir sonraki bölümde yer verildiğinden burada ayrıca bir inceleme yapılmayacaktır. Ancak birkaç hususa değinilmesi gerekir. Verinin tamamen değişmesi veya yok edilmesi aranmaksızın kısmi

³²⁴ Madde gerekçesinde de hükmün uygulanabilmesi için failin verileri yok etmek veya değiştirmek kastıyla hareket etmemesi gerektiği ifade edilmiştir.

³²⁵ Koca/ Üzülmöz, s. 904; Meran, s. 566; Parlar, s. 19; Ekici Şahin/ Koruculu, s. 617; Ketizmen, s. 111; Karagülmez, s. 190; Soyaslan, s. 697.

³²⁶ Koca/ Üzülmöz, s. 905.

³²⁷ Meran, s. 566; Parlar, s. 19; Ketizmen, s. 111; Karagülmez, s. 191.

³²⁸ Hafizoğulları/ Özen, s. 450.

³²⁹ Yaşar/ Gökcan/ Artuç, s. 7297.

³³⁰ Karagülmez, s. 190-191; Yaşar/ Gökcan/ Artuç, s. 7298.

değişme veya yok etme durumunda da üçüncü fıkra uygulanacaktır.³³¹ Üçüncü fıkra metninde değişmesine veya yok edilmesine neden olunan verinin niteliği dikkate alınmadığından, değişen veya yok olan verilerin niteliği önemli değildir; veriler sistemde yer alan herhangi bir bilgi niteliğinde olabileceği gibi sistemin işleyişi için gerekli yazılımlar olabilecektir.³³² Değişen veya yok olan veriler bilişim sisteminin çalışması için gerekli bir veri niteliğindeyse, bu verinin silinmesi durumunda artık sistemin işleyişine müdahale söz konusudur ve eğer silinen veri olmaksızın sistem kendinden beklediği şekilde çalışmıyorsa sistemin işleyişinin bozulması ya da engellenmesi söz konusu olabilecektir. Ancak böyle bir ayrıma gidilmediğinden, veri önemsiz bir veri olsa dahi fail bu fıkradan sorumlu olacaktır.³³³

Üçüncü fıkra düzenlenen neticesi sebebiyle ağırlaşmış suç bakımından, veriler silinmeden veya yok edilmeden, sistem engellenir veya bozulursa sorumluluk doğmayacaktır. Mevcut düzenlemede sistem için önemsiz veriler yok olsa dahi daha ağır cezaya hükmedilebilecekken, sistemin işleyişinin engellenmesi veya bozulması durumunda böyle bir neticesi sebebiyle ağırlaşmış suça yer verilmemesi bir eksikliktir. Fransız Ceza Kanunu'ndaki benzer bir düzenlemeye yer verilerek bu fıkra *“bilişim sisteminin işleyişinin herhangi bir şekilde değişimine neden olunması”* eklenmelidir.³³⁴

TCK 243. maddesi bakımından hem cezayı hafifletici halin hem de neticesi sebebiyle ağırlaşmış halin aynı olayda gerçekleşmesi mümkündür. Doktrinde bir görüşe göre TCK 61/4. maddesi gereği faile verilecek cezanın belirlenmesinde önce üçüncü fıkra gereği ceza tespit edilip, daha sonraysa ikinci fıkra gereği indirim yapılır.³³⁵ Ancak TCK 61/4. maddesi neticesi sebebiyle ağırlaşmış suçlar için değil, suça etki eden sebepler için uygulama alanı bulur. Bizim de katıldığımız görüşe göre bedeli karşılığı yararlanılabilen

³³¹ Yaşar/ Gökcan/ Artuç, s. 7298.

³³² Tezcan/ Erdem/ Önok, s. 1154; Koca/ Üzülmüş, s. 905.

³³³ Yaşar/ Gökcan/ Artuç, s. 7298.

³³⁴ Karagülmez, s. 207.

³³⁵ Ekici Şahin/ Koruculu, s. 618; Yargıtay 8. CD uygulaması da bu yöndedir. Özsoy, s. 309.

sisteme girilmesi ya da sistemde kalınması durumunda sistemdeki veriler yok olur ya da değişirse yine TCK 243/3 hükmü uygulama alanı bulacaktır.³³⁶ Zira TCK 243/3. maddesinin uygulanması için birinci fıkra ve ikinci fıkraya ilişkin bir farklılık öngörülmemiştir.³³⁷ Başka bir ifadeyle girilen veya kalınan bilişim sisteminin bedeli karşılığı yararlanılabilen bir sistem olup olmadığı gözetilmeksizin “*bilişim sistemine girme veya sistemde kalma*” hareketleri neticesinde verilerin yok olması ya da değişmesi yeterli görülmektedir.³³⁸ Dolayısıyla yalnızca üçüncü fıkraya göre cezaya hükmedilecektir.³³⁹

G. SUÇUN ORTAYA ÇIKIŞ BİÇİMLERİ

a. TEŞEBBÜS

TCK 35. maddesine göre bir kimse “*işlemeyi kastettiği bir suçu elverişli hareketlerle doğrudan doğruya icraya başlayıp da elinde olmayan nedenlerle tamamlayamaz ise*” teşebbüsten sorumlu olacaktır. 6698 S KVKK ile 24.03.2016 tarihinde TCK 243. maddesinin ilk fıkrasına “ve” bağlacı yerine “veya” bağlacının getirilmesi konusunda yapılan değişiklik öncesi, doktrinde bazı yazarlar bu suçta teşebbüsün mümkün olmadığını savunmaktaydı.³⁴⁰ Bu görüşe göre değişiklik öncesi bu suç mütemadi bir suç olduğundan yani suçun işlenebilmesi için ihlalin belirli bir süre devam etmesi gerektiğinden, tek başına sisteme girme eylemi bu suçta teşebbüs sayılamazdı ve sistemde kalma hareketiyse parçalara ayıramayacağından bu suçta teşebbüs mümkün değildi.³⁴¹ Değişiklik öncesi bu suçta teşebbüsün mümkün olduğunu savunan bazı yazarlarsa, suçun çok hareketli bir suç olduğunu benimsemelerinden

³³⁶ Tezcan/ Erdem Önok, s. 1154.

³³⁷ Yazara göre burada fikri içtima kuralı uygulanmalıdır zira fail tek bir fiille kanunun farklı hükümlerini ihlal etmiştir. Dolayısıyla daha ağır ceza öngörülen üçüncü fıkra uygulama alanı bulur. Erdoğan, s. 172.

³³⁸ Koca/ Üzülmüş, s. 905.

³³⁹ Ketizmen, s. 111-112; Karagülmez, s. 191-193; Yaşar/ Gökcan/ Artuç, s. 7301; Hafizoğulları/ Özen, s. 449.

³⁴⁰ Taşkın, s. 30; Hafizoğulları/ Özen, s. 447.

³⁴¹ Ketizmen, s. 108.

hareketle suça teşebbüs için failin sisteme girmiş olmasını ve sistemde kalmak için en azından icra hareketlerine başlamış yani sistemde kalmaya başlanmış ancak suçun tamamlanması için yeterli sürenin geçmemiş olması gerektiğini savunmaktaydı.³⁴² Yani bu görüş, bu suça teşebbüs için bilişim sistemine girmeyi şart görmekteydi. Dolayısıyla sisteme girmeye çalışıldığı sırada elinde olmayan nedenlerle sisteme giremeyen failin, teşebbüsten sorumluluğunun doğmayacağını savunmaktaydılar.³⁴³ Bu suça teşebbüsün mümkün olduğunu savunan diğer görüş ise sisteme girmeyi şart koşturmaksızın, failin elinde olmayan nedenlerle icrasına başladığı sisteme girme fiilini tamamlayamaması durumunda suça teşebbüsten sorumluluğunun doğacağını kabul etmekteydi.³⁴⁴

2016’da yapılan değişiklik sonrası seçimlik hareketli bir suç haline getirilen TCK 243. maddesi neticesiz bir suç olduğundan, bu suça teşebbüs kural olarak söz konusu değildir. Suç girme hareketi bakımından sistemin bir kısmına veya tamamına girilmesiyle; kalma hareketi bakımındansa belirli bir süre sistemde kalınmasıyla tamamlanmakla birlikte failin sistemden çıkmasıyla son bulur.³⁴⁵ Ancak sisteme girme seçimlik hareketi bakımından, hareketin parçalara bölünebildiği hallerde bu suça teşebbüs mümkündür. Yani sistemin bir kısmına veya bütününe girmek için elverişli hareketlerle suçun icrasına doğrudan başlandığı ancak elde olmayan nedenlerle suçun tamamlanamadığı durumda TCK 243. maddesine teşebbüsten sorumluluk doğacaktır.³⁴⁶ Örneğin elektriğin kesilmesi, sistemin kitlenmesi gibi durumlarda fail icrasına doğrudan doğruya elverişli hareketlerle başladığı bilişim sistemine girme suçunu elinde olmayan nedenlerle tamamlayamadığından, teşebbüsten cezalandırılacaktır.³⁴⁷

³⁴² Erdoğan, s. 165.

³⁴³ Parlar, s. 18; Sisteme girdikten sonra sistemde anlık kalmayı dahi teşebbüs olarak nitelendirmemekte Karagülmez, s. 185; Yaşar/ Gökcan/ Artuç, s. 7300; Parlar/ Hatipoğlu, s. 3471.

³⁴⁴ Kurt, s. 263.

³⁴⁵ Tezcan/ Erdem/ Önok, s. 1159.

³⁴⁶ Koca/ Üzülmüş, s. 905.

³⁴⁷ Meran, s. 567.

Sistemde kalma seçimlik hareketi bakımından, sisteme hukuka uygun girilmesi ardından haksız bir şekilde belli bir süre sistemde bulunulması arandığından, kalma seçimlik hareketi açısından bu suça teşebbüs mümkün değildir.³⁴⁸ Nitekim kalma seçimlik hareketi bakımından bilişim sistemine girme suçu mütemadi suç niteliğindedir ve suçun tamamlanması için gerekli süre, failin sistemden çıkabileceği en kısa sürenin aşıldığı süredir.³⁴⁹ Yani kalma hareketi gerçekleştirilerek bilişim sistemine girme suçunun işlenebilmesi için gereken net bir sürenin ortaya konması mümkün olmadığından, başka bir deyişle sistemde kalmaya başlanmasıyla zaten suç gerçekleştiğinden bu hareket bakımından suça teşebbüs mümkün değildir.

TCK 243/3. maddesine yani bilişim sistemine girme ya da sistemde kalma neticesinde sistemdeki verilerin yok olması ya da değişmesi haline teşebbüs mümkün değildir.³⁵⁰ Zira teşebbüsten sorumluluğun doğması için kasten hareket etme aranırken; neticesi sebebiyle ağırlaştırılmış suçtan sorumluluk için failin netice bakımından kasten hareket etmemiş olması gerekir.³⁵¹

Failin, suçun icra hareketlerine başlayıp bilişim sistemine girmekten kendi isteğiyle vazgeçmesi durumunda gönüllü vazgeçme söz konusu olacak ve failin teşebbüsten sorumluluğu doğmayacaktır. Ancak o ana kadar gerçekleştirilen hareketler bir suç oluşturuyorsa, failin sorumluluğu sadece gerçekleşen suç bakımından doğacaktır. (TCK 36)

b. İŞTİRAK

“Tek bir kişi tarafından işlenebilecek bir suçun, birden çok kişi tarafından birlikte gerçekleştirilmesi haline suça iştirak” denmektedir.³⁵² Bilişim sistemine girme suçu,

³⁴⁸ Tezcan/ Erdem/ Önok, s. 1160; Özbek/ Doğan/ Bacaksız, s. 965.

³⁴⁹ Meran, s. 567.

³⁵⁰ Yaşar/ Gökcan/ Artuç, s. 7300; Aksi Görüş İçin bkz. Özbek/ Doğan/ Bacaksız, s. 965.

³⁵¹ Tezcan/ Erdem/ Önok, s. 1160.

³⁵² Yalçın/ Köprülü, s. 513.

iştirak açısından özellik arz etmemekte ve genel kurallar (TCK 37-41) bu suç için de geçerlidir.³⁵³

Bilişim sistemine girme seçimlik hareketi bakımından bu suç ani hareketli bir suç olduğundan, sisteme girilmesiyle suç tamamlanır ve suç tamamlandıktan sonra bu suçta iştirak mümkün değildir. Ancak sistemde kalma seçimlik hareketi bakımından bilişim sistemine girme suçu mütemadi bir suç olduğundan, suç bitene kadar azmettirme dışındaki iştirak türleriyle suça katılmak mümkündür.³⁵⁴

TCK 243. maddesini işleyen faile, TCK 245/A maddesinde sayılan şekilde yardım eden kimsenin durumunun özel olarak değerlendirilmesi gerekir. TCK 245/A maddesi gereği *“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”* cezalandırılacaktır. Bir kimsenin bilişim sistemine girme suçunu işlemesi için TCK 245/A maddesinde sayılan suçu işleyen kimse, iştirak iradesiyle hareket etmemişse sadece TCK 245/A maddesinden; iştirak iradesiyle hareket etmiş ve bilişim sistemine girme fiili üzerinde ortak hakimiyet kurmuşsa müşterek fail olarak hem TCK 243 hem TCK 245/A maddesinden sorumlu olacaktır. Eğer bu kişi bilişim sistemine girme suçu bakımından sadece iştirak iradesiyle hareket etmiş ve örneğin suçun işlenmesi için yardım eden sıfatıyla sisteme girme suçunu işleyecek faile bunun için bir program satmışsa, TCK 243 bakımından yardım eden, TCK 245/A maddesi bakımından fail konumundadır. Failliğin şerikliğe nazaran asliliği kuralı gereğince bu kimse sadece TCK 245/A maddesinden sorumlu olacaktır.

³⁵³ Koca/ Üzülmüş, s. 906; Taşkın, s. 30.

³⁵⁴ Yaşar/ Gökcan/ Artuç, s. 7300.

c. İÇTİMA

1. Genel Olarak

Bir kimsenin, ceza kanununun aynı veya farklı hükmünü; tek veya birden çok fiille birçok defa ihlal etmesi durumunda suçların içtimalı söz konusudur. Böyle bir durumda failin sorumluluğu tek bir suçtan ancak cezası ağırlaştırılarak belirlenecektir.³⁵⁵

Suçların içtimalı dışında, görünüşte birleşme denilen hallerde failin fiiline uygulanabilecek tek bir ceza normu vardır. Ancak bu hallerde adından da anlaşılacağı üzere fiil birden çok normu görünüşte ihlal etmektedir.³⁵⁶ Özel- genel norm, tüketen-tüketilen norm, asli-tali norm ilişkileri görünüşte birleşmenin örnekleridir.³⁵⁷

Doktrinde bir görüşe göre, TCK 243. maddesinde düzenlenen bilişim sistemine girme ya da sistemde kalma suçu genellikle başka suçların işlenmesi için geçilmesi gereken suçtur.³⁵⁸ TCK 244 (“*sistemi engelleme, bozma, verileri yok etme veya değiştirme*”), 134 (“*özel hayatın gizliliğini ihlal*”), 136 (“*kişisel verilerin hukuka aykırı olarak ele geçirilmesi*”), 132 (“*haberleşmenin gizliliğini ihlal*”). maddelerindeki suçların işlenebilmesi için öncelikle sisteme girilmesinin zorunlu olması dolayısıyla bu suçlar geçitli suçtur.³⁵⁹ Geçitli suç ilişkisi görünüşte birleşme örneği olarak asli-tali norm çerçevesinde değerlendirilebilir. Geçitli suçta “*failin bir suçu işleyebilmek için bu suçla aynı hukuki değeri koruyan daha hafif bir suçu işlemesi zorunludur*”.³⁶⁰ Geçitli suç ilişkisinin söz konusu olabilmesi için; her iki suçun koruduğu hukuki değer aynı olması,

³⁵⁵ Hafizoğulları/ Özen, Genel Hükümler, s. 354.

³⁵⁶ İçel, İctima, s. 36.

³⁵⁷ İçel, İctima, s. 39 vd.

³⁵⁸ TCK 244-245-132-134-135-136-142-158 suçları açısından TCK 243 geçilmesi gereken suç olduğundan, TCK 243 bu suçlar içinde erimektedir. Soyaslan, s. 696.

³⁵⁹ Yazar TCK 244, 245, 132, 133, 134, 135, 136, 142/2-e, 158/1-f suçları açısından TCK 243’ün geçit suç niteliği taşıdığını iddia etmektedir. PARLAR, s. 18; Yazara göre Bazı suçların işlenebilmesi için bilişim sistemine girme zorunluluk teşkil ediyorsa, TCK 243.maddesi bu suçlar açısından geçit suç niteliği gösterir. Örneğin TCK 244, 245, 142/2-e, 158/1-f suçlarında bilişim sistemine girme zorunluluk arz ediyorsa geçit suç ilişkisinden dolayı faille sadece ikinci suçtan dolayı ceza verilecek; ancak sisteme girildikten sonra bu suçlar gerçekleştiriliyorsa gerçek içtima kuralı gereği her iki suçtan ayrı ayrı cezalandırma yapılacaktır. Taşkın, s. 33-34.

³⁶⁰ İçel İctima, s. 46.

daha ağır suçun işlenmesi için geçilmesi gereken hafif suçun işlenmesinin zorunluluk arz etmesi, her iki suçun mağdur ve failinin aynı kişiler olması, sonuçların failin fiiline tek bir nedensellik bağıyla yüklenebilmesi ve son olarak failin kastının en baştan itibaren ağır suçu işlemeye yönelik olması gerekir.³⁶¹ Ancak sayılan hiçbir norm bakımından TCK 243. maddesi geçilmesi gereken suç değildir zira bu suçların hukuki konuları bilişim sistemine girme suçunun hukuki konusuyla aynı olmadığı gibi bu suçların işlenmesi için TCK 243. maddesinin ihlal edilmesi zorunluluk arz etmez.

Bu suçlarla TCK 243. maddesi arasındaki ilişki araç suç-amaç suç ilişkisi niteliğindedir. Bilişim sistemine girme suçu, başka suçların gerçekleştirilebilmesi için işlenebilmekte yani araç suç niteliği taşıyabilmektedir.³⁶² Araç suç-amaç suç bağlantısının varlığı halinde tipik hareketler örtüşmediği takdirde gerçek içtima kuralı gereği her bir suçtan ayrı ayrı ceza verilir; hareketlerin örtüştüğü durumundaysa fikri içtima kuralı uygulanır.³⁶³ Fail sisteme girme veya sistemde kalma hareketlerini başka suçları işlemek amacıyla gerçekleştirmişse, gerçek içtima kuralı gereği failin hem TCK 243. maddesinden hem de amaç suçtan cezalandırılması gerekir.³⁶⁴ Örneğin bir bilişim sistemine girilerek kişinin özel verilerinin (fotoğraf, mail vb.) elde edilmesi durumunda hem TCK 243. maddesi hem de duruma göre TCK 132, 134 veya 136 oluşmuş olacaktır.

TCK 243. ve 244. maddeleri arasındaki içtima ilişkisi hususunda öğretide çok farklı fikirler savunulmuştur. Bir görüşe göre, TCK 243. ve 244. maddeleri arasında tüketen-tüketilen norm ilişkisi vardır. Tüketen-tüketilen norm ilişkisinden bahsedilebilmesi için tüketen normun diğer normun koruduğu hukuki değeri de ortak bir şekilde koruması gerekir. Tüketen normun işlenebilmesi için tüketilen normun işlenmesi aranmaz.³⁶⁵ Dolayısıyla “*bilişim sisteminin işleyişini engelleme veya bozma; sistemdeki*

³⁶¹ İçel İçtima, s. 47-48.

³⁶² Koca/ Üzülmüş, s. 906.

³⁶³ Koca/ Üzülmüş, s. 906.

³⁶⁴ Tezcan/ Erdem/ Önok, s. 1160.

³⁶⁵ İçel, İçtima, s. 38.

verileri yok etme veya değiştirmek” ya da bu fiiller aracılığıyla haksız yarar sağlama suçlarının işlenmesi amacıyla sisteme girilmesi ya da sistemde kalınması durumunda fail TCK 243. maddesinden değil; TCK 244. maddesinden sorumlu olacaktır.³⁶⁶ Ancak ileride de anlatılacağı üzere TCK 244. maddesiyle korunan hukuki değer, bilişim sistemine girme suçuyla korunmaya çalışılan hukuki değerle aynı değildir. Bilişim sistemine girme suçuyla sistemin güvenliği ve güvenilirliğine ilişkin menfaat korunmaya çalışılırken; TCK 244 sistemin işleyişine ve sistemdeki verilerin güvenliğine ilişkin menfaat korunmaktadır.

Bir başka görüşe göre, TCK 243. ve 244. maddeleri arasında fikri içtima ilişkisi vardır. Çünkü bilişim sistemine girme fiili TCK 244. maddesinde sayılan fiillerle örtüşmektedir.³⁶⁷ Ancak iki suçun gerçekleştirilmesi için icra edilen fiiller farklıdır. Nitekim TCK 243. maddesinde cezalandırılan sisteme girme veya sistemde kalma fiili, TCK 244. maddesinde cezalandırılan sistemin işleyişini engelleme, bozma veya verilerin değiştirilmesi, yok edilmesi fiilleriyle örtüşmemektedir.

TCK 244. maddesindeki hareketlerin gerçekleştirilmesi için sisteme girilmesi veya sistemde kalınması zorunlu olmadığından bu iki suç arasında geçitli suç ilişkisi yoktur. Her iki suçun hukuki konuları farklı olduğundan bu suçlar arasında tüketen-tüketilen norm ilişkisi de yoktur. Burada gerçek içtima kuralı gereği fiil sayısınca suç oluşacağından, her bir fiil ayrı ayrı cezalandırılacaktır.³⁶⁸ Başka bir ifadeyle bilişim sistemine hukuka aykırı olarak giren fail, TCK 244’deki seçimlik hareketlerden birini de işlerse her iki maddeden ayrı ayrı ceza verilmesi yoluna gidilir. Zira bilişim sistemine girme veya sistemde kalma TCK 244. maddesindeki tipik fiille örtüşmemektedir.³⁶⁹

³⁶⁶ Tezcan/ Erdem/ Önok, s. 1160.

³⁶⁷ Koca/ Üzülmüş, s. 906.

³⁶⁸ Meran, s. 568.

³⁶⁹ Orta, s. 119.

Doktrinde TCK 243 ve 245. maddeleri arasında tüketen-tüketilen norm ilişkisi olduğu ileri sürülmüştür.³⁷⁰ TCK 245. maddesinde fail kart ve şifresini elde ederek kartı çıkaran bankanın bilişim sistemine hukuka aykırı olarak girmektedir. Yani bu fiille TCK 243. maddesi de ihlal edilmektedir. Ancak TCK 245. maddesi tüketen norm olduğundan, bu madde uygulama alanı bulur.³⁷¹ Yukarıda da bahsedildiği üzere tüketen-tüketilen norm ilişkisinden bahsedilebilmesi için tüketen normun diğer normun koruduğu hukuki değeri koruması gerekir. Bu iki madde farklı hukuki konulara sahip olduğundan ve hukuka aykırı elde edilmiş kart ve şifreyle ATM'ye girilmesi bilişim sistemine girilmesi olarak değerlendirilemeyeceğinden, sadece TCK 245. maddesi uygulama alanı bulacaktır.

2. Bileşik Suç

TCK 42. maddesine göre “*Biri diğerinin unsurunu veya ağırlaştırıcı nedenini oluşturması dolayısıyla tek fiil sayılan suçta bileşik suç denir. Bu tür suçlarda içtima hükümleri uygulanmaz.*” Bilişim sistemine girme suçu bileşik suç değildir. Zira iki farklı suçun unsurları veya nitelikli hal yönünden bir araya gelmesi bu suç bakımından söz konusu değildir.

Bilişim sistemine girme suçu başka bir suçun unsurunu ya da nitelikli halini oluşturuyorsa artık bileşik suç söz konusu olacak ve sadece o düzenlemeden sorumluluk doğacaktır. Yani hem TCK 243'ten hem de diğer suçtan sorumluluk söz konusu olmayacaktır. Doktrinde bir görüşe göre TCK 142/2-e ve TCK 158/1-f maddeleri bileşik suçtur. Zira hırsızlık ve dolandırıcılık suçunun işlenmesinde bilişim sistemlerinin araç olarak kullanılması cezayı ağırlaştırıcı nitelikli hal olarak öngörülmüştür ve TCK 42. maddesi gereği sadece nitelikli hırsızlık veya dolandırıcılıktan cezaya hükmedilecektir.³⁷² Ancak bu görüşe katılmak mümkün değildir zira bilişim sistemine girmek zorunlu olarak

³⁷⁰ Parlar, s. 55.

³⁷¹ Mahmutoğlu, s. 877.

³⁷² Mahmutoğlu, s. 864.

TCK 142/2-e ve 158/1-f maddelerinin unsuru değildir. Söz konusu maddelerde suçun bilişim sistemleri aracılığıyla işlenmesi nitelikli hal olarak öngörülürken; bu suçların failinin, mağdurun bilişim sistemine hukuka aykırı olarak girmesi aranmamıştır. Sonuç olarak bilişim sistemine girme fiili hırsızlık veya dolandırıcılık suçlarının nitelikli halini teşkil etmediğinden, bileşik suç söz konusu değildir. Bilişim sistemine girme suçu başka bir suçun unsurunu veya nitelikli halini oluşturmadiğundan, TCK 243. maddesi açısından bileşik suç mümkün değildir.

3. Zincirleme Suç

TCK 43. maddesinin birinci fıkrasına göre “*Bir suç işleme kararının icrası kapsamında, değişik zamanlarda bir kişiye karşı aynı suçun birden fazla işlenmesi durumunda, bir cezaya hükmedilir.*” Ancak bu ceza, belli oranda artırılır. Maddenin ikinci fıkrasına göre “*Aynı suçun birden fazla kişiye karşı tek bir fiille işlenmesi durumunda da birinci fıkra hükmü uygulanır.*”

TCK 243. maddesindeki suç işleme kararının icrası kapsamında değişik zamanlarda, bir kişiye karşı birden çok kez bilişim sistemine girme veya sistemde kalma suçu işlenirse zincirleme suç söz konusu olduğundan tek bir cezaya hükmedilecek ancak verilecek ceza dörtte birinden dörtte üçüne kadar artırılabacaktır. (TCK 43/1)³⁷³ Örneğin bir internet sitesindeki güvenlik açıklarını tespit etmek amacıyla sisteme değişik zamanlarda birden fazla kez giren fail için zincirleme suç kuralı gereği belirli oranda ağırlaştırılarak tek cezadan hüküm kurulacaktır. Ayrıca TCK 243. maddesi tek fiille birden fazla kişiye karşı işlenirse de aynı şekilde ceza verilecektir. (TCK 43/2)³⁷⁴

Girilen veya kalınan bilişim sisteminde başka bir kimsenin kişisel dosyasının bulunması ve bu dosyanın içeriğinin öğrenilmesi durumunda ayrıca dosya sahibi kişiye

³⁷³ Koca/ Üzülmüş, s. 906; Meran, s. 567; Parlar, s. 18; Soyaslan, s. 696.

³⁷⁴ Meran, s. 567.

karşı da TCK 243. maddesinin işlendiği ve TCK 43/2. maddesi gereği tek bir fiille aynı suçun birden fazla kişiye karşı işlendiği savunulmuştur.³⁷⁵ Ancak yukarıda da belirtildiği üzere bu suçun öngörülmesiyle korunmaya çalışılan değer sistemin güvenliğidir, bu sebeple de sisteme girilmesi ve sistemde kalınması ceza yaptırımına bağlanmıştır. Bir kimsenin şahsi dosyasının girilen sistemde olması TCK 243. maddesinin işlenmesi açısından önem arz etmemektedir. Dolayısıyla hala tek bir mağdur vardır ve o da sistem sahibidir. Ancak dosya sahibinin verileri ele geçirilmişse bu durumda gerçek içtima kuralı gereği hem TCK 243. maddesi hem de 136. maddesi dolayısıyla ayrı ayrı cezaya hükmedilecektir.³⁷⁶

4. Fikri İçtima

TCK 44. maddesi gereği “İşlediği bir fiil ile birden fazla farklı suçun oluşmasına sebebiyet veren kişi, bunlardan en ağır cezayı gerektiren suçtan dolayı cezalandırılır.” Doktrinde bazı yazarlar TCK 243. maddesiyle TCK 124 (“haberleşmenin engellenmesi”), 132 (“haberleşmenin gizliliğini ihlal”) ve 134 (“özel hayatın gizliliğini ihlal”). maddeleri arasında fikri içtima ilişkisinin olduğunu ileri sürmektedir.³⁷⁷ Ancak sayılan bu suçlarla bilişim sistemine girme suçunun fiilleri örtüşmediğinden fikri içtima ilişkisi söz konusu değildir. Fail hem bilişim sistemine giriyor hem de sayılan bu suçlara vücut verecek fiillerde bulunuyorsa gerçek içtima kuralı gereğince her suçtan ayrı ayrı cezalandırılacaktır.³⁷⁸

³⁷⁵ Mahmutoglu, s. 864; Çetin, s. 21; Erdoğan, s. 1418.

³⁷⁶ Yazarlara göre tek bir fiille birden fazla bilişim sistemine girme veya kalma gerçekleştirilemeyeceğinden TCK 43/2. maddesinin uygulaması bu suç için söz konusu değildir. Yaşar/ Gökcan/ Artuç, s. 7301.

³⁷⁷ Özbek/ Doğan/ Bacaksız, s. 966; Ekici Şahin/ Koruculu, s. 620.

³⁷⁸ Yargıtay 12. CD de bir kararında özel hayatın gizliliğini ihlal ve bilişim sistemine girme suçları arasında fikri içtima ilişkisi olmadığı yönünde hüküm kurmuştur. Bkz. “Sanık hakkında düzenlenen iddianamede; sanığın, mağdura ait facebook ve telefon hesaplarına rızası dışında girerek bilişim sistemine girme, mağdurun orijinal fotoğrafları ile birlikte çıplaklık içeren fotoğrafları mağdura aitmiş gibi internette paylaşarak görüntü veya seslerin ifşa edilmesi suretiyle özel hayatın gizliliğini ihlal suçlarını işlediği iddia edilmiş olup, sanığa yüklenen farklı eylemlerden dolayı ayrı ayrı hüküm kurulması gerektiği, TCK’nın 44/1. madde ve fıkrasındaki fikri içtima koşullarının bulunmadığı gözetilmeden, “bilişim sistemlerine girme ve özel hayatın gizliliğini ihlal suçlarının sabit olmakla birlikte tek bir eylem ile icra edildiğinden TCK’nın 44. maddesinin bu suçlar yönünden tatbik edilmesine” biçimindeki yasal ve yeterli olmayan gerekçelerle yazılı

Doktrinde TCK 136 ve TCK 243. maddeleri arasında fikri içtima ilişkisi olduğunu ileri süren yazarlar vardır.³⁷⁹ Ancak bilişim sistemine girme ve sistemden kişisel verilerin elde edilmesi durumunda iki ayrı fiil söz konusu olduğundan iki ayrı suç vardır. Bilişim sistemine giren kişi, zorunlu olarak verileri elde etme amacıyla sisteme girmemektedir. Dolayısıyla iki ayrı fiil söz konusudur ve gerçek içtima kuralına göre iki ayrı suçtan ceza belirlenmelidir.

H. YAPTIRIM, SORUŞTURMA, KOVUŞTURMA

Suçun temel şeklinin cezası TCK 243/1. maddesinde “*bir yıla kadar hapis veya adli para cezası verilir.*” şeklinde ifade edilmiştir. Yani seçenек yaptırım olarak hâkim hapis cezası veya adli para cezasından birine hükmedebilecektir.³⁸⁰ Maddede hapis cezasının alt sınırı, adli para cezasının alt ve üst sınırı gösterilmemiştir. TCK 49. maddesine göre “*Süreli hapis cezası, kanunda aksi belirtilmeyen hallerde bir aydan az, yirmi yıldan fazla olamaz. Hükmedilen bir yıl veya daha az süreli hapis cezası, kısa süreli hapis cezasıdır.*” TCK 61/9. maddesine göre “*Adli para cezasının seçimlik ceza olarak öngörüldüğü suçlarda bu cezaya ilişkin gün biriminin alt sınırı, o suç tanımındaki hapis cezasının alt sınırından az; üst sınırıda, hapis cezasının üst sınırından fazla olamaz.*” Kanun koyucu adli para cezasını seçenек yaptırım olarak öngördüğünden, TCK 50/2. maddesi gereği hâkim temel cezayı hapis cezası olarak belirlemişse artık bu cezayı adli para cezasına dönüştüremeyecektir.³⁸¹

şekilde görüntü veya seslerin ifşa edilmesi suretiyle özel hayatın gizliliğini ihlal suçundan mahkumiyet hükmü kurulması BOZMA NEDENİ YAPILMIŞTIR.” YARGITAY 12.CD. E. 2018/8261 K. 2019/6852

³⁷⁹ Mahmutoglu, s. 865.

³⁸⁰ Koca Üzülmöz, s. 907; Meran, s. 568.

³⁸¹ Koca/Üzülmöz, s. 907; Meran, s. 568.

TCK 243. maddesinde öngörülen ceza iki yıldan az hapis cezası olduğundan diğer koşulların da gerçekleşmesi halinde CMK 231. maddesi uyarınca hükmün açıklanması geri bırakılabileceği gibi TCK 51. maddesi uyarınca hapis cezası ertelenebilir.³⁸²

Suçun cezayı hafifletici nitelikli şekli için verilecek cezanın yarı oranında indirileceği; neticesi sebebiyle ağırlaşmış halin gerçekleşmesi durumundaysa “*altı aydan iki yıla kadar hapis cezasına*” hükmedileceği belirtilmiştir. Üçüncü fıkraya göre hükmedilen hapis cezası TCK 50/1. maddesi gereği adli para cezasına çevirebilir ancak bu durumda TCK 51. madde uyarınca hapis cezasının ertelenmesi imkânı bulunmamaktadır.³⁸³

TCK 243. maddesi açısından herhangi bir muhakeme şartı söz konusu değildir; suç resen soruşturulur ve kovuşturulur.³⁸⁴ Doktrinde bazı yazarlar bu suç için öngörülen cezanın az olması dolayısıyla suçun resen soruşturulabilir, kovuşturulabilir olmasını eleştirmekte; suçun muhakemesinin şikâyetle bağlı hale getirilmesinin daha yerinde olacağını savunmaktadır.³⁸⁵

Bilişim sistemine girme veya sistemde kalma suçunda görevli mahkeme 5235 S Kanun 11 ve 12. maddesine göre Asliye Ceza Mahkemesidir. 30.11.2021 tarihli Resmi Gazete yayımlanan HSK’nın 1229 numaralı kararı gereğince 15.12.2021 tarihinden itibaren görev yapacak Bilişim İhtisas Mahkemeleri belirlenmiştir.³⁸⁶ Karara göre “*iki asliye ceza mahkemesi bulunan yerlerde 2; üç, dört veya beş asliye ceza mahkemesi bulunan yerlerde 3; altı, yedi, sekiz veya dokuz asliye ceza mahkemesi bulunan yerlerde 6; on veya daha fazla asliye ceza mahkemesi bulunan yerlerde 8; yirmi beş veya daha*

³⁸² Erdoğan, s. 173.

³⁸³ Meran, s. 569.

³⁸⁴ Koca/ Üzülmöz, s. 907; Yaşar/ Gökcan/ Artuç, s. 7302.

³⁸⁵ Koca/Üzülmöz, s. 907.

³⁸⁶ Doktrinde bir görüşe göre özel uzmanlık mahkemelerin kurulması, mahkemelerin yetki ve görevlerine ilişkin karmaşaya yol açacağından bilişim suçlarıyla alakalı teknik konularda bilirkişiye başvurulması daha yerinde bir tercih olacaktır. Ünver, s. 145.

fazla asliye ceza mahkemesi bulunan yerlerde 20 ve 21; otuz beş veya daha fazla asliye ceza mahkemesi bulunan yerlerde 20, 21, ve 22 numaralı asliye ceza mahkemeleri ihtisas mahkemesi olarak” görevlendirilmiştir.

CMK 12. maddesi gereğince yetkili mahkeme suçun işlendiği yer mahkemesidir. Bilişim sistemine girme suçu, bizzat sistemin üzerinde gerçekleştiriliyorsa genel kurallar sorunu çözmeye yeterlidir ve doğrudan fiilin icra edildiği yerde suç işlenmiş sayılacaktır. Ancak bilişim suçlarında suçun işlendiği yerin tespiti bazı durumlarda özellik arz etmektedir. Zira bilişim suçlarıyla gerçekleştirilen ihlaller klasik suçlarla gerçekleştirilen ihlallerden farklılık arz eder çünkü klasik suç tiplerinde fiilen suçun gerçekleştirildiği fiziki bir mekân vardır. Fakat bilişim suçlarında sisteme girme, verileri elde etme gibi fiiller sanal ortamda örneğin bir ağ aracılığıyla gerçekleştirilmektedir. İşte böyle durumlarda suçun nerede işlenmiş sayılacağı başka bir ifadeyle suçun işlenmesinde araç olarak kullanılan sistemin bulunduğu yer mi yoksa girilen ya da kalınan sistemin bulunduğu yer mi suçun işlendiği yer sayılacağı sorunu karşımıza çıkmaktaydı.³⁸⁷ Bu sorunu çözmek için 7331 S Kanunla 08.07.2021 tarihinde CMK 12. maddesine eklenen altıncı fıkra gereğince “*Bilişim sistemlerinin, banka veya kredi kurumlarının ya da banka veya kredi kartlarının araç olarak kullanılması suretiyle işlenen suçlarda mağdurun yerleşim yeri mahkemeleri de yetkilidir.*” Yani artık hem suçun işlendiği yer mahkemesi hem de mağdurun bulunduğu yer mahkemesi yetkili olacağından, birden fazla yetkili mahkeme söz konusudur.

Bilişim sistemine girme suçu için dava zamanasını TCK 66. maddesi gereğince “*Beş yıldan fazla olmamak üzere hapis veya adli para cezasını gerektiren suçlarda sekiz*

³⁸⁷ Hem suçun işlenmesinde araç olarak kullanılan bilişim sisteminin bulunduğu yerin hem de üzerinde suçun işlendiği bilişim sisteminin bulunduğu yerin suçun işlendiği yer olarak kabul edilmesi gerektiğini savunmaktaydı. Mahmutoglu, s. 860.

yıl”; ceza zamanaşımıysa TCK 68. maddesi gereğince “Beş yıla kadar hapis ve adli para cezalarında on yıl”dır.

Bilişim sistemine kasten giren veya kalmaya devam eden bir kimsenin hareketleri neticesinde kastı olmaksızın verileri ele geçirmesi durumunda TCK’da olaya uygulanabilecek bir hüküm söz konusu değildir. Bu konuda bir boşluk olduğundan bunun yapılacak bir değişiklikle bir an önce giderilmesi gereklidir.³⁸⁸

II. VERİ NAKİLLERİNİN TEKNİK ARAÇLARLA İZLENMESİ SUÇU (TCK 243/4)

A. GENEL OLARAK

İlk bölümde ifade edildiği üzere bilişim alanındaki suçlar, bilişim sistemleri aracılığıyla veya bu sistemlere karşı gerçekleştirilen suçlardır. Bilişim suçlarının işlenmesi için sisteme erişim zorunluluk arz etmemekte ve hatta günümüz teknolojiyle sisteme girmeksizin veri nakillerinin izlenmesi mümkün olabilmektedir. Örneğin bluetooth aracılığıyla aktarılan verilerin izlenmesi durumunda, bilişim sistemine bir müdahale olmadığından fiil TCK 243 veya 244. maddeleri kapsamında cezalandırılmayacaktır. Bir kimsenin veri nakillerinin izlenmesi haksızlık teşkil eden bir fiil olduğundan, bu fiilin cezasız kalmaması ve AKSSS’ye uyum sağlanması için TCK 243. maddesine 6698 S. KVKK ile 4. fıkra eklenmiştir.³⁸⁹ Fıkraya göre, “Bir bilişim sisteminin kendi içinde veya bilişim sistemleri arasında gerçekleşen veri nakillerini, sisteme girmeksizin teknik araçlarla hukuka aykırı olarak izleyen kişi, bir yıldan üç yıla kadar hapis cezası ile cezalandırılır.” Eklenen bu fıkrayla AKSSS’ye uyum sağlanmış³⁹⁰

³⁸⁸ Karagülmez, s. 199-200.

³⁸⁹ Dülger, s. 312.

³⁹⁰ Akbulut, s. 157.

ve Sözleşmenin 3. maddesinde³⁹¹ “yasadışı araya girme”³⁹² şeklinde tanımlanan fiil Türk Hukukunda da suç haline getirilmiştir.³⁹³

Veri nakillerinin teknik araçlarla izlenmesi, TCK 243. maddesinin dördüncü fıkrasında düzenlense de bilişim sistemine girme suçundan tamamen farklı, bağımsız bir suç tipidir.³⁹⁴ Ancak TCK 243. maddesinin başlığının bilişim sistemine girme olduğu göz önünde bulundurulduğunda, sisteme girmeksizin teknik araçlarla verilerin izlenmesi suçunun bu maddede düzenlenmesi kanunun sistematığı bakımından yerinde olmamıştır.³⁹⁵ Bu fıkranın ayrı bir maddede bağımsız bir suç olarak düzenlenmesi daha yerinde bir tercih olacaktır.³⁹⁶

B. MADDİ KONU

Suç teşkil eden fiilin üzerinde işlendiği şey, bilişim sisteminin kendi içerisinde ya da başka bir bilişim sistemiyle arasında nakle konu verilerdir.³⁹⁷ Verilerin niteliğine ilişkin özel bir belirleme yapılmadığından, nakle konu her veri bu suçun maddi konusu olabilir.³⁹⁸ Suçun gerçekleşmesi için nakil sürecinin devam ediyor olması³⁹⁹ arandığından, verilerin nakil sürecinin bitmesinden sonra bu suç işlenemez.⁴⁰⁰ Dolayısıyla nakle konu olmayan, sistemde bulunan verilerin sisteme girilerek veya

³⁹¹ “Taraflardan her biri bilgisayar verisi taşıyan bir bilgisayar sisteminden, elektromanyetik dalgalarla yayılma da dahil, bilgisayar verilerinin bir bilgisayar sisteminden diğer bir bilgisayar sistemine veya bir bilgisayar sisteminin kendi içinde umuma kapalı olarak iletimi esnasında teknik yöntemler kullanılarak gerçekleştirilen araya girme fiilinin haksız yere ve kasten yapıldığı zaman kendi iç hukuku kapsamında, suç olarak tanımlanması için gerekli yasama tedbirlerini ve diğer tedbirleri kabul edecektir.”

³⁹² Dördüncü fıkra düzenlenirken fiilin İngilizce karşılığı olan “interface” araya girme şeklinde Türkçeye çevrilmiştir. Kanun koyucumuz araya girme ifadesi yerine veri naklini teknik araçlarla izleme ifadesini tercih etmiştir. Dülger, s. 311.

³⁹³ Koca/ Üzülmüş, s. 908.

³⁹⁴ Dülger, s. 310.

³⁹⁵ Özbek/ Doğan/ Bacaksız, s. 962.

³⁹⁶ Akbulut, s. 158-159.

³⁹⁷ Koca/ Üzülmüş, s. 909; Çetin, s. 23; Özsoy, s. 313.

³⁹⁸ Dülger, s. 314.

³⁹⁹ İngiltere’de Edmondson Davasında sesli mesaj kutularında depolanan mesajlar, iletimine devam edilen veri olarak kabul edilmiştir. Servis sağlayıcılarının bu mesajı sistemde alıcısının alması için hazır bekletmesinin veri naklinin sona ermesi şeklinde yorumlanamayacağı, kararda ifade edilmiştir. Dülger, s. 314.

⁴⁰⁰ Akbulut, s. 160.

girilmeden ele geçirilmesi durumunda, TCK 243/4. maddesindeki tipik fiil gerçekleşmediğinden, bu suçtan sorumluluk doğmayacaktır.⁴⁰¹

Burada teknik araçlarla izlenen verilerin niteliğine ilişkin bir ayrıma gidilmediğinden, nakle konu veri, kişisel veri olabilir. İzlenen veriler kişisel veri niteliğindeyse fiil TCK 135 vd maddeleri kapsamında değerlendirilebilir ancak her durumda kişisel veri nakillerinin izlenmesi verilerin ele geçirildiği anlamına gelmez.⁴⁰² Bazı durumlarda teknik araçlarla veri naklinin izlenmesi fiili; “*haberleşmenin engellenmesi*”, “*haberleşmenin gizliliğini ihlal*”, “*özel hayatın gizliliğini ihlal*” suçlarıyla da örtüşebilir.⁴⁰³ Fakat her sistemler arası veri naklinin izlenmesi durumunda bu suçların kanuni tanımındaki tipik fiil gerçekleşmemektedir. Sonuç olarak AKSSS’ye paralel olarak veri naklinin teknik araçlarla izlenmesi suçuna TCK’da yer verilmesi bazı fiillerin cezasız kalmasını engellemiştir.⁴⁰⁴

C. HUKUKİ KONU

Veri nakillerinin teknik araçlarla izlenmesi suçunun hukuki konusuna ilişkin farklı görüşler ileri sürülmüştür. Bir görüş suçun hukuki konusunun hem sistem güvenliği hem de özel yaşamın gizliliği olduğunu savunmaktadır.⁴⁰⁵ Ancak öncelikle burada sisteme erişim söz konusu olmadığından sistemin güvenliğinin korunduğu ileri sürülemez. Ayrıca maddede veri nakilleri denmiş, dolayısıyla bu verilerin kişinin özel yaşamına ilişkin olması zorunlu değildir. Doktrinde başka bir görüşse bu düzenlemeyle öncelikle verilerin güvenliğine ilişkin değerin korunduğunu ileri sürmüştür.⁴⁰⁶ Ancak veri nakillerinin teknik araçlarla izlenmesi suçunun gerçekleşmesi için verilerin içeriğinin öğrenilmesi, verilerin

⁴⁰¹ Tezcan/ Erdem/ Önok, s. 1163.

⁴⁰² Tezcan/ Erdem/ Önok, s. 1162.

⁴⁰³ Koca/ Üzülmüş, s. 908.

⁴⁰⁴ Koca/ Üzülmüş, s. 908.

⁴⁰⁵ Tezcan/ Erdem/ Önok, s. 1162.

⁴⁰⁶ Dülger, s. 312.

elde edilmesi aranmamıştır. Dolayısıyla getirilen düzenlemeyle verilerin güvenliğınden ziyade başka bir değeri korunmaya çalışılmaktadır.

Bu suçla ihlal edilip, cezai müeyyideyle korunmaya çalışılan değeri, sisteme girme veya sistemde kalma suçundan farklı olarak sistemin güvenliğı olmayıp; veri nakillerinin gizliliğıdir.⁴⁰⁷ AKSSS'nin açıklayıcı raporunda da bu suçun getirilmesiyle veri iletişiminin gizliliğinin korunmasının amaçlandığı belirtilmiştir.⁴⁰⁸

D. FAİL

Herkes bu suçun faili olabilir.⁴⁰⁹ Fail olmak bakımından herhangi bir nitelik ya da statüde olmak aranmadığından bu suç özgü suç değildir.⁴¹⁰ Bu sebeple “*bir bilişim sisteminin kendi içinde veya bilişim sistemleri arasında gerçekleştirilen veri nakillerini*” teknik araçlarla izleyen herhangi bir kimse, suçun faili olabilir.

Nakle konu verilerin tasarrufuna bırakıldığı kimse, veri naklinin teknik araçlarla izlenmesi suçunun faili olamaz. Zira veriler üzerinde tasarruf hakkı olan kimsenin, bu verileri izlemesi hukuka aykırı değildir.⁴¹¹

5237 S. TCK ile cezai sorumluluğun şahsiliğı ve tüzel kişilerin ceza sorumluluğunun olmadığı kabul edildiğinden, tüzel kişiler herhangi bir suçun faili olamaz.⁴¹² Bu sebeple veri nakillerinin teknik araçlarla izlenmesi suçunun da faili olamaz. Ancak TCK 246. maddesi gereğı bu suçla “*yararına haksız menfaat sağlanan tüzel kişiler hakkında bunlara özgü güvenlik tedbirlerine hükmolunur.*”

⁴⁰⁷ Koca/ Üzülmöz, s. 908.

⁴⁰⁸ Dölger, s. 311.

⁴⁰⁹ Akbulut, s. 159.

⁴¹⁰ Tezcan/ Erdem/ Önok, s. 1162; Koca/ Üzülmöz, s. 909.

⁴¹¹ Akbulut, s. 160.

⁴¹² Özgenci, s. 213-214.

E. MAĞDUR

Veri nakillerinin teknik araçlarla izlenmesi suçunun mağduru herkes olabilir.⁴¹³ Doktrinde bir görüş bu suçun mağdurunun, teknik araçlarla izlenen nakle konu veriler üzerinde hak sahibi kimse yani veriler üzerinde tasarruf hakkı sahibi kimse olduğunu ileri sürmektedir.⁴¹⁴ Ancak maddenin ihdas edilmesiyle “*bilişim sisteminin kendi içinde veya bilişim sistemleri arasında gerçekleşen veri nakillerini, sisteme girmeksizin teknik araçlarla hukuka aykırı olarak izleyen*” kimsenin cezalandırılması amaçlanmaktadır. Yani bir kimse teknik araçlarla bilişim sistemindeki veri naklini izlemeye karar verdiğinde, veri sahibinin kim olduğunu bilerek veya bilmeksizin bilişim sistemini esas alarak hareket etmektedir. Yani tipik fiili gerçekleştiren kimse, veri sahibinden bağımsız olarak belli bir bilişim sistemini esas alarak fiilini icra etmektedir. Dolayısıyla suçun mağduru veri sahibinden ziyade teknik araçlarla veri nakli izlenen bilişim sistemi üzerindeki hak sahibi kimsedir.

Ayrıca bilişim sistemleri arasında gerçekleşen veri nakillerinde iki ayrı sistem söz konusu olmaktadır. Yani sistem hem verilerin iletiildiği sistem olabilir hem de verileri ileten sistem olabilir. Doktrinde bir görüşe göre nakle konu veriler üzerinde hak sahibi kişi, veriler alıcısına ulaşmışsa alıcı; alıcının verileri almasına kadar geçen sürede gönderendir. Dolayısıyla suçun mağduru da verilerin alıcısına ulaştığı durumda alıcı; veriler alıcısı tarafından alınana kadar gönderendir.⁴¹⁵ Ancak bizce burada fail veri naklini bilişim sistemine girmeksizin izlemek istediğinde bilişim sistemini esas aldığından yani verinin hangi sisteme gönderildiğini veya hangi sistemden geldiğini gözetmeksizin belli bir bilişim sistemindeki veri naklini izlediğinden, mağdur izlenen sistem üzerinde hak sahibi kimsedir. Tüzel kişinin üzerinde hak sahibi olduğu bir bilişim sistemi aracılığıyla

⁴¹³ Dülger, s. 313.

⁴¹⁴ Tezcan/ Erdem/ Önok, s. 1162; Koca/ Üzülmöz, s. 909. Akbulut, s. 160.

⁴¹⁵ Akbulut, s. 160.

gerçekleştirilen veri nakli teknik araçlarla izleniyorsa, suçun mağduru tüzel kişilik olacaktır.⁴¹⁶

F. SUÇUN UNSURLARI

a. MADDİ UNSUR

“Bir bilişim sisteminin kendi içinde veya bilişim sistemleri arasında gerçekleşen veri nakillerini, sisteme girmeksizin teknik araçlarla hukuka aykırı olarak izlemek” suretiyle tipik fiil gerçekleştirilecektir. Burada dikkat edilmesi gereken husus izleme hareketinin sisteme girilmeksizin ve teknik araçlarla yapılmasıdır. Yani suçun kanuni tanımında failin sisteme girmeksizin veri aktarımını izlemesi arandığından, sisteme erişim halinde bu suç gerçekleşmemektedir.

TDK sözlüğünde izlemek *“gözlemek, incelemek”* şeklinde tanımlanmıştır. Fıkranın gerekçesindeyse *“verilerin izlenmesi eylemi, bilişim sistemlerine herhangi bir müdahalede bulunmaksızın teknik araçlarla bilişim sistemleri arasındaki veri nakillerinin takip edilmesini ifade etmektedir.”* şeklinde tanımlanmıştır.⁴¹⁷ Veri nakillerinin izlenmesi, *“veri trafiğinin takip edilmesidir”*.⁴¹⁸ 5651 S. Kanunun 2/1-h maddesinde izleme *“İnternet ortamındaki verilere etki etmeksizin bilgi ve verilerin takip edilmesi”* şeklinde tanımlanmıştır. Suçun oluşması için veri nakillerinin izlenmesi yeterli olup, verilerin ele geçirilmesi, içeriğinin öğrenilmesi aranmamaktadır.⁴¹⁹ Verilerin nakli, *“bilişim sisteminin kendi içinde veya bilişim sistemleri arasında”* gerçekleştiriliyor olabileceğinden, örneğin bir bilgisayardan yazıcıya, veri taşıma aracına veri nakli sırasında yapılan izleme bu madde kapsamında cezalandırılabilir.⁴²⁰

⁴¹⁶ Suçun mağdurunun tüzel kişileri oluşturan gerçek kişiler olduğunu savunan görüş için bkz.: Akbulut, s. 160.

⁴¹⁷ Akbulut, s. 157.

⁴¹⁸ Akbulut, s. 164

⁴¹⁹ Akbulut, s. 165.

⁴²⁰ Dülger, s. 314-315.

“Bilişim sisteminin kendi içinde veya bilişim sistemleri arasında gerçekleştirilen verilerin naklinin” teknik araçla izlenmesi tipik fiil olduğundan, her türlü veri nakil yöntemi (örneğin: e-mail, akıllı telefon, telefaks, elektromanyetik dalga⁴²¹ gibi) bilişim sistemi aracılığıyla gerçekleştirilmesi koşuluyla madde kapsamına girmektedir.⁴²² Suçun kanuni tanımında tipik fiilin teknik araç yardımıyla işlenebileceği belirtildiğinden, teknik araç kullanılmadan yapılan izlemeler bu madde kapsamında değerlendirilemeyecektir.⁴²³

Verilerin bilişim sistemleri aracılığıyla nakledilmesi USB, CD gibi cihazlar aracılığıyla gerçekleştirilebileceği gibi ağlar aracılığıyla da gerçekleştirilmektedir. TCK 243/4. maddesiyle yasaklanan, bilişim sistemleri arasında ağlar aracılığıyla gerçekleştirilen veri nakilleridir.⁴²⁴ Veri naklinin ağ aracılığıyla nasıl gerçekleştirildiği önemli değildir.⁴²⁵ Bilişim sisteminin kendi içindeki veri naklinin izlenmesi de bu suçta vücut verdiğinden, bilişim sisteminden veri taşıma aracına veri aktarılırken veya tersi durumda teknik araçlarla bu naklin izlenmesi TCK 243/4. maddesinin ihlali niteliğindedir.⁴²⁶

Veri naklinin umuma açık yapılması bu suçun oluşmasını engelleyecektir.⁴²⁷ Suçun gerçekleşmesi için veri naklinin gizliliğinin korunması amacıyla herhangi bir tedbirin alınması şart değildir. Veri iletişimi yapan kimselerin, bu iletişimi başkalarının izlemesini istememesi, suçun oluşması bakımından yeterlidir.⁴²⁸ Dolayısıyla tedbirin bulunup bulunmadığına bakılmaksızın veri naklinin kamuya açık olmaması suçun oluşması bakımından yeterlidir. “Bilişim sisteminin kendi içinde veya sistemler arasında

⁴²¹ AKSSS’nin aksine TCK’da elektromanyetik dalgalarla gerçekleştirilen veri nakilleri açıkça belirtilmemiş olsa da elektromanyetik dalgalarla gerçekleştirilen veri nakillerinin izlenmesi de madde kapsamında değerlendirilmelidir. Akbulut, s. 162.

⁴²² Akbulut, s. 161-162.

⁴²³ Koca/ Üzülmüş, s. 910.

⁴²⁴ Tezcan/ Erdem/ Önok, s. 1162.

⁴²⁵ Koca/ Üzülmüş, s. 909.

⁴²⁶ Dülger, s. 315.

⁴²⁷ Akbulut, s. 163.

⁴²⁸ Akbulut, s. 159.

gerçekleştirilen veri nakilleri” niteliği gereği gizli olduğundan, aksini kabule yol açacak bir durum olmadığı sürece bu nakillerin izlenmesi TCK 243/4. maddesine vücut verecektir.⁴²⁹

Madde metninde veri naklinin, hangi teknik araçlarla nasıl izleneceğine ilişkin bir belirleme yapılmamıştır. Teknik araçların ne olduğu konusunda maddede bir açıklamaya yer verilmediğinden, kullanılan herhangi teknik araç ve yöntemin veri naklini izlemeyi sağlaması durumunda suç oluşmaktadır. Başka bir deyişle kullanılan teknik araç veya yöntem önemli olmayıp; önemli olan veri naklini izlemeye elverişli araç kullanılıp kullanılmadığıdır.⁴³⁰ Verileri izleme hareketi, nakil sırasında yani aktarılan verinin kaynaktan çıktıktan ancak hedef sisteme ulaşmadan önce işlenmiş olması gerekir.⁴³¹ İzlenen verilerin niteliği önemsiz olup, nakle konu verilerin içeriğinin öğrenilip öğrenilmediği suçun oluşması bakımından aranmamış ve veri naklinin izlenmesi yeterli görülmüştür.⁴³²

TCK 243. maddesinin 4. fıkrasında düzenlenen fiil, sisteme girme veya sistemde kalma suçundan farklı bir suç teşkil etmektedir. Dolayısıyla veri nakillerinin teknik araçlarla sisteme girilmeksizin işlenmesi suçunun TCK 243. maddesinde düzenlenmesi yerinde bir tercih olmamıştır. Zira 243. maddede başlığından da anlaşılacağı üzere sisteme erişim, sistemde kalma cezalandırılırken veri naklinin izlenmesinde sisteme girme dahi söz konusu değildir. Dolayısıyla TCK 243/2 ve 3. fıkralarının bu suç bakımından uygulanması söz konusu olmayacaktır.⁴³³

Veri nakillerinin teknik araçlarla izlenmesi suçu, suçun kanuni tarifinde tipik hareketin nasıl gerçekleştirileceğinin öngörülmesi sebebiyle bağlı hareketli bir suçtur.

⁴²⁹ Koca/ Üzülmüş, s. 909.

⁴³⁰ Koca Üzülmüş, s. 910; Tezcan/ Erdem/ Önok, s. 1163.

⁴³¹ Koca/Üzülmüş, s. 910.

⁴³² Tezcan/ Erdem/ Önok, s. 1163.

⁴³³ Tezcan/ Erdem/ Önok, s. 1163.

Suçun kanuni tarifinde herhangi bir netice aranmadığından neticesiz bir suçtur.⁴³⁴ Ayrıca teknik araçlarla veri nakillerinin sisteme girilmeksizin izlenmesi halinde, herhangi bir zarar veya somut tehlikenin doğması aranmadığından bu suç, soyut tehlike suçudur.⁴³⁵

Veri naklinin izlenmesi fiilinin temadi teşkil etmesi ve ortaya çıkan haksızlığın belirli bir süre devam etmesi gerektiğinden bu suç mütemadi bir suçtur.⁴³⁶ Suçun gerçekleşmesi için fiilin belirli bir süre devam etmesi gerektiğinden, izleme fiilinin başlamasıyla suç gerçekleşir ancak fiil devam ettiği sürece suç bitmez. Veri naklinin izlenmesi suçunun işlenmesi için gereken izleme süresi, somut olaya göre hâkim tarafından takdir edilmelidir.

Fıkra metninde hukuka aykırı olarak tipik fiilin gerçekleştirilmesi özel olarak arandığından başka bir deyişle hukuka aykırılık suçun kanuni tanımından ayrıca gösterildiğinden, tipikliğin unsuru sayılmalıdır.⁴³⁷ Dolayısıyla fail veri naklini hukuka aykırı olarak izlediğini bilmelidir.⁴³⁸

b. MANEVİ UNSUR

Veri naklini teknik araçlarla izleme suçu ancak kasten işlenebilir.⁴³⁹ Bunun için de fail, “*bilişim sisteminin kendi içinde veya bilişim sistemleri arasındaki*” veri naklini teknik araçlarla izlediğini bilmeli ve istemelidir.

Suçun taksirli hali kanunda düzenlenmediğinden dikkat ve özen yükümlülüğüne aykırı olarak veri nakillerini teknik araçla izleyen kimse cezalandırılmayacaktır. Suçun

⁴³⁴ Akbulut, s. 168.

⁴³⁵ Tezcan Erdem Önok, s. 1164; Özsoy, s. 313; Koca/ Üzülmöz, s. 910.

⁴³⁶ Koca/ Üzülmöz, s. 910.

⁴³⁷ Özbek/ Doğan/ Bacaksız, s. 962.

⁴³⁸ Akbulut, s. 166.

⁴³⁹ Koca/ Üzülmöz, s. 910.

kanuni tarifinde, suçun belirli bir saikle işlenmesi aranmadığından genel kastla işlenebilen bir suçtur. Suç ancak doğrudan kastla işlenebilir.⁴⁴⁰

Fıkra metninde hukuka aykırılık ibaresi geçtiğinden failin kastı fiilin hukuka aykırı olduğunu da kapsamalıdır.⁴⁴¹ Failin hukuka aykırılık bilinciyle hareket etmesi arandığından suç ancak doğrudan kastla işlenebilir; olası kastla işlenemez.⁴⁴²

c. HUKUKA AYKIRILIK

Bu suçla bağdaşan hukuka uygunluk sebepleri, kanun hükmünün ve amirin emrinin icrası (TCK 24) ile ilgili kişinin rızasıdır. (TCK 26). Teknik araçlarla veri naklinin izlendiği bilişim sistemi üzerinde hak sahibinin rızası bu suçla bağdaşır zira *“kişinin üzerinde mutlak surette tasarruf edebileceği hakka”* ilişkin açıkladığı bir rıza söz konusudur.⁴⁴³

Kanun hükmünün icrası veya yetkili amirin verdiği emrin icrası çerçevesinde veri naklinin teknik araçlarla izlenmesi halinde de fiil hukuka uygundur. Örneğin önleme veya koruma tedbirleri kapsamında yapılan izlemeler hukuka uygunluk nedenidir. (CMK 135, PVSK ek madde 6-7, MİT Kanunu madde 6)⁴⁴⁴ CMK 140. maddesinde düzenlenen teknik araçlarla izleme koruma tedbiri, bu madde kapsamından hukuka uygunluk nedeni sayılmaz.⁴⁴⁵

⁴⁴⁰ Koca/ Üzülmüş, s. 910.

⁴⁴¹ Koca/ Üzülmüş, s. 910.

⁴⁴² Akbulut, s. 168.

⁴⁴³ Koca/ Üzülmüş, s. 910; Tezcan/ Erdem/ Önok, s. 1164.

⁴⁴⁴ Koca/ Üzülmüş, s. 910; Akbulut, s. 166-167.

⁴⁴⁵ Tezcan/ Erdem/ Önok, s. 1164.

G. SUÇUN ÖZEL GÖRÜNÜŞ BİÇİMLERİ

a. TEŞEBBÜS

“*Veri naklinin teknik araçlarla izlenmesi suçu*”, neticesiz bir suç olduğundan izlemenin gerçekleşmesiyle suç tamamlanır ve kural olarak bu suça teşebbüs mümkün değildir; ancak hareketin parçalara bölünebildiği durumlarda teşebbüs mümkündür.⁴⁴⁶ Örneğin teknik araçla veri naklini izlemek isteyen kimse cihazı çalıştırmış ancak cihaz bilişim sistemindeki güvenlik mekanizmalarını bertaraf ederek veri izlemeyi başaramamışsa teşebbüsten sorumluluk doğacaktır.

Veri naklinin teknik araçlarla izlenmesi suçu mütemadi bir suç olduğundan, izlemenin gerçekleşmesiyle suç tamamlanır ancak izlemeye son verilmedikçe suç bitmez. Dolayısıyla veri naklini teknik araçlarla izlemeye başlayan bir kimsenin elinde olmayan nedenlerle örneğin yakalanması halinde hareketine son vermek zorunda kalması durumunda fail teşebbüsten değil; tamamlanmış suçtan sorumlu olacaktır. Zira suç artık tamamlanmıştır.⁴⁴⁷ Bu suça teşebbüs veri naklinin izlenmeye başlamasına kadarki süreç için mümkündür. Veri naklinin izlenmeye başlanmasıyla artık suç gerçekleştiğinden, bu aşamadan sonra gönüllü vazgeçme durumu da mümkün olmayacaktır.⁴⁴⁸

Teşebbüsten sorumluluğun doğması için failin icra hareketlerine doğrudan doğruya başlamış olması gerekir. Dolayısıyla hazırlık hareketleri içerisinden değerlendirilebilecek hareketler örneğin teknik araç satın almak, kabul etmek, bulundurmak bu suça teşebbüs bakımından cezai sorumluluğun doğmasına sebebiyet vermeyecektir. Ancak bu hareketler TCK 245/A maddesinde bağımsız bir suç olarak

⁴⁴⁶ ÖZBEK/ DOĞAN/ BACAKSIZ, s. 965.

⁴⁴⁷ Tezcan/ Erdem/ Önok, s. 1164; Koca/ Üzülmüş, s. 911.

⁴⁴⁸ Akbulut, s. 169.

öngörüldüğünden, kişinin bu madde çerçevesinde cezai sorumluluğu söz konusu olacaktır.⁴⁴⁹

b. İŞTİRAK

TCK 243/4. maddesi iştirak bakımından özellik göstermez; TCK 37-41. maddeleri bu suç açısından da geçerlidir. Dolayısıyla suçun müşterek fail, dolaylı fail olarak işlenmesi ve bu suça azmettirme veya yardım mümkündür.

Veri naklinin teknik araçlarla izlenmesi suçu mütemadi bir suç olduğundan, fiilin icrası devam ettiği sürece bu suça iştirak mümkündür.⁴⁵⁰ Ancak veri naklini izlemeye başladıktan sonra artık suç işlenmiş olduğundan suça azmettirme mümkün değildir.⁴⁵¹

Doktrinde bir görüşe göre; teknik araç sağlayan kimse, veri naklini izleyen kimseyle ortak suç işleme iradesiyle hareket etmişse fail olarak TCK 243/4. maddesinden; sadece yardım etmek için yani iştirak iradesiyle hareket etmişse TCK 243/4. maddesine yardım eden olarak; iştirak iradesi hiçbir şekilde yoksa TCK 245/A maddesinden sorumlu olacaktır.⁴⁵² Ancak teknik araç sağlayan kimse veri naklini fiilen izleyen kimseyle ortak suç işleme iradesiyle hareket etmiş ve fiil üzerinde ortak hakimiyet kurulmuşsa bu kişi hem bağımsız olarak cezalandırılan hazırlık hareketi niteliğindeki TCK 245/A maddesinden hem de TCK 243/4. maddesinden cezalandırılmalıdır. Sadece izleme fiilini gerçekleştiren kişiye TCK 243/4. maddesinden sorumlu tutulmalıdır. Teknik araç sağlayan kişi, TCK 243/4. maddesindeki suçun işlenmesi için yani şerik sıfatıyla TCK 245/A maddesini gerçekleştirmişse, bu kişi TCK 245/A maddesi bakımından fail; TCK 243/4. maddesi bakımından yardım eden sıfatıyla şeriktir. Failliğin şerikliğe nazaran asliliği kuralınca bu kişi sadece TCK 245/A maddesinden sorumlu tutulmalıdır. Teknik

⁴⁴⁹ Tezcan/ Erdem/ Önok, s. 1165.

⁴⁵⁰ Akbulut, s. 169.

⁴⁵¹ Dülger, s. 319.

⁴⁵² Tezcan/ Erdem/ Önok, s. 1165.

araç sağlayan kişi iştirak iradesiyle hareket etmemişse sadece TCK 245/A maddesinden sorumlu olmalıdır.

c. İÇTİMA

Doktrinde bir görüş TCK 243/4. maddesiyle TCK 245/A maddesi arasında asli norm- tali norm ilişkisi olduğunu bu sebeple TCK 243/4. maddesindeki fiilin işlendiği durumlarda faili ayrıca TCK 245/A maddesinden sorumlu tutamayacağımızı ileri sürmektedir.⁴⁵³ Başka bir görüşse teknik araç satın alan kimsenin bu cihazla veri naklini izlemesi durumunda tek bir fiil olduğundan fail hakkında sadece TCK 243/4. maddesinden hüküm kurulması gerektiğini savunmaktadır.⁴⁵⁴ Ancak iki madde arasında böyle bir durum söz konusu değildir. Zira iki maddede düzenlenen tipik fiiller çok farklıdır. TCK 243/4. maddesinde teknik araçlarla verilerin izlenmesi suç haline getirilirken; TCK 245/A maddesinde bilişim suçlarının işlenmesinde hazırlık hareketi sayılabilecek fiiller suç haline getirilmiştir. İki maddede farklı fiiller suç olarak öngörüldüğünden söz konusu görüşe katılmak mümkün değildir. Failin veri naklini izlemek için teknik araç üretilip veya satın alıp, veri naklini izlemesi durumunda farklı fiiller söz konusu olduğundan, gerçek içtima kuralı gereğince fail hakkında TCK 243/4. maddesinden ve TCK 245/A maddesinden hüküm kurulacaktır.⁴⁵⁵

1. Bileşik Suç

“Bir bilişim sisteminin kendi içinde veya bilişim sistemleri arasında gerçekleşen veri nakillerini teknik araçla izleme suçu” başka bir suçun unsuru veya nitelikli hali olmadığından TCK 243/4. maddesi bakımından bileşik suç söz konusu değildir.

⁴⁵³ Tezcan/ Erdem/ Önok, s. 1165.

⁴⁵⁴ Yazara göre TCK 245/A maddesi cezalandırılmayan hazırlık hareketleri için getirildiğinden TCK 243/4. maddesinin gerçekleştirildiği hallerde sadece TCK 243/4. maddesinden ceza verilmelidir. Aksi halde çifte cezalandırılma yasağı ihlal edilmiş olur. Dülger, s. 319.

⁴⁵⁵ Akbulut, s. 170.

2. Zincirleme Suç

TCK 243/4. maddesindeki suç işleme kararının icrası kapsamında “*bir bilişim sisteminin kendi içinde veya bilişim sistemleri arasında gerçekleşen veri nakillerini*” teknik araçla farklı zamanlarda aynı kişiye karşı birden çok izleyen kimse TCK 43/1 maddesi gereğince zincirleme suç hükümlerine göre sorumlu tutulacaktır.⁴⁵⁶ Doktrinde bir görüşe göre failin teknik araçlarla naklini izlediği verilerin farklı kişilere ait olması durumunda, fail hakkında TCK 43/2. maddesi uygulanabilecektir.⁴⁵⁷ Ancak teknik araçlarla veri naklinin izlenmesi suçunun mağduru bilişim sistemi üzerinde hak sahibi kimse olduğundan, TCK 43/2. maddesi bu durumda uygulanmayacaktır zira tek bir mağdur vardır. Tek bir izleme fiiliyle birden çok bilişim sisteminden nakledilen verilerin izlenmesi durumunda birden fazla kişiye karşı bu suçun işlenmesi söz konusu olduğundan, TCK 43/2. maddesi uygulanacaktır.⁴⁵⁸

3. Fikri İçtima

“*Bir bilişim sisteminin kendi içinde veya bilişim sistemleri arasında gerçekleşen veri nakillerini*” teknik araçla izleyen fail; verilerin içeriğini öğrenmiş, kişisel verileri elde etmiş veya verilerin naklini engellemiş olabilir. Failin veri naklini engellemesi durumunda TCK 124. maddesi; verilerin içeriğinin öğrenilmesi durumunda TCK 132 veya 134. maddeleri; verileri elde etmesi durumunda TCK 136. maddesi de oluşmaktadır.⁴⁵⁹ Doktrinde bir görüşe göre bu halde fail gerçek içtima kuralı gereğince hem 243/4. maddesinden hem bu suçlardan ayrı ayrı cezalandırılmalıdır.⁴⁶⁰ Ancak böyle

⁴⁵⁶ Akbulut, s. 169

⁴⁵⁷ Koca/ Üzülmmez, s. 911.

⁴⁵⁸ Dülger, s. 319.

⁴⁵⁹ Tezcan/ Erdem/ Önok, s. 1165; Özbek/ Doğan/ Bacaksız, s. 962.

⁴⁶⁰ Koca/ Üzülmmez, s. 911; Dülger, s. 319.

bir durumda fail tek bir fiile bu suçları işlemişse fikri içtima kuralı⁴⁶¹; birden fazla fiille bu suçları işlenmişse gerçek içtima kuralı uygulanmalıdır.⁴⁶²

H. SORUŞTURMA, KOVUŞTURMA, YAPTIRIM

Veri naklinin teknik araçlarla izlenmesi suçu için “*bir yıldan üç yıla kadar hapis cezası*” öngörülmüştür. Kanundaki şartların gerçekleşmesi durumunda hapis cezasının ertelenmesi veya hükmün açıklanmasının geri bırakılması mümkündür.

Veri naklinin teknik araçlarla izlenmesi suçu ve TCK 245/A maddesi için öngörülen cezalar açısından bir dengesizlik yaratılmıştır. Zira TCK 243/4. maddesindeki suçun tamamlanmış hali için “*bir yıldan üç yıla kadar hapis cezası*” istenirken; suçun hazırlık hareketi boyutunda kalan fiilleri yaptırıma bağlayan TCK 245/A maddesi için “*bir yıldan üç yıla kadar hapis ve beş bin güne kadar adli para cezası*” öngörülmüştür.⁴⁶³

TCK 243/4 maddesinde düzenlenen suç resen soruşturulan, kovuşturulan bir suçtur, uzlaştırma kapsamında değildir. 5235 S. Kanunun 11 ve 12. maddeleri gereğince görevli mahkeme, Asliye Ceza Mahkemeleridir. 30.11.2021 tarihli Resmi Gazete yayımlanan HSK’nın 1229 numaralı kararı gereğince 15.12.2021 tarihinden itibaren görev yapacak Bilişim İhtisas Mahkemeleri belirlenmiştir.⁴⁶⁴ Karara göre “*iki asliye ceza mahkemesi bulunan yerlerde 2; üç, dört veya beş asliye ceza mahkemesi bulunan yerlerde 3; altı, yedi, sekiz veya dokuz asliye ceza mahkemesi bulunan yerlerde 6; on veya daha fazla asliye ceza mahkemesi bulunan yerlerde 8; yirmi beş veya daha fazla asliye ceza mahkemesi bulunan yerlerde 20 ve 21; otuz beş veya daha fazla asliye ceza mahkemesi*

⁴⁶¹ Akbulut, s. 170.

⁴⁶² Tezcan/ Erdem/ Önok, s. 1165.

⁴⁶³ Tezcan/ Erdem/ Önok, s. 1165.

⁴⁶⁴ Doktrinde bir görüşe göre özel uzmanlık mahkemelerin kurulması, mahkemelerin yetki ve görevlerine ilişkin karmaşaya yol açacağından bilişim suçlarıyla alakalı teknik konularda bilirkişiye başvurulması daha yerinde bir tercih olacaktır. Ünver, s. 145.

bulunan yerlerde 20, 21, ve 22 numaralı asliye ceza mahkemeleri ihtisas mahkemesi olarak” görevlendirilmiştir.

CMK 12. maddesi gereğince yetkili mahkeme suçun işlendiği yer mahkemesidir. Ayrıca 7331 S Kanunla 08.07.2021 tarihinde CMK 12. maddesine eklenen altıncı fıkra gereğince “Bilişim sistemlerinin, banka veya kredi kurumlarının ya da banka veya kredi kartlarının araç olarak kullanılması suretiyle işlenen suçlarda mağdurun yerleşim yeri mahkemeleri de yetkilidir.” Yani artık suçun işlendiği yer mahkemesi ve mağdurun bulunduğu yer mahkemesi yetkili olacağından, birden fazla yetkili mahkeme söz konusudur.

ÜÇÜNCÜ BÖLÜM

SİSTEMİ ENGELLEME, BOZMA, VERİLERİ YOK ETME VEYA DEĞİŞTİRME SUÇLARI

İ. GENEL OLARAK

“Sistemi engelleme, bozma, verileri yok etme veya değiştirme” suçu 5237 S TCK’nın ikinci kitabının, “Topluma Karşı Suçlar” başlıklı üçüncü kısmının onuncu bölümünde “Bilişim Alanında Suçlar” başlığı altında 244. maddede⁴⁶⁵ düzenlenmiştir. Maddede aslında üç ayrı suça yer verilmiştir. Birinci fıkroda “Bilişim sisteminin işleyişini

⁴⁶⁵ TCK 244. maddesinin gerekçesine göre “Maddenin birinci fıkrasında bir bilişim sisteminin işleyişini engelleme, bozma, sisteme hukuka aykırı olarak veri yerleştirme, var olan verileri başka bir yere gönderme, erişilmez kılma, değiştirme ve yok etme fiilleri, suç olarak tanımlanmaktadır. Böylece sistemlere yöneltilen ızzar fiilleri özel bir suç hâline getirilmiştir. Aracın fizik varlığı ve işlemlerini sağlayan bütün diğer unsurları, söz konusu suçun konusunu oluşturmaktadır. Fıkroda seçimlik hareketli bir suç meydana getirilmiştir.

İkinci fıkroda, bu fiillerin bir banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi hakkında işlenmesi hâlinde, verilecek cezanın artırılması öngörülmüştür.

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

engelleme veya bozma suçu”, ikinci fıkrada *“bilgişim sistemindeki verileri bozma, yok etme, deęiştirme veya erişilmez kılma, sisteme veri yerleřtirme, var olan verileri başka bir yere gönderme”* suçu ve dördüncü fıkrada birinci ve ikinci fıkrada sayılan hareketler aracılığıyla *“kişinin kendisinin veya başkasının yararına haksız çıkar sağlama suçu”* hüküm altına alınmıştır. Maddenin üçüncü fıkrasında cezayı ağırlaştırıcı nitelikli hal düzenlenmiş ve suçun *“bir banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilgişim sistemi üzerinde işlenmesi halinde, verilecek ceza yarı oranında artırılır.”* denmiştir.

TCK 244. maddesinde, madde başlığının da yansıttığı üzere sistemin işleyişine müdahale ve verilere müdahale teşkil eden eylemler ceza yaptırımına bağlanmak istenmiştir. Ancak dördüncü fıkrada düzenlenen suçla sistemin işleyişine müdahale veya verilere müdahale fiillerinden ziyade bu fiiller aracılığıyla haksız yarar sağlama fiili cezalandırılmak istenmiştir. Bu sebeple dördüncü fıkranın TCK 244. maddesi altında düzenlenmesi yerinde bir tercih olmamıştır.⁴⁶⁶ Çalışmamızda bilgişim sistemine ve verilere müdahale suçları bu başlık altında incelenecek olup, haksız çıkar sağlama suçu ayrı bir başlık altında incelenecektir.

TCK 244. maddesinin TBMM Adalet Alt Komisyonunda kabul edilen hali, maddenin mevcut halinden farklıdır.⁴⁶⁷ Maddenin komisyonda kabul edilen halinde, ilk iki fıkra yani sisteme ve verilere müdahale tek bir fıkrada düzenlenmişti. TBMM Genel Kurulunda verilen bir önergeyle sisteme müdahale teşkil eden fiillerle verilere müdahale nitelięi taşıyan fiillerin ağırlığının farklı olması dolayısıyla, öngörülen cezaların da

⁴⁶⁶ Koca/ Üzülmöz, s. 912.

⁴⁶⁷ Maddenin ilk hali: “Bir bilgişim sisteminin işleyişini engelleyen, bozan, sisteme hukuka aykırı olarak veri yerleřtiren, var olan verileri başka yere gönderen, erişilmez kılan, deęiştiren, yok eden kimseye bir yıldan üç yıla kadar hapis cezası verilir.” şeklindeydi.

işlenen fiillerin ağırlığına uygun olması gerektiğinden, ayrı fıkralarda ayrı iki suç olarak düzenlenmesi kabul edilmiştir.⁴⁶⁸

TCK 244. maddesinin karşılığı olarak, birebir aynı unsurları içermemelerine rağmen 765 S TCK’da 525/b maddesi gösterilebilir. TCK 244. maddesinde, eski kanundan farklı olarak “*verileri erişilmez kılmak, sisteme veri yerleştirmek ve var olan verileri başka bir yere göndermek*” hareketleri de yaptırım altına alınmış; sisteme zarar vermek ifadesineyse metinde yer verilmemiştir. Ayrıca suç özel kastla işlenebilen bir suç olmaktan çıkarılmış ve failin amacına bakmaksızın bilişim sistemi ve içerisindeki verilerin bütünlüğü koruma altına alınmıştır.⁴⁶⁹ Bunun yanında, sayılan hareketlerle haksız yarar elde etmek ancak başka suç oluşturmadığı takdirde uygulanabilecek bir suç olarak düzenlenmiştir.⁴⁷⁰

5237 S TCK 244. maddesi, 1997 ve 2003’te hazırlanan TCK Tasarılarında geçen düzenlemeler esas alınarak oluşturulmuştur. Her iki tasarıda da “*Bu suçlara teşebbüs halinde faillere tamamlanmış suçun cezası verilir.*” ifadesine yer verilmiş ancak bu ifadeye 5237 S TCK’da yer verilmemiştir.⁴⁷¹

TCK 244. maddesinde, AKSSS’nin “verilere müdahale” başlıklı 4. maddesi ve “sisteme müdahale” başlıklı 5. maddesinin karşılığını oluşturan fiiller hüküm altına alınmıştır.⁴⁷² Sözleşme sistematığında verilere müdahale fiillerine, sisteme müdahale fiillerinden önce yer verilmesinin sebebi; verilere müdahale edilerek sistemin işleyişinin engellenmesi veya bozulmasının mümkün olması ve bu hareketlerin sisteme müdahale suçu içerisinde değerlendirilmesinden kaynaklanmaktadır.⁴⁷³ 5237 S TCK’da ise kanun

⁴⁶⁸ Karagülmez, s. 213; Koca, s. 90-91.

⁴⁶⁹ 525/b maddesindeki düzenlemeyle fail bilişim sistemine veya verilere yönelik zarar verici fiili ancak yarar sağlama amacıyla gerçekleştirdiğinde cezalandırılmaktadır. Koca, s. 90.

⁴⁷⁰ Özel kast arandığından bu kastla hareket etmeyip sisteme zarar veren cezasız kalmaktaydı.

⁴⁷¹ Akbulut, s. 10-11.

⁴⁷² Ketizmen, s. 114; Kurt, s. 160.

⁴⁷³ Akbulut, s. 13.

koyucu, önce sisteme müdahaleye daha sonra verilere müdahaleye yer vermeyi tercih etmiştir. Verilere müdahale suçunun ilk fıkrada düzenlenmesi daha doğru bir tercih olacaktır. Nitekim birinci fıkrada düzenlenen sisteme müdahale suçu, ikinci fıkrada sayılan hareketlerin gerçekleştirilmesi suretiyle de işlenebilmektedir. Bu sebeple TCK sistematığı açısından bu iki fıkranın yer değiştirmesi daha yerinde bir tercih olacaktır.⁴⁷⁴ Ayrıca Sözleşmede “*sisteme veri yerleştirmek*” ve “*var olan verileri başka yere göndermek*” hareketleri sisteme müdahale altında düzenlenmiştir. TCK 244. maddesindeyse bu hareketlere verilere müdahalenin düzenlendiği ikinci fıkrada yer verilmiştir.⁴⁷⁵

TCK 244/2. maddesinde düzenlenen seçimlik hareketlerden “erişilmez kılma”, “sisteme veri yerleştirme”, “var olan verileri başka yere gönderme” hareketleri AKSSS’nin 7. maddesinde düzenlenen “*bilgisayar bağlantılı sahtecilik*” ve 8. maddesinde düzenlenen “*bilgisayar bağlantılı dolandırıcılık*” fiillerine paralel nitelikte düzenlemeler olup, TCK’yı Sözleşmeyle uyumlu hale getirmiştir.⁴⁷⁶ Ancak TCK’da bilgisayar bağlantılı sahtecilik suçuna yer verilmemiştir. Söz konusu 7. madde kapsamındaki fiiller TCK 244/2. maddesi ve evrakta sahtecilik suçları (TCK 204 vd) kapsamında değerlendirilebilecek olsa da AKSSS’nin getirdiği yükümlülük gereğince bilgisayarlarla gerçekleştirilen sahtecilik fiillerinin TCK’da yaptırıma bağlanması gerekir.⁴⁷⁷

⁴⁷⁴ Akbulut, s. 31.

⁴⁷⁵ Alman Ceza Kanunda da Siber Suç Sözleşmesine uyumlu bir sistematik tercih edilmiş ve 303/a maddesinde verilerin değiştirilmesi, 303/b maddesinde bilgisayar sabotajı düzenlenmiştir. Akbulut, s. 13.

⁴⁷⁶ Karagülmez, s. 214; Kurt, s. 183.

⁴⁷⁷ Ünver, s. 96.

A. HUKUKİ KONU

Suçun hukuki konusu “suç ile ihlal edilen; ceza normuyla korunmaya çalışılan değer veya menfaattir”.⁴⁷⁸ TCK 244. maddesinde düzenlenen suçların hukuki konularına ilişkin de bilişim sistemine girme suçunda olduğu gibi çok farklı fikirler ileri sürülmüştür.⁴⁷⁹

TCK 244. maddesinde birden fazla suç tipi düzenlendiğinden, her bir fıkra için ayrı hukuki konu belirlemesi yapılmalıdır. Zira suçun ilk halinden farklı düzenlenmesinin sebebi de verilere müdahale ve sistemin işleyişine müdahale durumunda farklı hukuki yararların ihlal edilmiş olmasıdır. Öncelikle madde gerekçesi incelendiğinde “...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.” denilerek sisteme ve bünyesindeki verilere zarar verilmesinin engellenmesinin amaçlandığı ifade edilmiştir. İzzar fiili, mala zarar verme suçunu ifade ettiğinden, TCK 244. maddesi mala zarar verme suçunun özel bir işleniş şekli olarak düzenlenmek istenmiştir.⁴⁸⁰

Birinci fıkrada bilişim sisteminin doğru ve kendinden beklendiği şekilde işleyişine ilişkin yarar korunmak istenmiştir.⁴⁸¹ Ayrıca gerekçede de ifade edildiği üzere bu suç

⁴⁷⁸ Toroslu/Toroslu, s. 109.

⁴⁷⁹ Yazara göre suçun hukuki konusu bilişim sistemi veya veriler üzerinde hak sahibi kimsenin mülkiyet hakkı ve toplum menfaatidir. Yılmaz, s. 68; Yazarlara göre bu suçla korunmaya çalışılan değerler, bilişim sistemi ve içerisindeki verilerin güvenliği ile mülkiyet hakkıdır. Özbek/ Doğan/ Bacaksız, s. 969: İlk fıkradaki suçun hukuki konusu mülkiyet hakkı, bilişim sisteminin dokunulmazlığı, iletişim kurma ve teknolojik gelişim özgürlüğü; ikinci fıkradaki suçun hukuki konusuysa mülkiyet hakkı, fikri mülkiyet hakkı, özel hayatın gizliliği, ticari sırların korunmasıdır. Parlar, s. 25; Bu suçun hukuki konusu, bilişim suçlarının “Topluma Karşı Suçlar” bölümünde düzenlenmesi sebebiyle “bilişim ortamının oluşturulmasına, geliştirilmesine, sağlıklı, güvenli, güvenilir işleminin sağlanmasına, istenmeyen bir zarara tehlikesinin veya zararın ortaya çıkmasının önlenmesine ilişkin ferdi-kamusal yarardır. Hafizoğulları/ Özen, s. 452; TCK 244/4. maddesiyle korunan hukuki değer “bir bütün olarak malvarlığı”dır Tezcan/Erdem Önok, s. 1166.

⁴⁸⁰ Tezcan/ Erdem/ Önok, s. 1166; Koca, s. 91; Yaşar/ Gökcan/ Artuç, s. 7307.

⁴⁸¹ Akbulut, s. 17.

mala zarar verme suçunun özel bir hali olarak öngörüldüğünden, başka bir deyişle TCK 244. maddesiyle kişinin mal varlığı değerlerine dahil olan bilişim sistemleri ve bu sistemlerdeki verilere müdahale engellenmek istendiğinden, bu maddeyle mülkiyet hakkı da korunmaktadır.⁴⁸² Doktrinde bir görüşe göre⁴⁸³ TCK 244. maddesinin ilk fıkrasında bilişim sistemlerinin işleyişini koruyabilmek için sistemin soyut unsurlarına yönelik saldırılar hüküm altına alınmıştır.⁴⁸⁴ Bu suç her ne kadar mala zarar verme suçunun özel bir işleniş şekli olarak düzenlense de maddeye “*Kişilere Karşı Suçlar*” bölümünde değil de “*Topluma Karşı Suçlar*” bölümünde yer verilmesi göz önünde tutulduğunda, bilişim sistemi ve içindeki verilerin kişilerin mal varlığına dahil bir değer olmasından ziyade toplumun sistemin işleyişine ilişkin menfaati korunmaya çalışılmaktadır.⁴⁸⁵ Kısacası bu suçlarla bilişim sistemlerinin doğru bir şekilde işleyişine ilişkin menfaat korunmaktadır.⁴⁸⁶ Ancak bilişim alanında suçlar düzenlenirken hukuki konuya göre bir ayırım yapılmamıştır. Dolayısıyla burada yazarların iddia ettiği gibi bilişim alanında suçlar sadece bilişim sistemlerini korumak amacıyla bu bölümde ihdas edilmemiş; kanun koyucu bilişim alanında tüm suçlara hukuki konusuna bakmaksızın bu bölümde yer vermiştir. Bu nedenle bu bölümde mal varlığı da korunmak istenmiştir. Dolayısıyla burada tek bir hukuki konudan bahsedilemez.

İkinci fıkra düzenlenen suçun hukuki konusuysa “*veriler üzerinde tasarruf yetkisi olan kişilerin bu verileri (bozulmadan, engel çıkartılmadan, verilere müdahale*

⁴⁸² Ketizmen, s. 128; Yazarlara göre bilişim sistemleri ve içerisindeki veriler, “mal” niteliği taşımadığından bunlara zarar verilmesi halinde bu fiillerin cezasız kalmaması için böyle bir düzenleme yoluna gidilmiştir. Dolayısıyla bu suçlarla korunmaya çalışılan esas değer, mala zarar verme suçunda olduğu gibi mülkiyettir. Tezcan/ Erdem/ Önok, s. 1166.

⁴⁸³ Karşı görüş içi ayrıca bkz.: Bu suçla veriler ve sistem üzerindeki mülkiyetin korunduğu dolayısıyla suçun hukuki konusunun mülkiyet hakkı olduğu görüşüne iştirak etmemekteyiz. Zira korunmaya çalışılan husus mülkiyetten ziyade sistemin işleyişine ve verilerin güvenliğine ilişkin menfaattir. Mülkiyet hakkı dersek sadece sistem ve veri sahiplerinin menfaatinin korunduğu sonucu çıkar fakat bu suçla veri ve sistem üzerinde hak sahibi olan yani tasarruf hakkı bulunan herkesin menfaati korunmaktadır. Akbulut, s. 19.

⁴⁸⁴ Koca, s. 91.

⁴⁸⁵ Kişinin malvarlığına dahil bir değer olan bilişim sistemlerinin doğru ve düzgün işleyişine ilişkin toplumsal yarar da bu suçla korunmuş olduğundan bu suçlar topluma karşı suçlar bölümünde düzenlenmiştir. Koca, s. 91.

⁴⁸⁶ Koca/ Üzülmüş, s. 913.

*olmadan kullanılmasına ilişkin) istediği şekilde, müdahale olmadan kullanmasına ilişkin yararadır”*⁴⁸⁷. Kısacası TCK 244. maddesiyle birden fazla hukuki değer korunmaya çalışılmıştır. Birinci fıkrada bilişim sisteminin işleyişine ilişkin menfaat ve mülkiyet hakkı; ikinci fıkrada verilerin bütünlüğüne ilişkin menfaat korunmaktadır.

B. MADDİ KONU

“Suçun maddi konusu, suçun üzerinde işlendiği kişi veya şeydir”.⁴⁸⁸ Bilişim sistemi ifadesinin kapsamı ve sınırı konusunda kanun metninde veya gerekçede bir belirleme yapılmadığından, ifadenin sistemin hem somut hem soyut unsurlarını mı yoksa sadece soyut unsurlarını mı kapsadığı sorunu ortaya çıkmaktadır.⁴⁸⁹ Yani TCK 244. maddesinde düzenlenen suçun maddi konusuna ilişkin doktrinde tartışma vardır. Bir görüşe göre, birinci fıkrada düzenlenen suçun maddi konusu bilişim sistemidir ancak bilişim sisteminin fiziki unsurlarından ziyade soyut unsurları (program ve yazılımlar) maddi konudur.⁴⁹⁰ Zira maddenin düzenlendiği bölüm göz önünde bulundurulduğunda bilişim sisteminin fiziki varlığına yönelik müdahalelerin mala zarar verme suçuna; sistemin işleyişine yani soyut varlığına yönelik müdahalelerinse TCK 244’e vücut vermektedir. Kısacası 244. maddede bilişim sisteminden ziyade sistemin işleyişi korunma altına alınmıştır.⁴⁹¹ Dolayısıyla bilişim sistemlerinin somut unsurlarına yönelik fiziki zarar verme fiilleri (örneğin sopayla bilgisayarın kırılması) TCK 151. maddeye göre mala zarar verme suçu; sistemin soyut unsurlarına yönelik zarar verici fiillerse (örneğin virüsle sistemin bozulması) TCK 244/1. maddeye göre sisteme müdahale suçunu oluşturacaktır.⁴⁹²

⁴⁸⁷ Akbulut, s. 17.

⁴⁸⁸ Yalçın/Köprülü, s. 157.

⁴⁸⁹ Hafizoğulları/ Özen, s. 452.

⁴⁹⁰ Hafizoğulları/ Özen, s. 453.

⁴⁹¹ Koca, s. 93.

⁴⁹² Yaşar/ Gökcan/ Artuç, s. 7308; Apaydın, Cengiz: Bilişim Sisteminin İşleyişini Engelleme ve Bozma Suçları, **Ceza Hukuku Dergisi**, C. 10, S. 29, 2015, s. 5.

Doktrindeki diğerk görüşe göre TCK 244. maddesinde ihdas edilen suçlarla bilişim sistemlerine ve içerisindeki unsurlara zarar verilmesi fiilleri cezalandırılarak sistemin hem soyut unsurları hem de somut unsurları koruma altına alınmak istenmiştir. TCK 244. maddesinin gerekçesinde de belirtildiği gibi “*Aracın fizik varlığı ve işlemlerini sağlayan bütün diğerk unsurları, söz konusu suçun konusunu oluşturmaktadır.*” Dolayısıyla birinci fıkrada düzenlenen suçun maddi konusu bozulan veya engellenen bilişim sisteminin soyut ve somut tüm unsurları⁴⁹³ olduğundan sistemin somut unsurlara (donanıma) yönelik zarar verici fiiller de TCK 244. maddesi kapsamında değerlendirilmelidir.⁴⁹⁴

Bize göre de gerekçede gerek suçla “*bilişim sistemlerine karşı ızzar fiillerinin özel bir suç haline getirildiği*” gerek suçun maddi konusunun “*aracın fizik varlığı ve işlemlerini sağlayan bütün diğerk unsurlar*” olduğu söylendiğinden, birinci fıkrada düzenlenen suçun maddi konusu bilişim sisteminin soyut ve somut tüm unsurlarıdır.

Bir bilişim sisteminin işleyişinin engellenmesi veya bozulabilmesi için öncelikle işlevini yerine getirebilen bir sistemin varlığı gereklidir.⁴⁹⁵ Bozuk bir bilişim sisteminin işleyişine yönelik engelleme veya bozma hareketlerinin icrası halinde işlenemez suç söz konusu olacaktır.

Doktrinde bir görüşe göre maddenin öngörölme sebebi bilişim sisteminin işleyişine ve verilere zarar verilmesini engellemek olduğundan içerisinde veri olmayan bir bilişim sistemi birinci fıkranın konusunu oluşturamaz. Dolayısıyla birinci fıkrada düzenlenen suçun konusu içerisinde veri barındıran bilişim sistemidir.⁴⁹⁶ Ancak içerisinde veri barındırmayan bir bilişim sistemi düşünülemez zira bilişim sisteminin

⁴⁹³ Özbek/ Doğan/ Bacaksız, s. 971; Yazarlara göre suçun konusu bilişim sisteminin işleyişidir. Koca/ Üzülmöz, s. 914; Meran, s. 571; Kurt, s. 162.

⁴⁹⁴ Parlar, s. 24; Parlar/ Hatipoğlu, s. 3475; Soyaslan, s. 698; Orta, s. 117; Yazıcıoğlu, s. 260.

⁴⁹⁵ Yazarlara göre bu suç ancak soyut unsurlara yönelik zarar verici fiiller aracılığıyla gerçekleştirilebilir. Somut unsurlara yönelik zarar verici fiiller mala zarar verme suçuna vücut verecektir. Koca/ Üzülmöz, s. 916.

⁴⁹⁶ Soyaslan, s. 700.

işlemesini sağlayan yazılım ve programlar da verilerden oluşur. Dolayısıyla bu görüşe katılmak mümkün değildir.

İkinci fıkranın maddi konusuysa bozulan, yok edilen, değiştirilen veya erişilmez kılınan, sisteme yerleştirilen, başka yere gönderilen verilerdir.⁴⁹⁷ Ancak sistemin her bir unsuru verilerden oluştuğundan veri kavramı kapsam itibarıyla çok geniştir. Bilişim sistemindeki bir yazılım programının silinmesi de verilerin silinmesi olduğundan TCK 244/2. maddesinde yasaklanan sistemin unsurunu oluşturmayan verilerdir.⁴⁹⁸ Şayet sistemin unsurunu oluşturan bir veri silinirse artık burada sistemin işleyişine yönelik bir müdahale söz konusu olduğundan TCK 244/1. maddesindeki eylemin gerçekleştiği kabul edilmelidir. Kısacası TCK 244/2. maddesinde maddi unsur, sistemin unsuru olmayan verilerdir. Bu veriler, kişisel veri niteliğinde olabileceği gibi ekonomik değer de olabilir.⁴⁹⁹

Doktrinde tartışmalı diğer bir konuysa veri taşıma araçlarında bulunan verilerin, ikinci fıkradaki suçun maddi konusu olup olamayacağına ilişkindir. Bir görüşe göre ikinci fıkrada düzenlenen suçun maddi konusu muhakkak sistemde mevcut olan verilerdir. Dolayısıyla tek başına bilişim sistemi sayılmayacak USB, CD, disket gibi sadece veri depolayabilen araçlarda saklanan verilere müdahale edilmesi bu suça vücut vermeyecektir.⁵⁰⁰ Bu araçlara verilere ulaşılmasının engellenmesi amacıyla zarar verilmesi TCK 244. maddesini değil; TCK 151. maddesini (mala zarar verme) oluşturacaktır.⁵⁰¹ Başka bir görüşse veri taşıma cihazlarındaki verilerin bu suçun konusunu oluşturmayacağını ancak veri taşıma cihazının bir bilişim sistemine takılması

⁴⁹⁷ Koca/ Üzülmmez, s. 914; Meran, s. 571; Yaşar/ Gökcan/ Artuç, s. 7308; Apaydın, s. 8.

⁴⁹⁸ Özbek/ Doğan/ Bacaksız, s. 969.

⁴⁹⁹ Akbulut, s. 15.

⁵⁰⁰ Koca/ Üzülmmez, s. 914; Ketizmen, s. 143; Tezcan/ Erdem/ Önok, s. 1167; Veri taşıma aracındaki verilere zarar vermek amacıyla bu cihazlara zarar verilmesi durumunda mala zarar verme suçu oluşacaktır. Koca, s. 94.

⁵⁰¹ Koca/Üzülmmez, s. 914; Tezcan/ Erdem/ Önok, s. 1167.

durumunda artık cihaz bilişim sisteminin bir unsuru haline geleceğinden cihazdaki verilerin de bu suçun maddi konusu olabileceğini savunmaktadır.⁵⁰²

Karşı görüşe göreyse bilişim sistemleri farklı unsurların bir araya gelmesiyle oluştuğundan, sistem içerisinde bulunan veri kavramından sadece sistemin hafızasında bulunan veriler anlaşılmalıdır; veri taşıma cihazlarında saklanan veriler de anlaşılmalıdır.⁵⁰³ Hakeza TCK 244. maddesinin esas alındığı AKSSS'nin 4. maddesinde “veriye müdahale” suçunun oluşumu açısından, verinin bilişim sisteminde veya veri taşıma aracında olması önemli değildir. Veri taşıma aracında olan bir veriye müdahale teşkil eder nitelikteki eylemler de bu suç kapsamında değerlendirilmektedir.⁵⁰⁴ Bizce de veri taşıma araçlarında bulunan verilerin maddenin koruma kapsamından çıkarılması, maddenin amacı ile bağdaşmadığından veri taşıma araçlarındaki veriler de TCK 244/2. maddesindeki suçun maddi konusu olabilecektir.

TCK 244/3. maddesinde suçun “*bir banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinde işlenmesi*” cezayı ağırlaştırıcı sebep olarak öngörülmüştür. Dolayısıyla buradaki maddi konu banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi veya bu sistemin ihtiva ettiği verilerdir.

C. FAİL

Sisteme müdahale veya verilere müdahale suçlarının işlenebilmesi için failin herhangi bir statüde veya niteliğinin olması aranmadığından, bu suçu herkes işleyebilir.⁵⁰⁵ Fiilin bilişim sistemine mi sistemdeki verilere mi yönelik olduğunun tespiti failin belirlenebilmesi için elzemdir.⁵⁰⁶ Nitekim bilişim sistemi üzerinde hak sahibi kimseyle

⁵⁰² Erdoğan, s. 210-211.

⁵⁰³ Akbulut, s. 27.

⁵⁰⁴ Ketizmen, s. 114.

⁵⁰⁵ Özbek/ Doğan/ Bacaksız, s. 972; Koca/ Üzülmüş, s. 913; Meran, s. 570; Parlar, s. 25; Apaydın, s. 7.

⁵⁰⁶ Apaydın, s. 7.

sistemdeki veriler üzerinde hak sahibi kimse her zaman aynı kişi olmayabileceğinden, suç teşkil eden fiil bilişim sistemi üzerinde hak sahibi kimse tarafından sistemdeki veriler üzerinde hak sahibi kimseye karşı işlenebileceği gibi sistemdeki veriler üzerinde hak sahibi kimse de bilişim sistemi sahibine karşı bu suçu işleyebilir. Dolayısıyla suçun faili sistem veya veri üzerinde hak sahibi olmaksızın sisteme veya verilere müdahale eden kişi ya da kişilerdir.

Sistem veya veri üzerinde hak sahibi olan kişiden bahsedildi. Hak sahipliği geniş bir ifadedir sadece mülkiyet hakkını içermez. Bu sebeple kimlerin hak sahibi olduğunun tespit edilmesi gerekir. Hak sahipliği kavramının içerisine sistem sahibi, veri sahibi, bunlar üzerinde tasarruf hakkı verilmiş kişiler girer.

Bilişim sistemini veya içerisindeki verileri kullanım hakkının verildiği kişileri, kendilerine verilen kullanım yetkisi bağlamında değerlendirmek gerekecektir çünkü kullanım hakkı kapsamında her türlü tasarrufu yapmasına izin verilmemiş olabilir. Ayrıca sistem sahibinin, veri sahibinin ve tasarruf hakkı olan kişilerin belirlenmesi TCK 244. maddesinde belirtilen suçların işlenip işlenmediğinin; işlendiyse fail ve mağdur kim olduğunun tespiti bakımından önemlidir.⁵⁰⁷ Yani sistem sahibi de suçun kanuni tanımındaki unsurları gerçekleştirmesi halinde, sistemi kullanma hakkına sahip kişiye karşı TCK 244. maddesini işlemiş sayılabilir. Aynı şekilde sistemi kullanan kişi de sistem veya veri sahibine karşı bu suçu işlemiş olabilir.

Burada bilişim sisteminin mülkiyetiyle kullanım hakkının farklı kişilere ait olması durumunda, sistem ve veriler üzerindeki tasarruf yetkisi hak sahibi kişiler arasındaki hukuki ilişkiye göre tespit edilir. Sistem sahibinin kendi sistemine ve verilerine yönelik maddede geçen hareketleri işlemesi, bu suça vücut vermez. Ancak sistem sahibi, sistemi veya veriyi kullanması için başkasına yetki vermişse sisteme veya veriye verdiği zarar

⁵⁰⁷ Akbulut, s. 19; Soyaslan, s. 699.

TCK 244. maddesine vücut verecektir.⁵⁰⁸ Sistemle ilgili sınırlı bir yetki verildiğinde bu yetki dışında sisteme müdahale ya da verilere müdahale edilmesi yine TCK 244. maddedeki suçu oluşturacaktır.

Tüzel kişiler TCK 20. maddesi gereği suçun faili olamaz ancak bu suçla tüzel kişi yararına haksız menfaat sağlanması durumunda TCK 246. maddesi gereği TCK 60. maddesindeki güvenlik tedbirleri tüzel kişiler hakkında uygulanabilir.⁵⁰⁹

Bu suç özgü suç olarak öngörülmemiş ancak kamu görevlileri, banka ve kredi kurumu çalışanları için cezayı ağırlaştırıcı neden öngörülerek nitelikli hal bakımından özgü suç yaratılabilirdi. Zira sayılan kimseler kurum bilgisayarlarına rahatlıkla erişim sağlayabildiğinden TCK 244. maddesini ihlal etmeleri daha kolay olacaktır.⁵¹⁰

D. MAĞDUR

Suçun mağduru, *suçla zarara uğratılan veya tehlikeye maruz bırakılan hak veya yararın sahibidir.*⁵¹¹ Doktrinde bir görüşe göre, suçun Topluma Karşı Suçlar bölümünde düzenlenmesiyle güvenli bilişim ortamı yaratılması amaçlandığından kamu menfaati korunmaya çalışılmıştır. Dolayısıyla suçun mağduru kamu idaresidir; kişilerse ancak suçtan zarar gören olabilir.⁵¹² Ancak ilk bölümde de ifade edildiği üzere bilişim suçları, düzenlendiği bölümden bağımsız değerlendirilmelidir.

Suçun mağduru suç teşkil eden fiille ihlal edilen; ceza normuyla korunan menfaat veya değer sahibi olduğundan suçun mağdurunun tespiti, suçun hukuki konusundan yola çıkarak yapılmalıdır.⁵¹³ Birinci fıkrada bilişim sisteminin işleyişine ilişkin menfaat kime aitse suçun mağduru o kimsedir. İkinci fıkradaysa verilerin bütünlüğüne ilişkin

⁵⁰⁸ Akbulut, s. 20.

⁵⁰⁹ Tezcan/ Erdem/ Önok, s. 1166.

⁵¹⁰ Erdoğan, s. 197.

⁵¹¹ Dönmezer/ Erman, s. 726.

⁵¹² Hafizoğulları/ Özen, s. 452.

⁵¹³ Tuğrul Katoğlu, s. 660-661.

menfaat sahibi kimse suçun mağduru o kimsedir. Yani TCK 244. maddesinin birinci fıkrasında düzenlenen suçun mağduru işleyişine müdahale edilen sistem üzerinde hak sahibi kimseyken; ikinci fıkrada düzenlenen suçun mağduru müdahale edilen veriler üzerinde hak sahibi kimse veya kimselerdir.⁵¹⁴

Sisteme müdahale suçu açısından mağdur bozulan ya da engellenen sistem üzerindeki hak sahibi kişi olduğundan, bu kimse doğrudan sistemin sahibi olabileceği gibi sistemin kullanıcısı ya da işleticisi olabilir.⁵¹⁵ Verilere müdahale suçu açısından mağdur *“bozulan, yok edilen, değiştirilen, erişilmez kılınan, başka yere gönderilen ya da yerleştirilen veriler”* üzerinde hak sahibi kimsedir. Burada vurgulanması gereken nokta mağdurun verilerin ilgili olduğu kişilerin değil; bu veriler üzerinde tasarruf yetkisi bulunan kişiler olduğudur.⁵¹⁶ Yani verilerin hakkında olduğu kişiler suçun mağduru değil ancak suçtan zarar görendir.

Bilişim sistemi veya veriler üzerinde birden fazla kişinin hak sahibi olması durumunda birden fazla mağdur vardır.⁵¹⁷ Ancak örneğin sistemin engellendiği veya bozulduğu durumda, başka bir kimsenin sistemde dosyasının bulunması halinde bu suçun mağduru sistem sahibinin kendisidir. Sistemde dosyası bulunan kimse ise ancak suçtan zarar gören sayılabilir. Bilişim sisteminin başkasına, sistemdeki verilerin başkasına ait olması durumunda bu verilerin bozulması, yok edilmesi, değiştirilmesi halinde TCK 244/2. maddesi bakımından mağdur verilerin sahibidir. Çünkü suçla veri sahiplerinin menfaatleri korunmaya çalışılmıştır. Dolayısıyla suçun mağduru da veri sahipleridir.

Veriler soyut kavramlar olduğundan ve bu kavramlar klasik anlamda eşya teşkil etmediklerinden, veriler üzerinde hak sahibinin kim olduğu sorunu ortaya çıkmaktadır.⁵¹⁸

⁵¹⁴ Kurt, s. 163; Yaşar/ Gökcan/ Artuç, s. 7307; Meran, s. 570; Koca/ Üzülmüş, s. 913-914.

⁵¹⁵ Akbulut, s. 21.

⁵¹⁶ Akbulut, s. 21.

⁵¹⁷ Yazarlara göre bir kimsenin banka hesabına girilip oradaki bilgilerin silinmesi durumunda hem banka hem hesap sahibi mağdurdur. Yaşar/ Gökcan/ Artuç, s. 7308.

⁵¹⁸ Akbulut, s. 21.

Veriler üzerinde hak sahibi kimse, verilerin ilgili oldukları kişiler olmadığından tasarruf yetkisi sahibi mülkiyet ilişkisine bağlı belirlenmemektedir.⁵¹⁹ Veriler üzerinde hak sahibi kişinin tespit edilmesi noktasında farklı ölçütler ileri atılmıştır. Farklı yazarlar tarafından verileri hukuka uygun iktisap eden, verilerin ilgili olduğu kimseler, veri taşıyıcısının sahibi, veriler üzerinde fikri hak sahibi (ilgilisi dikkate alınmaksızın verileri üreten kimse), verileri kaydeden veya nakleden kimsenin tasarruf yetkilisi olduğuna dair görüşler ortaya atılmıştır.⁵²⁰ Ancak veriler üzerinde tasarruf yetkisine sahip kişinin tespitinde bu ölçütlerin hiçbirisi tek başına yeterli olmadığından ölçütler bir arada değerlendirilerek tespitte bulunulmalıdır.⁵²¹

Veri üzerinde hak sahibi kişi belirlenmesi noktasında net bir ölçüt vermek yerine somut olaya göre değerlendirme yapılması daha doğru bir çözüm olacaktır. Zira her durumda veri üzerinde hak sahibi kimse sistem sahibi veya verileri işleyen veya verinin ilgilisi olmamaktadır. Dolayısıyla veriler üzerinde hak sahibi kimse doğrudan bilişim sisteminin sahibi olabileceği gibi sistem sahibiyle aralarındaki hukuki ilişkiye dayalı sistemi kullanan bir kimse de olabilir.

TCK 244/3. maddesinde ilk iki fıkrada sayılan “*fiillerin bir banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinde işlenmesi*” düzenlenmiştir. Bu fıkra göre mağdursa sistem sahibi banka veya kredi kurumu ya da kamu kurum veya kuruluşunun tüzel kişiliğidir.⁵²² Bu sistemlerdeki verilerin ilgilisiye suçtan zarar görendir.

⁵¹⁹ Akbulut, s. 21.

⁵²⁰ Akbulut, s. 22.

⁵²¹ Akbulut, s. 22.

⁵²² Doktrinde bazı yazarlar tüzel kişilerin suçun mağduru olabileceğini kabul etmemektedir. Ancak gerçek kişilerin mağdur olabileceğini savunan bu yazarlara göre bu suçun mağduru toplumu oluşturan herkes; tüzel kişiler ise suçtan zarar görendir. Akbulut, s. 21; Tüzel kişiler ancak suçtan zarar gören olabilir. Suçun mağduru tüzel kişiyi oluşturan gerçek kişilerdir. Suçun devlete ait bir kurumun bilişim sistemine karşı işlenmesi halinde toplumu oluşturan herkes mağdurdur. Koca/ Üzülmez, s. 914.

Lisans sözleşmesi gereği satılan kullanım programlarının veya yazılımların ele geçirilmesinde kimin mağdur olduğu sorunu ortaya çıkabilir. Hukuka aykırı olarak programların kopyalanması veya elde edilen yazılımın kullanılması halinde mağdur programı satın alıp kullanan kimse midir; yoksa bunu üretilip pazarlayan kimse midir sorusu ortaya çıkabilir. Kanaatimizce ceza normuyla korunmaya çalışılan esas değer kime aitse bu fiil bakımından mağdur o olacaktır. Hem kullanan hem de bunu üretilip satan, duruma göre ayrı ayrı veya beraber bu suçun mağduru olabilirler.⁵²³

E. SUÇUN UNSURLARI

a. MADDİ UNSUR

1. Genel Olarak

Suçun maddi unsuru fiildir. Fiilsiz suç olmaz ilkesi gereğince bir suçtan bahsedilebilmesi için ortada insana izafe edilebilen bir fiil olması gerekir.⁵²⁴ Fiil de neticeli suçlar bakımından “*hareket, netice ve bu ikisi arasındaki nedensellik bağı*” olmak üzere üç alt unsura sahiptir. Ancak bütün suçlar neticeli olmadığından, netice ve nedensellik bağı fiilin zorunlu unsuru olmayıp sırf hareket suçları da denilen neticesiz suçlar bakımından hareket suçun maddi unsurunu teşkil etmektedir.⁵²⁵

Kanun koyucu bilişim sistemine ve sistemdeki verilere müdahale niteliğindeki hiçbir fiilin cezasız kalmaması amacıyla TCK 244. maddesinde düzenlenen suçun fiil unsurunu olabildiğince geniş kapsamlı düzenlemeye çalışmış ancak bu durum suçun fiil unsuru olarak düzenlenen bazı hareketlerin birbirinden ayırt edilmesini zorlaştırmıştır.⁵²⁶

TCK 244. maddesinde iki ayrı fıkarda, iki suç için tipik fiiller öngörülmüştür. “*Bilişim sisteminin işleyişini engelleme veya bozma*” ve “*bilişim sistemindeki verileri*

⁵²³ Yazıcıoğlu, s.232.

⁵²⁴ Hafizoğulları/ Özen, Genel Hükümler, s. 167.

⁵²⁵ Hafizoğulları/ Özen, Genel Hükümler, s. 168.

⁵²⁶ Taşkın, s. 49-50.

bozma, yok etme, deęiřtirme veya eriřilmez kılma, sisteme veri yerleřtirme, var olan verileri bařka bir yere gnderme” suun kanuni tanımındaki hareketlerdir. İncelemenin daha rahat ve sistematik bir řekilde yapılabilmesi iin her bir hareket ayrı ayrı aıklanacaktır.

2. Sisteme Ynelik Hareketler

a. Genel Aıklamalar

TCK 244. maddesinin ilk fıkrasında tipik hareket olarak “biliřim sisteminin iřleyiřini engelleme veya bozma” ngrlmřtr. Biliřim sisteminin iřleyiřine mdahale suunun, seimlik hareketli bir su mu serbest hareketli bir su mu olduęu konusunda doktrinde tartiřma vardır. Bir grř bu suun serbest hareketli bir su olduęunu; suun kanuni tanımında yazılı engelleme ve bozmanın aslında hareket deęil netice olduęunu dolayısıyla aslında bu su bakımından belirli bir hareket unsuruna yer verilmedięinden, engelleme ve bozma neticelerini meydana getirmeye elveriřli her trl hareketle bu suun iřlenebileceęini savunmaktadır.⁵²⁷ Dięer grřse bu suun seimlik hareketli olduęunu; suun sistemin iřleyiřini engelleme veya bozma hareketleriyle gerekleřtirilebileceęini savunmaktadır.⁵²⁸ Biz de bu suun seimlik hareketli bir su olduęu grřne iřtirak etmekteyiz. Zira suun kanuni tanımında ngrlen hareketler netice olarak deęerlendirilemez.

Biliřim sisteminin iřleyiřine mdahale suu seimlik hareketli bir su olarak ngrldęnden, engelleme veya bozma hareketlerinden bir tanesinin ya da her ikisinin yapılmasıyla bu su gerekleřmiř olacaktır.⁵²⁹ Hareketlerden her ikisinin iřlendięi

⁵²⁷ Erdoęan, s. 186.

⁵²⁸ Karaglmez, s. 187.

⁵²⁹ Aynı ynde grř iin bkz. Parlar, s. 25; Erdaę, s. 289; Ketizmen, s.128-129; Koca, s. 93. Suun serbest hareketli olduęunu iddia eden grř iin bkz. Koca/ zlmez; Akbulut, s. 27; Hocalar neticeyi gerekleřtirmeye elveriřli her trl hareketle bu suun iřlenebileceęini savunmaktadır.

durumda tek bir suç söz konusu olacak ancak bu durum cezanın belirlenmesinde göz önünde tutulacaktır.⁵³⁰

“Bilişim sisteminin işleyişinin engellenmesi veya bozulması suçu” icrai hareketle ya da ihmal suretiyle de gerçekleştirilebilir.⁵³¹ Örneğin bilişim sisteminin çalışabilmesi için sisteme yüklenmesi gereken bir programın, görevli kimse tarafından yüklenmemesi durumunda bilişim sisteminin işleyişi ihmali hareketle engellenmiş olmaktadır.

Doktrinde bazı yazarlar “sistemin işleyişinin engellenmesi veya bozulması” suçunun, kanuni tanımında bir neticeye yer verilmediğinden bu suçun neticesiz bir suç olduğunu savunmaktadır.⁵³² Ancak doktrinde suçun kanuni tanımında belirtilen sistemin işleyişinin engellenmesi veya bozulmasının aslında suçun neticeleri olduğunu dolayısıyla bu suçun neticeleri meydana getirmeye elverişli her türlü hareketler işlenebileceğini ileri süren görüşler de vardır.⁵³³ Bu görüşe göre bu suç neticeyi meydana getirmeye elverişli her türlü hareketle işlenebildiğinden serbest hareketli bir suçtur.⁵³⁴

Bilişim sisteminin işleyişine müdahale suçunun zarar suçu mu tehlike suçu mu olduğu hususunda da doktrinde tartışma vardır. Zarar suçu olarak değerlendiren bir görüşe göre gerçekleştirilen bozma veya engelleme hareketleri sonucu sistemin normalde yerine getirdiği işleyiş artık yerine getirilemediğinden, ortada bir zarar vardır ve bu zarar neticedir.⁵³⁵ Zarar suçu olduğunu düşünen diğer görüşse bu suçun hangi hareketlerle işleneceğinin belirtilmediğini ancak kanuni tanımda belirtilen engelleme ve bozmanın suçun neticeleri olduğunu, buradan hareketle bu suçun zarar suçu olduğunu

⁵³⁰ Koca, s. 93.

⁵³¹ Erdoğan, s. 185.

⁵³² Özbek/ Doğan/Bacaksız, s. 975.

⁵³³ Yazar sistemin işleyişinin engellenmesi ve bozulmasını suçun neticesi olarak nitelendirdiğinden maddeyi biçimsel kanunilik ilkesi bakımından sakıncalı bulmaktadır. Zira suçun hangi hareketlerle işlenebileceği öngörülmemiştir. Dolayısıyla suçun hangi fiillerle işlenebileceğinin belirlilik ilkesinin gerçekleştirilebilmesi için belirtilmesi gerekmektedir. Akbulut, s. 51. Koca/ Üzülmmez, s. 915.

⁵³⁴ Koca/ Üzülmmez, s. 915; Akbulut, s. 27.

⁵³⁵ Yaşar/ Gökcan/ Artuç, s. 7309.

savunmaktadır.⁵³⁶ Tehlike suçu olduğunu düşünen yazarlarsa bu seçimlik hareketler neticesinde bir zararın doğması ihtimal dahilinde olsa da suçun oluşması için mutlaka bir zararın doğması gerekmediğini, aksi halde yani hareketin gerçekleştirilmesi sonucu bir zararın doğmasının aranmasının suçun uygulama alanını daraltacağını dolayısıyla bu suçun tehlike suçu olduğunu ileri sürmektedir.⁵³⁷ Yazarlara göre “*sistemin işleyişinin engellenmesi veya bozulması*” sonucu bilişim sisteminin veri işlem ve iletişim yapamaması suçun işlenmiş olması için yeterli olduğundan bu suç neticesiz bir suçtur.⁵³⁸

Suçun kanuni tarifinde yazan engelleme veya bozma hareketi sonucu bilişim sistemi kendinden beklenen şekilde çalışamaz hale gelmektedir. Dolayısıyla tipik hareketlerin işlenmesiyle dış dünyada bir değişiklik meydana getirildiğinden bu suç neticeli bir suçtur. Ancak burada suçun neticesi iddia edildiği gibi madde metninde yazan bilişim sisteminin işleyişini engelleme veya bozma değil; sistemin işlevsiz hale gelmesidir. Sistemin işleyişinin engellenmesi veya bozulması suçun kanuni tanımındaki hareketlerdir. Doktrinde sisteme müdahale olarak adlandırılan bu suç sistemin işleyişinin engellenmesi veya bozulması şeklinde icra edilebileceğinden bu suç seçimlik hareketli bir suçtur.

“*Bilişim sisteminin işleyişinin engellenmesi veya bozulması*” sonucu, suçun maddi konusu üzerinde bir zarar meydana gelmektedir. Nitekim bilişim sistemi artık faaliyet gösteremez bir hal almaktadır. Bu hareketler sonucu sistem geri dönülmez bir şekilde işlevsiz hale getirilebileceği gibi sistemin eski haline getirilmesi için çaba sarf edilmesi gerekebilir. Her iki durumda da maddi konu olan bilişim sistemi üzerinde bir zarar meydana gelmiştir. Kısacası bilişim sistemine müdahale suçu zarar suçudur.

⁵³⁶ Erdoğan, s. 187.

⁵³⁷ Pallı, s. 169; Hafizoğulları/ Özen, s. 453.

⁵³⁸ Meran, s. 572.

Her iki seçimlik hareket bakımından bu suç ani hareketli bir suçtur. Doktrinde bir görüş TCK 244. maddesindeki seçimlik hareketlerin süreklilik teşkil edecek şekilde işlenmesi durumunda bu suçun mütemadi nitelik kazandığını ileri sürmüştür. Örneğin elektriğin kesilmesi veya veri taşıma aracının saklanması durumlarında fiil belli bir süre devam etmektedir.⁵³⁹ Bu durumda suç hareketin gerçekleştirilmesiyle işlenmiş sayılmakta ancak tamamlanmamaktadır, zamanaşımı hesabında da suçun kesintiye uğradığı an esas alınmalıdır.⁵⁴⁰ Ancak bu görüşe katılmak mümkün değildir. Zira verilen örneklerde işlenen fiilin etkisinin devam ediyor olması bu suçu mütemadi hale getirmez. Sistemi engelleme veya bozma hareketinin etkisinin belli bir süre devam ediyor olması suçu mütemadi suç yapmaz.⁵⁴¹

“Bilişim sisteminin işleyişinin engellenmesi veya bozulması”, temelde sistemin veri işleme faaliyetinin engellenmesi veya bozulmasıdır.⁵⁴² Doktrindeki bir görüşe göre “bilişim sisteminin işleyişinin engellenmesi veya bozulması”, sistemin somut unsurlarına verilen zararların, soyut unsurların işleyişini engellemesi veya bozması durumunda değil; bilişim sisteminin soyut unsurlarına yönelik zarar verici fiiller sonucu somut unsurların işlevsiz kalması halinde söz konusu olur.⁵⁴³ Sistemin yazılım unsurlarına yönelik yani veri işlemeye yönelik fiiller sistemin işleyişini bozmuş veya engellemişse TCK 244. maddesi kapsamında değerlendirilecek; sisteme yönelik fiziki müdahaleler neticesinde sistemin işleyişinin engellenmesi veya bozulması durumundaysa mala zarar verme suçu söz konusu olacaktır.⁵⁴⁴ Örneğin donanım unsurlarından olan sistem anakartına, sabit diskine zarar verilmesi sonucu sistem kendinden beklendiği gibi çalışamazsa bu fiil mala zarar verme suçu içerisinde değerlendirilecektir.⁵⁴⁵ Bu görüşe göre TCK 244. maddesi

⁵³⁹ Erdoğan, s. 185.

⁵⁴⁰ Taşkın, s. 54.

⁵⁴¹ Hafızogulları/ Özen, s. 453.

⁵⁴² Ketizmen, s. 129.

⁵⁴³ Koca/ Üzülmüş, s. 916.

⁵⁴⁴ Ketizmen, s. 133; Erdağ, s. 289-290.

⁵⁴⁵ Ketizmen, s. 135.

olmasaydı dahi sistemin işleyişinin bozulması mala zarar verme suçu içerisinde mütalaa edilecekti zira mala zarar verme suçu açısından sistemin işlev göremez hale getirilmesinin fiziksel bir müdahale veya verilere yönelik bir müdahaleyle olması suçun oluşması bakımından önemli değildir. Dolayısıyla bilişim sisteminin işleyişinin bozulmasına TCK 244/1. maddesinde ayrıca yer verilmesi de bu hükmün fiziksel müdahalelerden ziyade yazılım unsurlarına yönelik müdahaleyi kapsadığını kanıtlamaktadır.⁵⁴⁶

Doktrinadaki başka bir görüşe göreyse suçun kanuni tanımında hareket bilişim sisteminin işleyişinin engellenmesi veya bozulması olarak tanımlandığından hareketin bilişim sisteminin soyut unsuru olan yazılım unsuruna yönelik olması gerekir ancak sistemin işleyişinin engellenmesi veya bozulması donanım unsurlarına yönelik fiziki bir müdahaleyle de gerçekleştirilebilir.⁵⁴⁷ Donanım unsurlarına yönelik fiziki müdahalelerle sistemin işleyişinin engellenmesi veya bozulması durumu mala zarar verme suçu niteliğindeyken yazılıma yönelik hareketlerle donanım unsurlarının işlevsiz kılınması TCK 244 kapsamında mütalaa edilmelidir.⁵⁴⁸ Mala zarar verme suçundan bu suçun ayırmak için dikkat edilmesi gereken konu, failin sistemin donanım unsurlarını bir mal varlığı değeri olarak düşünerek müdahalede bulunmayıp; sistemin işleyişine müdahale etmek için donanım unsurlarına fiziki müdahalede bulunup bulunmadığıdır.⁵⁴⁹ Suçun maddi konusu kısmında açıkladığımız üzere, biz de bu suçun hem somut hem soyut unsurlara müdahale şeklinde gerçekleştirilebileceği düşüncesine iştirak etmekteyiz. Yargıtay'ın da bu yönde kararları mevcuttur.⁵⁵⁰

⁵⁴⁶ Ketizmen, s. 136.

⁵⁴⁷ Açıkgöz, s. 81-82.

⁵⁴⁸ Açıkgöz, s. 81.

⁵⁴⁹ Açıkgöz, s. 82.

⁵⁵⁰ “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 Türk Ceza Kanununun 525/b-1 maddesindeki “bilişim sistemini engellemek veya yanlış biçimde çalışmasını sağlamak suretiyle yarar sağlamak suçuna uygun bulunduğu gözetilmeden yazılı şekilde 765 sayılı Türk Ceza Kanununun 525/b-2 maddesinden hüküm kurulmak suretiyle eksik ceza tayini” Yargıtay 11. CD. E. 2010/6346, K. 2012/3544. Yaşar/ Gökcan/ Artuç, s. 7334.

b. Bilişim Sisteminin İşleyişini Engelleme

Bilişim sisteminin işleyişinin engellenmesi, sistemin kendisinden beklediği şekilde işlevini yerine getirmesinin kısmen veya tamamen önlenmesidir.⁵⁵¹ Sistemin engellendiği durumda, sistem bozulmamakta ancak kendisinden beklenen fonksiyonları yerine getirmesi önlenmektedir.⁵⁵² Bu önleme sistemin tamamen işlevsiz hale getirilmesi şeklinde olabileceği gibi sistemin faaliyet ve kapasitesinin sınırlandırılması şeklinde olabilir.⁵⁵³ Doktrinde bir görüşe göre bilişim sisteminin işleyişinin yavaşlatılması durumunda da sistemin engellenmesi söz konusudur.⁵⁵⁴ Ancak bilişim sisteminin işleyişinin yavaşlatıldığı durumda, sistemin işleyişi engellenmediğinden bu suçun gerçekleştiğinden bahsedilemez.⁵⁵⁵

Sistemin işleyişinin engellenmesi; veri işlem ve veri iletişimi yapılmasının önlenmesi yani sisteme veri girilmesine, verilerin saklanmasına ve işlenmesine, bu verilerden sonuç çıkarılmasına veya veri aktarımına mâni olunmasıdır.⁵⁵⁶ Birinci fıkrada sistemin işleyişinin engellenmesi ve bozulması ayrı seçimlik hareketler olarak öngörüldüğünden engelleme seçimlik hareketi bakımından sistemin çalışamaz duruma gelmemesi gerekir.⁵⁵⁷ Sistemin işleyişinin engellenmesi seçimlik hareketi bakımından suçun oluşumu için engellemenin kısa süreli veya uzun süreli olması fark yaratmaz.⁵⁵⁸

Bilişim sisteminin işleyişinin engellenmesi, sistemin somut unsurlarına yönelik fiziki bir müdahaleyle olabileceği gibi sistemin soyut unsurlarına yani yazılım veya

⁵⁵¹ Özbek/ Doğan/ Bacaksız, s. 973.

⁵⁵² Kurt, s. 164; Koca/ Üzülmmez, s. 915; Yaşar/ Gökcan/ Artuç, s. 7309.

⁵⁵³ Kurt, s. 161; Erdoğan, s. 189.

⁵⁵⁴ Kurt, s. 162.

⁵⁵⁵ Akbulut, s. 28.

⁵⁵⁶ Akbulut, s. 27; Koca/ Üzülmmez, s. 916; Yaşar/ Gökcan/ Artuç, s. 7309; Parlar, s. 25.

⁵⁵⁷ Açıkgöz, s. 80.

⁵⁵⁸ Açıkgöz, s. 80.

programlarına yönelik bir müdahaleyle de gerçekleştirilebilir.⁵⁵⁹ Nitekim kanun koyucu sistemin işleyişinin engellenmesinin sadece soyut unsurlara yönelik hareketlerle işlenebileceğini kabul etseydi bunu AKSSS 5. maddede⁵⁶⁰ belirtildiği gibi düzenlerdi. Böyle sınırlayıcı bir ifade 244. maddede bulunmadığından sistemin işleyişinin engellenmesi amacıyla sistemin soyut veya somut unsurlarına yönelik her türlü engelleme hareketi 244/1 kapsamındadır.⁵⁶¹

Bilişim sisteminin işleyişini engellemek çok farklı şekillerde gerçekleştirilebilir. Örneğin “*sisteme yoğun elektro manyetik dalgaların gönderilerek sistem merkezinin etkilenmesini sağlamak ya da sisteme müdahale edilerek işletim sisteminin geçici süre devre dışı bırakılması*”, “*bilişim sistemi hiç kullanılmaksızın bir iç ağda (intranet) bilgisayarları birbirine bağlayan kabloların kesilmesi, sisteme virüs gibi zararlı bir yazılımın bulaştırılması, sistem şifresinin değiştirilmesi*”⁵⁶² bilişim sisteminin kullanıcıdan çalmak, gizlemek gibi fiillerle alınması, şifresiz sisteme şifre konması, sistemin kitlenmesi⁵⁶³ sistemin elektriğini kesme, sistemden donanıma ait bir parçanın çıkarılması şeklinde işlenebilir.⁵⁶⁴

⁵⁵⁹ Ergün, s. 92-93; Akbulut, s. 28; Suçun maddi konusunun bilişim sistemlerinin fiziki varlığı olabileceğini kabul etmeyen yazarlar sistemin somut unsurlarına yönelik zarar verici filleri TCK 151 kapsamında değerlendirmektedir. Koca/ Üzülmüş, s. 916.

⁵⁶⁰ AKSSS 5. Madde- Sisteme Müdahale

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 suç olarak tanımlanması için gerekli olabilecek yasama tedbirlerini ve diğer tedbirleri kabul edecektir.

⁵⁶¹ “*Alman Ceza Kanununun 303/b maddesinde de veri işlem tesisine veya veri taşıyıcısına müdahalelerin de bilgisayar sabotajını oluşturacağı kabul edilmiştir. Bizim kanunumuz hareketleri tek tek saymayarak sadece neticeye yer vererek geniş belirleme yapmıştır. Ancak bu düzenleme kanunilik ilkesi açısından sorun doğuracak niteliktedir. Zira kanunilik ilkesinin sonuçlarından biri olan belirlilik ilkesi, haksızlık teşkil eden fiilin tam ve özenli bir dille anlatılmasını istemektedir. Sınırları belirli olmayan hükümlerden oluşan normların, geniş yorumlama imkânı veren kavramların varlığı, belirlilik ilkesine aykırıdır. Siber Suç Sözleşmesinde veya Alman Ceza Kanunun 303 b maddesinde olduğu gibi bilişim sisteminin işleyişinin engellenmesi veya bozulmasının hangi fiillerle gerçekleştirileceğinin açıklığa kavuşturulması gerekmektedir.*” Akbulut s. 29.

⁵⁶² Dülger, s. 328.

⁵⁶³ Akbulut, s. 28.

⁵⁶⁴ Meran, s. 571; Parlar, s. 25, Cankat, s. 337.

Bilişim sisteminin işleyişine engel olma, doğrudan tüm sistemin işleyişini engelleme şeklinde olabileceği gibi sistemin işleyişinde etkisi olan bir unsurun çalışmasını engelleyerek sistemin çalışmasının kısmen veya tamamen önlenmesi şeklinde gerçekleştirilebilir.⁵⁶⁵

Doktrinde bir görüşe göre engelleme hareketi sonucu sistemin geçici ya da sürekli olarak işlevini gereği gibi yerine getirememesi açısından bir fark olmayıp, sistemin engellendiği her durumda bu suç gerçekleşmiş olacaktır.⁵⁶⁶ Ancak sistemin işleyişinin sürekli olarak engellendiği durumda başka bir deyişle sistemin işlevsiz hale getirilmesi, süreklilik arz ediyorsa artık sistemin işleyişinin engellenmesi değil; bozulması söz konusudur. Zira sistem kendisinden beklenen veri işlemi yapamayacak hale geldiğinden yani bozulmuş sayılacağından sistemin işleyişinin engellenmesi geçici nitelikte olmalıdır.⁵⁶⁷ Sistemin bozulması seçimlik hareketinde sistem tamamen işlevsiz yani çalışamaz hale getirilmektedir. Engelleme seçimlik hareketi bakımından da sistem tamamen işlevsiz hale gelebilmekte ancak bu durum geçici bir sebepten ileri gelmektedir.⁵⁶⁸ Sistemin işleyişinin bozulması seçimlik hareketi bakımından da aslında sistemin işleyişine engel olunmaktadır. Ancak her ne kadar her bozma durumunda sistem engellenmiş olsa da her engelleme hareketi sistemin işleyişini bozma sonucunu doğurmaz.⁵⁶⁹

Sistemin işleyişinin engellenmesi TCK 244/2. maddesinde sayılan “*verileri bozma, yok etme, değiştirme veya erişilmez kılma, sisteme veri yerleştirme, var olan verileri başka bir yere gönderme hareketleri*” aracılığıyla da gerçekleştirilebilir. Burada önemli olan sistemin işleyişinin engellenip engellenmediğidir.⁵⁷⁰

⁵⁶⁵ Karagülmez, s. 211.

⁵⁶⁶ Ketizmen, s. 129; Yazıcıoğlu, s. 263; Karagülmez, s. 211.

⁵⁶⁷ Erdoğan, s. 190; Meran, s. 571; Apaydın, s. 11.

⁵⁶⁸ Kurt, s. 164.

⁵⁶⁹ Koca, s. 93.

⁵⁷⁰ Akbulut, s. 28.

c. Bilişim Sisteminin İşleyişini Bozma

Bilişim sisteminin işleyişini bozma, sistemin normalde yerine getirdiği işlevi yapamaz duruma getirilmesidir.⁵⁷¹ Yani sistemin, olağan durumda gerçekleştirebildiği veri işlem ve veri iletişimi artık yapamayacak hale getirilmesidir.⁵⁷² Bu sistemin hiçbir şekilde kendisinden beklenen işlevleri yapamamasına sebep olmak şeklinde olabileceği gibi sistemin yanlış şekilde işlemesine neden olmak şeklinde de gerçekleştirilebilir.⁵⁷³

Bilişim sisteminin işleyişinin bozulması doğrudan sistemin bozulması şeklinde olabileceği gibi sistemin çalışmasını sağlayan bir unsurun işlevsiz hale getirilmesi sonucu sistemin kısmen veya tamamen işlevsiz hale getirilmesi şeklinde gerçekleştirilebilir.⁵⁷⁴ Sistemin tamamının değil de belli işlevi yerine getiremeyecek şekilde kısmen bozulması da TCK 244. maddesi kapsamında suç sayılacaktır.⁵⁷⁵ Zira suçun kanuni tanımında sistemin tamamen bozulması konusunda herhangi bir belirleme yapılmamıştır. Örneğin bilişim sistemindeki kurulum yazılımının kodlarının değiştirilmesi sonucu bilişim sisteminde gerçekleştirilen asıl faaliyetin yapılamaması halinde sistemin bozulması söz konusudur ve sistemde diğer programların çalıştırılabiliyor olması (örneğin film izlemek, müzik dinlemek) bozma seçimlik hareketinin gerçekleşmesini engellemez. İşletim sistemine ilişkin dosyalara zarar verilmesi halinde de sistem işlevsiz bir hale geleceğinden yine bozma söz konusu olacaktır.⁵⁷⁶

Doktrinde bir görüş; her ne kadar gerekçede bilişim sistemlerinin somut unsurlarının bu suçun konusunu oluşturacağı belirtilmişse de suçun kanunda düzenlendiği yeri dikkate alarak sistemin fiziki unsurlarına yönelik zarar verici fiilleri mala zarar verme suçu kapsamında; sistemin işleyişini sağlayan soyut unsurlara yönelik zarar verici

⁵⁷¹ Meran, s. 571; Parlar, s. 25.

⁵⁷² Koca/ Üzülmüş, s. 916; Ketizmen, s. 129; Yaşar/ Gökcan/ Artuç, s. 7310.

⁵⁷³ Akbulut, s. 31; Ketizmen, s. 129-130.

⁵⁷⁴ Karagülmez, s. 212.

⁵⁷⁵ Akbulut, s. 31; Koca, s. 93.

⁵⁷⁶ Kurt, s. 165-166.

fiillerinse TCK 244 kapsamında değerlendirilmesi gerektiğini savunmaktadır.⁵⁷⁷ Ancak bizim de katıldığımız görüşe göre sistemin işleyişinin bozulması, sistemin somut unsurlarına yönelik bir müdahaleyle gerçekleştirilebileceği gibi sistemdeki veri, program gibi soyut unsurlara yönelik müdahalelerle de gerçekleştirilebilir.⁵⁷⁸ Yani bilişim sisteminin işleyişini bozmaya elverişli herhangi bir hareketle suç işlenebilecektir.⁵⁷⁹ Sistemin baltayla tahrip edilerek tamamen işlevsiz hale getirilmesi de virüs gibi zararlı yazılımlarla tahrip edilmesi de bu fıkra göre cezalandırılacaktır.⁵⁸⁰

Engelleme ve bozma hareketlerinin her ikisinde de sistem olağan şartlar altında yerine getirdiği işlevini yapamaz duruma getirildiğinden, iki hareketin birbirinden ayrımını yapmak çok kolay değildir.⁵⁸¹ Aslında sistemin işleyişinin bozulduğu her durumda sistemin işleyişi engellenmiş olmaktadır ancak sistemin işleyişinin engellendiği her durumda sistemin işleyişi bozulmamaktadır.⁵⁸² Dolayısıyla maddede sadece sistemin işleyişinin engellenmesinin yazması yeterli olabilirdi.⁵⁸³

Sistemin işleyişinin bozulması seçimlik hareketi bakımından sistem kendinden beklenen işlevleri yerine getiremezken yani işlev göremez hale gelmekteyken; engelleme seçimlik hareketi bakımından sistemin işlevlerini yerine getirmesi geçici olarak önlenmektedir.⁵⁸⁴ Aslında sistemin işleyişinin engellenmesi seçimlik hareketi bakımından da sistem işlevsiz hale getirilmekte ancak bu durum geçici nedenden kaynaklanmakta olup sistem sağlamdır. Sistemin işleyişinin bozulması seçimlik

⁵⁷⁷ Koca/ Üzülmüş, s. 915; “Bir bilişim sisteminin fizik varlığı olmadan soyut unsurlarının işlenmesi söz konusu olmazsa da 244. Maddede bilişim sisteminin kendisi değil, sistemin işleyişi korunmaktadır.” Özbek/ Doğan/ Bacaksız, s. 974.

⁵⁷⁸ Meran, s. 571; Kurt, s. 166; Orta, s. 116.

⁵⁷⁹ Parlar, s. 25.

⁵⁸⁰ Parlar, s. 25.

⁵⁸¹ Doktrinde bir görüş iki hareket arasındaki ayrımı şu şekilde yapmaktadır: Eğer hareket sistemin işleyişini geçici olarak kesintiye uğratiyorsa engelleme; sistemin işleyişi kalıcı olarak sonlandırılmışsa bozma söz konusu olmaktadır. Özbek/ Doğan/ Bacaksız, s. 973

⁵⁸² Koca/ Üzülmüş, s. 915

⁵⁸³ Karagülmez, s. 212.

⁵⁸⁴ Açıkgöz, s. 80.

hareketindeyse sistem tamamen işlevsiz hale getirilip, devre dışı bırakılmaktadır.⁵⁸⁵ Ayrıca bilişim sisteminin işleyişinin engellendiği durumda, engel ortadan kalktıktan sonra sistem işlevini yerine getirmeye sağlıklı bir şekilde devam edebilirken; sistemin işleyişinin bozulduğu durumda, sistemin tekrar işlevini yerine getirebilmesi için düzeltilmesi, tamir edilmesi gerekecektir.

Bilişim sisteminin işleyişine müdahale niteliğindeki eylemler aslında sistemin işlevi veri işleme olduğundan, veriye müdahale niteliğinde eylemlerdir. Dolayısıyla verileri bozarak, yok ederek, değiştirerek veya erişilmez kılarak, sisteme veri yerleştirerek, var olan verileri başka bir yere göndererek bilişim sisteminin işleyişinin engellenmesi durumunda, sorumluluk TCK 244/2. maddesinden değil; 244/1. maddesinden doğacaktır. TCK 244/2. maddesinin gerçekleştirilmesi için verilere yönelik bu hareketlerin sistemin işleyişini engellememesi gerekir.⁵⁸⁶

3. Verilere Yönelik Hareketler

a. Genel açıklama

Bilginin işlenmesi, saklanması, aktarılması için hayatımızın vazgeçilmez teknolojileri haline gelen bilişim sistemlerinde, kişisel bilgilerimizden kurumların kurumsal bilgilerine kadar her türlü bilgi depolanmaktadır. Bilişim sisteminde veri haline gelen bu bilgilerin korunması amacıyla yeni suçlar ihdas edilmiştir. Bu çerçevede TCK 244/2. maddesinde bilişim sistemlerinde yer alan her türlü veri koruma altına alınmıştır.⁵⁸⁷

TCK 244. maddesinin ikinci fıkrasında verilere yönelik tipik hareketler sayılmıştır. Buna göre “*sistemdeki verileri bozma, yok etme, değiştirme veya erişilmez*

⁵⁸⁵ Kurt, s. 164.

⁵⁸⁶ Koca/ Üzülmüş, s. 917.

⁵⁸⁷ Apaydın, Cengiz, “Bilişim Sistemindeki verileri yok etme, bozma, erişilmez kılma, değiştirme, hukuka aykırı olarak verileri yerleştirme veya gönderme suçu ile bu suretle hukuka aykırı yarar elde etme suçunun değerlendirilmesi”, s. 8.

kılma, sisteme veri yerleştirme, var olan verileri başka bir yere gönderme” hareketleri ceza yaptırımına bağlanmıştır. Bu fıkradan dolayı sorumluluğun doğması için maddede sayılan hareketlerin bilişim sisteminin işleyişini engellememesi veya bozmaması gerekir.⁵⁸⁸

Doktrinde suçun serbest hareketli bir suç mu seçimlik hareketli bir suç mu olduğu konusunda tartışma vardır. Bir görüşe göre ikinci fıkra yazılı olan hareketler, aslında suçun hareket unsuru olmayıp, neticeleridir. Dolayısıyla ikinci fıkra bakımından da suç, fıkra sayılı neticeleri gerçekleştirmeye elverişli her türlü hareketle işlenebileceğinden serbest hareketli bir suçtur.⁵⁸⁹ Diğer görüşe göre suç seçimlik hareketli bir suçtur.⁵⁹⁰ Bize göre de maddede sayılan hareketler, suçun neticeleri olmayıp hareketleri olduğundan, bu suç seçimlik hareketli bir suçtur. Dolayısıyla hareketlerden birinin ya da birkaçının işlenmesiyle suç gerçekleşecektir.⁵⁹¹ Birden fazla hareketin yapıldığı durumda yine tek bir veriye müdahale suçu gerçekleşmiş olacaktır.⁵⁹²

Verilere müdahale suçu hem icrai hem ihmali hareketle işlenebilir.⁵⁹³ Örneğin sistemdeki verilerin düzenli ve otomatik olarak silindiği bir bilişim sisteminde, önemli verilerin silinmemesi konusunda talimat alan çalışanın, bu konuda hareketsiz kalması durumunda ihmali olarak bu suçun işlendiği kabul edilmelidir. Verilere müdahale suçu ani hareketli bir suçtur. Hareketlerin etkisinin belli bir süre devam ediyor olması suçu mütemadi hale getirmez.⁵⁹⁴

⁵⁸⁸ Koca/ Üzülmüş, s. 917.

⁵⁸⁹ Erdoğan, s. 217.

⁵⁹⁰ Hafizoğulları/ Özen, s. 455; Özbek/ Doğan Bacaksız, s. 975; Parlar, s. 26.

⁵⁹¹ Koca, s. 94; Erdağ, s. 290.

⁵⁹² Yaşar/ Gökcan/ Artuç, s. 7314.

⁵⁹³ Erdoğan, s. 219; Yazar burada bilişim sisteminin güvenliğinden sorumlu kimsenin sistemi korumaya yarayan antivirüs yazılımını yüklememesi dolayısıyla 244. Maddedeki suçun işlenmesini örnek göstermektedir. Ancak bu durumda görevli kimse suç teşkil eden duruma ihmaliyle sebep olmamaktadır. Taşkın, s. 50.

⁵⁹⁴ Hafizoğulları/ Özen, s. 455.

Verilere müdahale suçu, doktrinde bazı yazarlara göre neticesiz bir suçtur.⁵⁹⁵ Bu suçun neticeli olduğunu düşünen yazarlardan bazıları fıkra da sayılan unsurların aslında netice olduğunu dolayısıyla bu suçun neticeli bir suç olduğunu savunmaktadır.⁵⁹⁶ Ancak fıkra da sayılan hareketler, netice değildir; verilere müdahale suçunun seçimlik hareketleridir. Suç bu hareketlerin gerçekleştirilmesi suretiyle işlenmektedir. Verilere müdahale niteliğindeki bu hareketler sonucu, veriler kullanılamaz hale geldiğinden başka bir deyişle dış dünyada bir değişiklik meydana geldiğinden bu suç neticeli bir suçtur.

İkinci fıkra da sayılan seçimlik hareketlerden sisteme veri yerleştirilmesi dışındaki hareketler açısından suç zarar suçu; sisteme veri yerleştirme hareketi açısından suç, herhangi bir zararın doğması aranmadığından tehlike suçudur.⁵⁹⁷

TCK 244/2. maddesinin maddi konusunu oluşturabilecek başka bir ifadeyle bu fıkra kapsamında korunan veriler, bilişim sisteminin işleyişini sağlayan veriler değildir. Sistemin işleyişini sağlayan verilere yönelik müdahale bizzat sistemin işleyişine müdahale niteliğinde olduğundan birinci fıkra kapsamında değerlendirilecekken; sistemdeki diğer verilere müdahale niteliğindeki hareketler ikinci fıkra kapsamında değerlendirilecektir.⁵⁹⁸

İkinci fıkra da sayılan hareketler göz önünde bulundurulduğunda, kanun koyucu boşluk bırakmamaya çalışarak, her türlü ihtimali madde kapsamında düzenleme altına almaya çalışmıştır. Ancak bu durum işlenen bazı fiillerin, maddede sayılı hareketlerden birden fazlasının kapsamına girmesi durumuna neden olmuştur.⁵⁹⁹ Maddede sayılan birden fazla hareketin gerçekleştirilmesi durumunda ortada yine tek suç vardır zira bu suç seçimlik hareketli bir suçtur.

⁵⁹⁵ Meran, s. 372; Hafızoğulları/ Özen, s. 455.

⁵⁹⁶ Erdoğan, s. 219.

⁵⁹⁷ Yaşar/ Gökcan/ Artuç, s. 7314.

⁵⁹⁸ Erdoğan, s. 215.

⁵⁹⁹ Erdoğan, s. 219.

Doktrinde verilerin bilişim sisteminde değil de veri taşıma aracında olması durumunda veri taşıma aracı bir bilişim sistemi olmadığından, sisteme bağlı olmayan bu araçtaki verilere müdahale niteliğindeki fiillerin bu madde kapsamında değerlendirilmeyeceği iddia edilse de⁶⁰⁰ veri taşıma araçlarındaki veriler de TCK 244/2. maddesi kapsamında korunacaktır.⁶⁰¹

Verilere müdahalenin düzenlendiği ikinci fıkrada “*sisteme veri yerleştirme ve var olan verileri başka yere gönderme*” hareketlerine yer verilmesi yerinde bir düzenleme olmamıştır. Zira “*sisteme veri yerleştirme ve verileri başka bir yere gönderme*” hareketlerinde sistemdeki mevcut verilere yönelik bir müdahale söz konusu değildir.⁶⁰² Fail sisteme veri yerleştirirken veya verileri başka yere gönderirken sistemdeki mevcut verilere müdahale etmemekte ancak sisteme müdahale etmektedir. Nitekim veri yerleştirme hareketiyle verileri değiştirmek; verileri başka sisteme göndermek hareketiyle verileri bozma, yok etme kastediliyorsa bu hareketler zaten madde metninde yer aldığından gereksiz bir tekrara gidilmiş olacaktır. Bu sebeple verilere müdahale niteliği taşımayan bu hareketlerin bu fıkrada düzenlenmesi doğru bir tercih olmamıştır. Bu hareketler sistemin işleyişini engelliyor ya da bozuyorsa sisteme müdahale olarak değerlendirilmeli ancak sisteme müdahale söz konusu değilse farklı bir suç olarak düzenleme altına alınmalıdır.⁶⁰³

b. Verileri Bozmak

Verileri bozmak; “*verilerin içeriğine veya yapısına müdahale etmek suretiyle*”⁶⁰⁴ verilerin, verilerden istenilen şekilde yararlanılamayacak hale getirilmeleridir.⁶⁰⁵ Burada

⁶⁰⁰ Ketizmen, s. 143.

⁶⁰¹ Yazıcıoğlu, s. 261.

⁶⁰² Akbulut, s. 31/32; Bu hareketlerin başka fıkrada veya başka bölüm ya da bölümlerde (kişisel veri, özel hayat, sır vb. niteliğinde olmasına göre) düzenlenmesi (veya değişikliğe gidilmesi) uygun olurdu. Akbulut, s. 51.

⁶⁰³ Akbulut, s. 18.

⁶⁰⁴ Ketizmen, s. 139; Koca/ Üzülmüş, s. 917.

⁶⁰⁵ Mahmutoğlu, s. 867; Koca, s. 94.

veriler kısmen veya tamamen tahrip edilmekte ancak sistemden yok edilmemektedir.⁶⁰⁶

Verileri bozma seçimlik hareketinde, yok etme seçimlik hareketinden farklı olarak veriler sistemde bulunmaya devam etmektedir.⁶⁰⁷

Bilişim sistemine yönelik fiziki bir müdahale sonucu sistem içerisindeki veriler zarar görürse, örneğin bir disketin kırılması yoluyla⁶⁰⁸, yine bu seçimlik hareket gerçekleşmiş olacaktır.⁶⁰⁹

c. Verileri Yok Etmek

Verileri yok etmek, verilerin sistemdeki mevcudiyetine son verilmesi, verilerin ortadan kaldırılmasıdır.⁶¹⁰ Sistemde verilerin varlığına son vermek, verileri imha etmektir. Verileri yok etmek doğrudan sisteme girerek ya da ağ yardımıyla sisteme girme şeklinde işlenebilir.⁶¹¹

Verilerin bozulması ve yok edilmesi seçimlik hareketleri arasındaki fark, verilerin onarılarak geri kazandırılmaları konusunda ortaya çıkmaktadır.⁶¹² Verilerin bozulması seçimlik hareketinde, verilerin işlevsiz hale getirilmesi söz konusu olsa da verilerin düzeltilerek geri kazanılması mümkünken; verilerin yok edilmesi seçimlik hareketi bakımından sistemde geri kazanılabilecek bir veri dahi kalmamıştır.⁶¹³ Verilerin yok edilmesi, verilerin geri kazanılamayacak şekilde ya da büyük uğraşlar sonucu geri kazanılabilecek şekilde ortadan kaldırılmasıdır.⁶¹⁴

Sistemden yok edilen verilerin geri kazanılmasının mümkün olduğu durumlarda suçun oluşup oluşmadığı konusunda doktrinde farklı görüşler vardır. Bir görüş burada

⁶⁰⁶ Meran, s. 571.

⁶⁰⁷ Ketizmen, s. 139.

⁶⁰⁸ Parlar, s. 26.

⁶⁰⁹ Kurt, s. 167.

⁶¹⁰ Mahmutoglu, s. 867; Koca/ Üzülmöz, s. 917; Meran, s. 571; Parlar, s. 26; Ketizmen, s. 138.

⁶¹¹ Dülger, s. 331.

⁶¹² Parlar, s. 26.

⁶¹³ Kurrt, s. 168; Yaşar/ Gökcan/ Artuç, s. 7312.

⁶¹⁴ Ketizmen, s. 138.

verilerin geri getirilmesinin mümkün olup olmadığına bakılmaksızın, verilerin yok edilmesi durumunda suçun gerçekleşmiş sayılacağını savunmaktadır.⁶¹⁵ Bu görüşe göre verilere olağan şekilde erişilmesinin engellendiği yani normal şartlarda veriye ulaşılması için gereken komutun sisteme girilmesine rağmen veriye erişilemediği ancak bir takım araç ve programlarla ortadan kaldırılan verilerin geri kazanılmasının mümkün olduğu durumlarda dahi suç oluşmaktadır.⁶¹⁶ Verilerin, sistemden bir daha geri getirilemeyecek şekilde ortadan kaldırılması mümkün değildir.⁶¹⁷ Bu sebeple verilerin geri getirilebilir olması suçun oluşmasını engellemez.⁶¹⁸ Karşıt görüşe göre ise verilerin geri kazanılması imkanının bulunması durumunda verilerin ortadan kaldırılması söz konusu olmadığından verilerin yok edilmesi suçu oluşmayacaktır ancak duruma göre başka bir suça örneğin verilerin erişilmez kılınması söz konusu olabilecektir.⁶¹⁹

Bu tartışmaya paralel olarak, sistemden verinin silinmesi durumunda yok etme seçimlik hareketinin mi erişilmez kılma seçimlik hareketinin mi olduğu doktrinde tartışmalıdır. Bir görüşe göre, verinin sistemden silinmesi, o veriye ulaşılmasını sağlayan olağan yolların artık veriye ulaşılması için işe yaramaması yani olağan yollardan veriye erişilememesidir.⁶²⁰ Verilerin silinmesi de yok edilme kapsamındadır ve verilerin tekrar elde edilebilmesi imkanının olması bu durumu değiştirmez.⁶²¹ Verilerin sistemden bir daha geri kazanılamayacak şekilde silinmesi teknik olarak mümkün değildir.⁶²² Veriler bir kere sisteme kaydedildikten sonra silinse dahi bu verileri kolay ya da karmaşık işlemlerle geri kazanmak mümkün olduğundan, yok etmek seçimlik hareketi bakımından verilere normal erişim yollarının koparılması yeterlidir.⁶²³

⁶¹⁵ Özbek/ Doğan/ Bacaksız, s. 975.

⁶¹⁶ Koca/ Üzülmüş, s. 918; Özbek/ Doğan/ Bacaksız, s. 976.

⁶¹⁷ Ketizmen, s. 138.

⁶¹⁸ Özbek/ Doğan/ Bacaksız, s. 976.

⁶¹⁹ Akbulut, s. 33.

⁶²⁰ Ketizmen, s. 138; Erdoğan, s. 222.

⁶²¹ Ketizmen, s. 139; Koca, s. 94.

⁶²² Kurt, s. 168; Soyaslan, s. 702; Meran, s. 571-572.

⁶²³ Meran, s. 572.

Karşıt görüşe göreyse; bilişim sisteminden sil komutuyla bir verinin ortadan kaldırılmaya çalışılması halinde, veriler sistemden tamamen ortadan kaldırılmamakta yalnızca veriye erişim imkânı sağlayan yollar değiştirilmektedir. Yok etme seçimlik hareketi bakımından elzem olan verinin mağdurun tasarruf alanından çıkarılması olduğundan, dosyanın silinerek geri dönüşüm kutusuna taşınması verinin sistemde farklı bir yere taşınması niteliğinde olduğundan bu seçimlik hareket gerçekleşmez.⁶²⁴ Bu itibarla sistemden veriler yok olmadığından ancak verilere normal yoldan erişim imkanı engellendiğinden ve verilerin geri kazanılması için bir takım çaba gerektiğinden verilerin yok edilmesi seçimlik hareketi değil; verilerin erişilmez kılınması seçimlik hareketi gerçekleşmektedir.⁶²⁵ Verilerin erişilmez kılınması, verilerin yok edilmesi değildir.⁶²⁶ Verilere erişim engellendiği örneklerde veriler sistemde bulunmaya devam eder.⁶²⁷

Doktrinde bir görüşe göre ancak fiziki bir müdahaleyle örneğin veri taşıma aracının yakılması gibi bir durumda veriler tamamen yok edilebilmektedir.⁶²⁸ Fakat veri taşıma cihazına müdahaleyle verilerin geri dönülmez bir biçimde yok edilmesi dışında veri üzerine veri yazılarak da veriler geri döndürülemez şekilde yok edilebilmektedir.⁶²⁹ Verilerin bir daha geri kazanılamayacak şekilde ortadan kaldırılması mümkün olduğundan, yok etme seçimlik hareketi bakımından da verilerin sistemden geri dönüşü olmayacak şekilde ortadan kaldırılması anlaşılmalıdır.⁶³⁰

Yok edilmeye çalışılan verilerin sistemde kopyalarının olması durumunda, sistemden verilerin tamamen ortadan kaldırılması söz konusu olmadığından, yok etme seçimlik hareketi gerçekleşmemiş olacaktır.⁶³¹ Ancak burada yok etme seçimlik hareketi

⁶²⁴ Koca, s. 94.

⁶²⁵ Kurt, s. 168.

⁶²⁶ Özbek/ Doğan/ Bacaksız, s. 976.

⁶²⁷ Açıkgöz, s. 84. Erdoğan, s. 222.

⁶²⁸ Parlar, s. 26.

⁶²⁹ Dülger, s. 332.

⁶³⁰ Açıkgöz, s. 84.

⁶³¹ Akbulut, s. 33.

bakımından suça teşebbüs ya da kopyası bulunan verilere müdahalenin niteliğine göre diğer seçimlik hareketlerin işlenmesi söz konusu olabilecektir.

Bilişim sistemine zarar vererek de veriler yok edilebilir. Örneğin virüs göndererek sisteme zarar verilmesi, verilerin silinmesine de neden olabilir. Ancak bu durumda fiil; sistemin işleyişinin engellenmesine veya bozulmasına neden olmuşsa, sisteme müdahale suçuna vücut verecektir. Dolayısıyla bilişim sistemine zarar vererek, verilerin yok edilmesi seçimlik hareketinin gerçekleştiğinin kabulü için fiil sisteme müdahale niteliğinde olmamalıdır.⁶³²

d. Verileri Değiştirmek

Verileri değiştirmek, sistemdeki verilerin orijinal hallerinden uzaklaşmasına, kısmen veya tamamen farklı bir içerik kazanmalarına neden olmaktadır.⁶³³ Bu seçimlik harekette veriler, kullanılma amacından farklı bir biçime sokulmaktadır.⁶³⁴ Bu hareket “verilerin başka biçimlere sokulması, yeni içerik kazandırılması veya niteliklerinin değiştirilmesi” gibi şekillerde gerçekleştirilebilir.⁶³⁵ Verilerin kısmen veya tamamen değiştirilmesi suçun oluşumu açısından önem arz etmez.⁶³⁶

“Verilerin içeriğinin tamamen değiştirilmesi veya veri sonuçlarının değiştirilmesi veya program dilinin değiştirilmesi veya verilerin metin içindeki yerlerinin değiştirilmesi veya verilerin kısmî silinmesi veya verilere ilave şeylerin katılması” verilerin değiştirilmesine örnektir.⁶³⁷ Verilerin geri kazanılamaz biçimde sistemden silinmesi, yok etme seçimlik hareketi içerisinde değerlendirilmeliyken; bazı durumlarda verilerin silinmesi, verilerin değiştirilmesi olarak kabul edilmelidir. Eğer sistemden silinen veriler,

⁶³² Akbulut, s. 34.

⁶³³ Koca/ Üzülmüş, s. 918; Parlar, s. 26; Kurt, s. 168; Ketizmen, s. 140.

⁶³⁴ Özbek/ Doğan/ Bacaksız, s. 976; Meran, s. 572.

⁶³⁵ Dülger, s. 333.

⁶³⁶ Parlar, s. 26.

⁶³⁷ Akbulut, s. 34.

sistemden silinmeyen verilerin yeni bir içerik kazanmasına neden oluyorsa silme hareketi değiştirme seçimlik hareketi bağlamında değerlendirilmelidir.⁶³⁸

Doktrindeki bir görüşe göre bilişim sistemindeki veri veya programlara virüs gibi kötü amaçlı yazılımların eklenmesi, verinin değiştirilmesi olarak değerlendirilmelidir. Çünkü verilerin bozulmasından önce virüs eklenerek verinin önce değiştirilmesi söz konusudur.⁶³⁹ Ancak biz bu görüşe iştirak etmiyoruz. Çünkü sistemdeki verilerin değiştirilmesi seçimlik hareketi bakımından kastedilen, sistemdeki mevcut verilerin orijinal hallerinden uzaklaştırılmasıdır. Dolayısıyla bilişim sistemine virüs eklenmesiyle veriler bozulmuşsa, bozma seçimlik hareketinin işlenmesi suretiyle verilere müdahale suçu gerçekleşmektedir.

Sistemdeki verilerin hukuka aykırı olarak kopyalanması verilerin değiştirilmesi değildir.⁶⁴⁰ Doktrindeki bir görüşe göre tipik değiştirme hareketinin orijinal veriler üzerinde işlenmesi gerekir. Dolayısıyla kopyalanmış verilerin değiştirilmesi durumunda bu suç gerçekleşmemiştir.⁶⁴¹ Ancak madde metninde verilerin kopya veya asıl olmasına ilişkin bir ayırım yapılmadığından, kopyalanmış veriler üzerinde de bu seçimlik hareket işlenebilir.

e. Verileri Erişilmez Kılmak

Verileri erişilmez kılma, verilerin içeriğine yönelik bir müdahale olmaksızın verilere ulaşma imkânı sağlayan yolların değiştirilmesi veya silinmesidir.⁶⁴² Verilere erişimin engellenmesinde, veriler sistemden yok olmamakta, değiştirilmemekte veya zarar görmemektedir.⁶⁴³ Verilere erişim engellendiği örneklerde veriler sistemde

⁶³⁸ Akbulut, s. 34.

⁶³⁹ Ketizmen, s. 140.

⁶⁴⁰ Akbulut, s. 34.

⁶⁴¹ Akbulut, s. 35.

⁶⁴² Parlar, s. 26; Kurt, s. 169; Ketizmen, s. 140; Yaşar/ Gökcan/ Artuç, s. 7312.

⁶⁴³ Ketizmen, s. 140; Özbek/ Doğan/ Bacaksız, s. 976.

bulunmaya devam eder.⁶⁴⁴ Ancak mağdur, bu verilere normalde ulaştığı şekilde erişememektedir.⁶⁴⁵ Örneğin şifresiz bir dosyaya şifre konması durumunda, normalde o dosyaya ulaşmak için verilen komut işe yaramaz hale gelmektedir.⁶⁴⁶

Verileri erişilmez kılma seçimlik hareketi çok farklı şekillerde işlenebilir. Örneğin verilere ulaşmak için gereken bağı koparılması, verilerin sistemdeki yerlerinin değiştirilmesi, dosyanın isminin değiştirilmesi, verilere şifre konması veya mevcut şifrenin değiştirilmesi, verilerin sistemden silinmesi, fiziki bir müdahaleyle veri üzerinde hak sahibi kimsenin veriye erişiminin engellenmesi (örneğin veri taşıma aracına el konması) gibi hareketlerle gerçekleştirilebilir.⁶⁴⁷

Bilişim sisteminden verilerin silinmesi durumunda, veriler sistemden tamamen ortadan kaldırılmamakta yalnızca veriye olağan yollardan erişim imkânı sağlayan yollar değiştirilmektedir. Bu itibarla sistemden veriler yok olmadığından ancak verilere normal yoldan erişim imkânı engellendiğinden ve verilerin geri kazanılması için bir takım çaba gerektiğinden verilerin yok edilmesi seçimlik hareketi değil; verilerin erişilmez kılınması seçimlik hareketi gerçekleşmektedir.⁶⁴⁸

Sisteme müdahale durumunda yani sistemin işleyişinin engellenmesi veya bozulması amacıyla gerçekleştirilen fiil sonucu veriler erişilmez kılınmışsa burada ayrıca TCK 244/2. fıkrasının gerçekleşmesi söz konusu değildir.⁶⁴⁹ Nitekim sistemin işleyişinin engellenmesi veya bozulması durumunda sistem işlevini yerine getiremez hale getirildiğinden, verilere erişememek bu müdahalenin doğal sonucudur.

⁶⁴⁴ Açıkgöz, s. 84; Erdoğan, s. 222.

⁶⁴⁵ Özbek/ Doğan/ Bacaksız, s. 977; Koca/ Üzülmöz, s. 918; Kurt, s. 169.

⁶⁴⁶ Koca, s. 95.

⁶⁴⁷ Kurt, s. 169; Akbulut, s. 35; Koca/ Üzülmöz, s. 918.

⁶⁴⁸ Kurt, s. 168.

⁶⁴⁹ Özbek/ Doğan/ Bacaksız, s. 977.

Verilerin erişilmez kılınmasının geçici veya sürekli olması suçun oluşumu açısından önem arz etmez.⁶⁵⁰ Erişilmez kılma belirli bir zaman dilimine yayıldığından, suç bakımından bu durumun ne kadar süre devam etmesi gerektiği belirsizdir. Doktrinde sürenin önemli bir zaman dilimini kapsaması, verinin kullanılamamasının en azından kesin bir süreyi göstermesi gerektiği gibi ölçütler ileri sürülmüştür.⁶⁵¹ Bu ölçütler de belirsizliği ortadan kaldırmaya yardımcı olmamaktadır. Verilerin erişilmez kılınmış sayılması için gereken süre, her somut olayda mahkeme tarafından takdir edilmelidir.

f. Sisteme Veri Yerleştirme

TCK 244/2. maddesinde verilere müdahale niteliğinde yani verilere zarar verici nitelikteki hareketler düzenleniyor demiştik ancak fıkrada bu mahiyette olmayan iki seçimlik harekete daha yer verilmiştir. Bunlardan ilki sisteme veri yerleştirme, sistemde bulunan verilere müdahale etmeden, sisteme daha önce orada bulunmayan verilerin eklenmesi, kaydedilmesidir.⁶⁵² Sisteme veri yerleştirmede fail bu suçu; hukuka uygun veya aykırı olarak girdiği sisteme doğrudan sistemde olmayan verileri girerek veya internet gibi ağ sistemleri aracılığıyla sisteme veri girerek ya da veri taşıma araçları aracılığıyla sisteme veriyi aktararak işleyebilmektedir.⁶⁵³ Kısacası failin sisteme hukuka uygun veya aykırı olarak girmiş olmasının ve verilerin sisteme hangi yöntemle yerleştirildiğinin bir önemi yoktur.⁶⁵⁴

g. Var Olan Verileri Başka Yere Gönderme

Verilere müdahale niteliğinde olmayan ikinci seçimlik hareket, var olan verileri başka yere göndermedir. “*Var olan verileri başka yere gönderme*” seçimlik hareketi

⁶⁵⁰ Parlar, s. 26; Kurt, s. 169; Erdoğan, s. 225; Soyaslan, s. 704; Özbek/ Doğan/ Bacaksız, s. 977.

⁶⁵¹ Daha detaylı bilgi için bkz. Akbulut, s. 37.

⁶⁵² Meran, s. 572; Parlar, s. 27; Taşkın, s. 48; Yaşar/ Gökcan/ Artuç, s. 7313.

⁶⁵³ Koca/ Üzülmüş, s. 918; Taşkın, s. 48; Soyaslan, s. 704.

⁶⁵⁴ Yaşar/ Gökcan/ Artuç, s. 7313; Soyaslan, s. 704.

bakımından öncelikle ifade oldukça belirsizdir.⁶⁵⁵ Verilerin başka yere gönderilmesi; bilişim sistemindeki mevcut verilerin başka bir bilişim sistemine veya veri taşıma aracına, aktarılan verilerin bulundukları sistemden yok edilmeden aktarılması⁶⁵⁶, kaydedilmesidir.⁶⁵⁷

Verilerin başka yere gönderilmesi durumunda iki ihtimal karşımıza çıkmaktadır. Bunlardan ilki verilerin orijinallerinin sistemden tamamen ortadan kaldırılarak başka bir yere gönderilmesi; diğeri ise sistemdeki orijinal dosyanın sistemden kaldırılmadan bir kopyasının başka bir yere gönderilmesidir. Suçun kanuni tanımında bu seçimlik hareket bakımından böyle bir ayrıma yer verilmediğinden maddeden her iki anlam da çıkarılabilir. Ancak verilerin kopyasının gönderilmesi durumunda veriye bir müdahale söz konusu olmadığından; veriler sistemde orijinal haliyle kaldığından TCK 244/2. maddesinde böyle bir harekete yer verilmesi yerinde bir tercih olmamıştır.⁶⁵⁸ Verinin orijinalinin sistemde bırakılmayacak şekilde elde edilmesi durumunda, veri sistemden ortadan kaldırıldığı için bu durum verilerin yok edilmesi hareketi içerisine girecektir. Dolayısıyla burada iki seçimlik hareketin birbirinden ayrılması için verinin sistemden kaldırılmadan kopyasının alındığı örneklerin, bu seçimlik hareket kapsamında değerlendirilmesi gerekir⁶⁵⁹

Bu seçimlik hareket; hak sahibinin veri üzerinde tasarruf imkanının verinin bütünlüğüne zarar verilmeden engellenmesi şeklinde anlaşıldığında, bu hareket verileri erişilmez kılmak seçimlik hareketiyle karışmaktadır. Bu seçimlik hareketin verileri

⁶⁵⁵ Bir bilişim sisteminde gerçekleştirilen her türlü işlem için mutlaka bir veri iletimi gerçekleştirilir. Buradaki veri iletimi de kanun koyucunun bu seçimlik harekette öngördüğü var olan verileri başka yere gönderme hareketine girmektedir. Ağ aracılığıyla bilgisayarlar arasında kurulan her türlü iletişim, veri aktarımıyla olur. Örneğin bir web sitesine erişmek için sayfa bağlantısının tarayıcıya girilmesi halinde web sayfasının kayıtlı olduğu sunucuya bir komut yani veri gönderilmektedir. Özbek/ Doğan/ Bacaksız, s. 977.

⁶⁵⁶ Verinin sistemden tamamen ortadan kaldırılarak aktarıldığı durumda zaten yok etme söz konusu olduğundan bu ifadeyi verinin sistemden tamamen ortadan kaldırılarak hak sahibinin tasarruf yetkisine son verme şeklinde anlamamak gerekir. Erdoğan, s. 227; Soyaslan, s. 705.

⁶⁵⁷ Koca/ Üzülmüş, s. 918; Taşkın, s. 49.

⁶⁵⁸ Akbulut, s. 38.

⁶⁵⁹ Yaşar/ Gökcan/ Artuç, s. 7313; Kurt, s. 170.

erişilmez kılma seçimlik hareketinden ayrımının sağlanması için mevcut verilerin sistem içerisinde yerinin değiştirilmesi şeklinde anlaşılmaması; tersine “*verilerin başka bir bilişim sistemine veya veri taşıma aracına gönderilmesi*” anlaşılmalıdır.⁶⁶⁰ Ancak doktrinde bazı yazarlar, verilerin başka yere gönderilmesi seçimlik hareketinden kastın, verilerin sistem içerisinde yerinin değiştirilmesi olduğunu savunmaktadır.⁶⁶¹ Bu yazarlara göre TCK 244. maddesinde sistemin işleyişine ve veriye müdahale fiilleri suç haline getirildiğinden, verinin başka yere gönderilmesinden verinin kopyalanması anlaşıldığında veriye yönelik müdahale olmadığından yani veri sistemde sağlıklı bir şekilde bulunmaya devam ettiğinden bu durum aslında maddenin getiriliş amacıyla uyusmamaktadır. “*Verinin başka yere gönderilmesi*” seçimlik hareketi, verinin sistemden ortadan kaldırılması şeklinde anlaşılırsa bu durum zaten yok etme kapsamına girdiğinden bu ifade anlamsız hale gelmektedir. Bu sebeplerle verilerin başka yere gönderilmesi seçimlik hareketinin sistemde verinin yerinin değiştirilmesi şeklinde anlaşılması bu ifadeyi anlamlı hale getirmektedir.⁶⁶²

Burada mağdurun gönderime konu veriye erişip erişemediği ya da verinin ortadan kaldırılıp kaldırılmadığı suçun oluşumu açısından fark yaratmayacaktır. Örneğin fail veriyi veri taşıma cihazına aktardıktan sonra sistemden yok etmişse her iki seçimlik hareket ayrı ayrı işlenmiş olacaktır.⁶⁶³

b. MANEVİ UNSUR

TCK 21. maddesine göre kast “*suçun kanuni tanımındaki unsurlarının bilerek ve istenerek gerçekleştirilmesidir.*” TCK 244. maddesinde kasten işlenebilen suçlar düzenlenmiştir.⁶⁶⁴ Fail hakkı olmaksızın “*sistemin işleyişini engellediğini veya*

⁶⁶⁰ Açıkgöz, s. 88.

⁶⁶¹ Tezcan/ Erdem/ Önok, s. 1169; Yaşar/ Gökcan/ Artuç, s. 7313; Erdoğan, s. 227.

⁶⁶² Ketizmen, s. 141-142.

⁶⁶³ Açıkgöz, s. 88-89; Koca/ Üzülmöz, s. 919.

⁶⁶⁴ Koca/ Üzülmöz, s. 919; Yaşar/ Gökcan/ Artuç, s. 7318.

bozduğunu ya da sistemdeki verileri bozduğunu, yok ettiğini, değiştirdiğini, erişilmez kıldığını, sisteme veri yerleştirdiğini, var olan verileri başka bir yere gönderdiğini” bilmeli ve istemelidir. Suçların özel bir saikle işlenmesi aranmadığından, suçlar genel kastla işlenebilir.⁶⁶⁵ Dolayısıyla amacı gözetilmeksizin sistemin işleyişine veya verilere müdahale eden kimse TCK 244. maddesindeki suçların faili olacaktır.

TCK 244. maddesinin birinci ve ikinci fıkrasındaki suçlar hem doğrudan hem olası kastla işlenebilir.⁶⁶⁶ Örneğin sistemi korumakla görevli mühendisin virüsleri temizlerken verilerin de silinebileceğini öngörüp hareketini yine de yapması halinde verileri yok etme suçu olası kastla işlenmiştir.

Taksirli sorumluluk istisnai olduğundan, suçun taksirli haline kanunda yer verilmiş olması gerekir. TCK 244. maddesindeki suçların taksirli haline kanunda yer verilmediğinden, dikkat ve özen yükümlülüğüne aykırı olarak bu hareketleri gerçekleştirenler cezalandırılmayacaklardır.⁶⁶⁷ Ancak suçun taksirli haline yer verilmemesi bir eksikliktir. Nitekim TCK 244. maddesindeki sistemin işleyişine veya verilere müdahale suçları taksirle işlenebilecek suçlardır. Örneğin hukuka uygun girdiği sistemde sistemin işleyişine veya verilere dikkat ve özen yükümlülüğüne aykırı olarak zarar veren kimse cezasız kalacaktır.

Üçüncü fıkarda düzenlenen nitelikli hal bakımından fail müdahale ettiği bilişim sisteminin veya verilerin banka veya kredi kurumuna ya da kamu kurum veya kuruluşuna

⁶⁶⁵ Karagülmez, s. 214; Yaşar/ Gökcan/ Artuç, s. 7318; 765 S TCK döneminde bu maddenin karşılığı olan 525/b maddesinde “zarar vermek veya yarar sağlamak” amacıyla hareket edilmesi arandığından suç özel kastla işlenebilen bir suçtu ve bu özel kastı taşımayan ancak bu hareketleri gerçekleştiren kimseler cezasız kalmaktaydı. Dolayısıyla düzenleme eleştirilmekteydi. TCK 244. maddesinde yapılan bu düzenleme yerinde bir düzenlemedir. Ersoy, s. 62.

⁶⁶⁶ Koca, s. 94-95; Yaşar/ Gökcan/ Artuç, s. 7318; Erdoğan, s. 200; Akbulut, s. 39; Özbek/ Doğan/ Bacaksız, s. 985; Koca/ Üzülmüş, s. 919; Doğrudan kastla işlenebileceğini düşünen yazar için bkz. Meran, s. 581.

⁶⁶⁷ Özbek/ Doğan/ Bacaksız, s. 985; Karagülmez, s. 214; Doktrinde Taşkın bu suçun taksirli haline kanunda yer verilmemesini bir eksiklik olarak değerlendirmektedir. Taşkın, s. 53.

ait olduğunu bilerek ve isteyerek fiilini gerçekleştirmelidir.⁶⁶⁸ Aksi halde TCK 30/3. maddesi kaçınılmaz hatanın bulunması durumunda uygulama alanı bulacaktır.

c. HUKUKA AYKIRILIK

Suç; ceza hukuku normuyla çatışan, normu ihlal eden fiildir. İhlalsiz suç olmaz ilkesi gereğince fiilin hukuka aykırı olması gerekir.⁶⁶⁹ Fiilin kanuni tipe uygun olması durumunda, fiil karine olarak hukuka aykırıdır. Ancak bu karine, fiili hukuka uygun hale getiren sebeplerin gerçekleşmesi halinde çürütülmekte ve fiil suç olmaktan, hukuk düzeniyle çatışma halinde olmaktan çıkmaktadır. Kanuni tipe uygun fiili, suç olmaktan çıkaran sebeplere hukuka uygunluk sebepleri denilmektedir.⁶⁷⁰ Hukuka aykırılığı tespit ederken de kanuni tipe uygun fiil bakımından hukuka uygunluk sebeplerinin olayda bulunup bulunmadığına göre belirleme yapılır. Fiil bakımından herhangi bir hukuka uygunluk nedeninin olayda gerçekleşmemesi durumunda, fiil suç teşkil etmektedir. Yani bir fiilin hukuka aykırı olarak nitelendirilebilmesi için fiilin tipik olması ve hukuka uygunluk sebeplerinin bulunmaması gerekir.⁶⁷¹

Hukuka uygunluk nedenlerinden kanun hükmünün ve yetkili amirin emrinin icrası (TCK 24), meşru müdafaa (TCK 25) ve ilgilinin rızası (TCK 26) bu suçla bağdaşmaktadır.⁶⁷² Yani bilişim sisteminin işleyişine veya sistemdeki verilere müdahale niteliğindeki hareketler; kanun hükmünün ya da amirin emrinin icrası için gerçekleştiriliyor veya ilgili kişinin rızası veyahut meşru müdafaa çerçevesinde işleniyorsa fiil hukuka uygundur.

⁶⁶⁸ Yaşar/ Gökcan/ Artuç, s. 7318.

⁶⁶⁹ Hafizoğulları/ Özen, Genel Hükümler, s. 193.

⁶⁷⁰ Koca/ Üzülmüş, Genel Hükümler, s. 265.

⁶⁷¹ Özen/ Hafizoğulları, Genel Hükümler, s. 195.

⁶⁷² Özbek/ Doğan/ Bacaksız, s. 984; Taşkın, s. 51; Yaşar/ Gökcan/ Artuç, s. 7318.

CMK 134 ve 135. maddeleri gereği verilmiş bir koruma tedbiri kararının⁶⁷³ veya 5651 S Kanun gereği verilmiş bir erişimin engellenmesi kararının yerine getirilmesi TCK 244. maddesindeki suç oluşturmayacaktır.⁶⁷⁴ Kamu hukukundan kaynaklı bir üst ast ilişkisinde, astın üstün vermiş olduğu emir doğrultusunda verileri bir sistemden silmesi TCK 244/2. maddesindeki suç oluşturmayacaktır.⁶⁷⁵

Doktrinde bir görüş, TCK'nın sistematüğını göz önünde bulundurarak bilişim sistemine girme suçunun Topluma Karşı Suçlar bölümünde düzenlenmesi ve kanun koyucunun burada toplumsal bir menfaate öncelik verdiği düşüncesinden hareketle ilgilinin rızası hukuka uygunluk nedeninin Bilişim Alanında Suçlar açısından geçerli olmadığını savunmaktadır. Ancak bu görüşe katılmak mümkün değildir. İlgilinin bilişim sistemi üzerindeki hakkı mutlak surette tasarrufta bulunabileceğı bir hak olduğundan, rıza bu suç bakımından hukuka uygunluk sebebi sayılmazdır.⁶⁷⁶

Kişinin bilişim sistemi ve sistemdeki veriler üzerindeki hakkı, üzerinde mutlak surette tasarruf edebileceğı bir hak olduğundan, sisteme veya verilere müdahale için sistem veya veri sahibinin göstermiş olduğu rıza fiili hukuka uygun kılacaktır. Rızayı göstermesi gereken kimse, tipik fiille ihlal edilen hukuki konunun sahibidir.⁶⁷⁷ Birinci fıkra bilişim sisteminin işleyişi ve mülkiyet hakkı; ikinci fıkrada verilerin bütünlüğü korunmak istendiğinden, rızayı göstermesi gereken kişi birinci fıkra için sistem üzerinde hak sahibi kişiyken; ikinci fıkra için veriler üzerinde hak sahibi kişidir. Sistem sahibinin “sistemin işleyişinin bozulması veya engellenmesine” yönelik rızası; veri sahibinin “verilerin bozulması, yok edilmesi, değiştirilmesi veya erişilmez kılınması, sisteme veri yerleştirilmesi, var olan verilerin başka bir yere gönderilmesine” yönelik rızası fiili

⁶⁷³ Tezcan/ Erdem/ Önok, s. 1171.

⁶⁷⁴ Özbek/ Doğan/ Bacaksız, s. 984; Koca/ Üzülmmez, s. 919.

⁶⁷⁵ Akbulut, s. 40.

⁶⁷⁶ Erdoğan, s. 109-110.

⁶⁷⁷ Artuk/ Gökçen, s. 550.

hukuka uygun hale getirecektir.⁶⁷⁸ Bu rıza açık veya örtülü verilebilir.⁶⁷⁹ Rızanın geçerli olabilmesi için rıza gösterinin iradesi hile, tehdit gibi sebeplerle sakatlanmamış olması yani rızanın özgür iradeyle verilmiş olması gerekir. Ayrıca sisteme veya verilere müdahale niteliğindeki hareketin hukuka uygun kabul edilebilmesi için fiilin rıza çerçevesinde gerçekleştirilmesi, rızanın sınırları dışına çıkılmaması gerekir. Aksi halde işlenen fiil hukuka uygun kabul edilmeyecektir.

Sisteme müdahale niteliğindeki bir harekete rıza gösterecek kimse, sistemin kullanıcısı değil; sistemin sahibi yani mülkiyet hakkı sahibi kimsedir. Ayrıca sistem kullanıcısıyla sistem sahibinin farklı kişiler olduğu durumda, sistem kullanıcısının sistem sahibinin özel verilerine müdahale niteliğindeki hareketlere ilişkin açıklayacağı rıza fiili hukuka uygun hale getirmeyecektir. Aynı şekilde sistem kullanıcısının farklı bir kişi olması durumunda, sistem sahibinin sistem kullanıcısına ait özel verilere müdahale niteliğindeki hareketlere ilişkin açıklayacağı rıza da fiili hukuka uygun hale getirmeyecektir.

Bilişim sistemine müdahale veya sistemdeki verilere müdahale fiilinin meşru müdafaa durumunda işlenmesi halinde, bu fiil suç teşkil etmeyecektir. Örneğin sosyal medya hesabından başkasının uygun olmayan görüntülerini izinsiz paylaşan ve uyarılmasına rağmen hesabından söz konusu fotoğrafları kaldırmayan kimsenin bilişim sistemine, şifresi kırılarak girilmesi ve fotoğrafların silinmesi durumu meşru müdafaa kapsamında değerlendirilebilir.⁶⁸⁰ Ancak savunmayı gerçekleştiren kimsenin, fotoğrafları silmesinin yanında diğer verilere veya sisteme zarar vermesi durumunda artık meşru müdafaada sınırın kasten aşılması söz konusudur. Bu halde verilere müdahale eden

⁶⁷⁸ Tezcan/ Erdem/ Önok, s. 1171.

⁶⁷⁹ Yaşar/ Gökcan/ Artuç, s. 7318.

⁶⁸⁰ Ekici Şahin/Koruculu, s. 610.

kişinin, meşru müdafaada sınırı aşması dolayısıyla gerçekleştirdiği suçtan kasten sorumluluğu doğacaktır.⁶⁸¹

Burada bilişim sistemleri veya veriler üzerinde hak sahibi kimsenin, bilişim sistemini veya verilerini koruyabilmek adına haksız birtakım fiilleri engellemek için önceden önlem alması ve bu çerçevede suç işlemeye kalkışan kimseleri zarara uğratma durumunun meşru müdafa çerçevesinde değerlendirilmesi gerekir. “*Örneğin bilgisayar dünyasındaki korsan kopya veya yazılım olarak adlandırılan izinsiz yazılımların dolaşımını, kullanımını engellemek amacıyla üretici firmalar yani yazılım evleri ürettikleri ürünlerin içine öngörülen usullerin dışında kullanılması halinde sisteme veya ürünün kendisine zarar vermek üzere çeşitli virüsler yerleştirmekte ve bu tertipler sayesinde de bu çeşit ürünün kullanıldığı sistem veya ürünün kendisi çeşitli zarara uğrayabilmektedir.*”⁶⁸² Ceza hukukunda *offendicula* adı verilen bir takım alet veya tertipler marifetiyle bu çeşit davranışların engellenmeye çalışılması genelde yazarlarca kabul edilen bir uygulamadır. Ancak burada gözetilmesi gereken ölçü, korunan yarar ile tecavüzde bulunana verilen zarar arasında denge kurulmasının gereğidir.⁶⁸³ İrlanda Mahkeme’si yazılım sahibinin bu yazılımı lisanssız kullanan kişinin bilişim sistemine mantık bombası göndererek yazılımını sistemden yok etmesi ancak sisteme herhangi bir zarar vermemesi durumunu hukuka uygunluk nedenleri içerisinde değerlendirmiştir.⁶⁸⁴

F. SUÇA ETKİ EDEN SEBEPLER

TCK 244. maddesinin üçüncü fıkrasında cezayı ağırlaştıran bir nedene yer verilmiştir. Fıkra göre 1. ve 2. fıkralarda sayılan fiillerin “*bir banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinde işlenmesi halinde, verilecek ceza yarı oranında artırılır.*” Bu cezayı ağırlaştırıcı nitelikli halin kabul

⁶⁸¹ Ekici Şahin/ Koruculu, s. 610.

⁶⁸² Yazıcıoğlu, s. 256.

⁶⁸³ Yazıcıoğlu, s. 256-257.

⁶⁸⁴ Taşkın, s. 51.

edilmesiyle söz konusu kurum ve kuruluşlarca bilişim sistemleri aracılığıyla yerine getirilen hizmetlere yönelik müdahaleleri engellemek ve dolayısıyla bu hizmetlerden faydalanan toplumun mağdur edilmesini engellemek amaçlanmıştır.⁶⁸⁵ Banka ve kredi kurumlarının bilişim sistemleri, elde edilebilecek haksız ekonomik kazancın büyüklüğü dolayısıyla kişisel bilişim sistemlerine nazaran daha büyük bir hedef olma potansiyeli taşıdığından ve ayrıca kamu kurum ve kuruluşlarının bilişim sistemlerine yönelik müdahale durumunda da kişisel bilişim sistemlerine nazaran çok daha kötü sonuçlar doğabileceğinden, bu kurumların bilişim sistemlerine yönelik müdahaleler ağırlaştırıcı sebep olarak öngörülmüştür.⁶⁸⁶

Cezayı ağırlaştırıcı nitelikli hal yalnızca banka veya kredi kurumu ya da kamu kurum veya kuruluşlarının bilişim sistemlerine yönelik olarak öngörülmüştür. Kurum ve kuruluşlar bakımından böyle bir ağırlaştırıcı halin kabul edilmesi yerinde görülmektedir. Çünkü kişisel bir bilişim sisteminin işleyişine ya da sistemdeki verilere müdahaleyle kurum ve kuruluşun sistemine ya da verilerine müdahaleyle ortaya çıkacak zararın büyüklüğü aynı nitelikte değildir.⁶⁸⁷ Doktrinde bir görüş böyle bir kurum sınırlaması getirilmesini eleştirmiştir. Çünkü başka şirket ya da kurumların bilişim sistemlerinin işleyişine veya verilerine müdahale edilmesi de çok büyük zararlara neden olabilmektedir. Dolayısıyla maddedeki kurum ve kuruluş sınırlaması yerinde görülmemiştir⁶⁸⁸

Bankacılık Kanununun 3. maddesinde banka “Mevduat bankaları ve katılım bankaları ile kalkınma ve yatırım bankalarını”; kredi kuruluşu “Mevduat bankalarını ve katılım bankalarını” ifade eder dendiikten sonra aynı maddenin devamında “*Mevduat bankası: Bu Kanuna göre kendi nam ve hesabına mevduat kabul etmek ve kredi*

⁶⁸⁵ Koca/ Üzülmmez, s. 919; Yaşar/ Gökcan/ Artuç, s. 7314.

⁶⁸⁶ Parlar, s. 28; Taşkın, s. 55-56; Kurt, s. 170.

⁶⁸⁷ Akbulut, s. 41.

⁶⁸⁸ Akbulut, s. 41.

kullandırmak esas olmak üzere faaliyet gösteren kuruluşlar ile yurt dışında kurulu bu nitelikteki kuruluşların Türkiye'deki şubelerini, Katılım bankası: Bu Kanuna göre özel cari ve katılma hesapları yoluyla fon toplamak ve kredi kullandırmak esas olmak üzere faaliyet gösteren kuruluşlar ile yurt dışında kurulu bu nitelikteki kuruluşların Türkiye'deki şubelerini, Kalkınma ve yatırım bankası: 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 eder şeklinde tanımlanmıştır. Burada banka veya kredi kurumu kamuya ait olabileceği gibi özel bir banka veya kredi kurumu olabilir.⁶⁸⁹ Kredi kurumu TCK 158/1-j gerekçesinde “banka olmamasına karşın kanunen borç vermeye yetkili kılınan kurumlardır.” şeklinde tanımlanmıştır. Dolayısıyla Kredi Kurumu ifadesinden bankalar anlaşılmamalıdır.

Üçüncü fıkra da nitelikli halin öngörüldüğü diğer kurumlar, kamu kurum ve kuruluşlarıdır. Öncelikle belirtmek gerekir ki kamu kurumları ifadesi, idare hukukunda “görev ve yetkileri belli bir hizmet ile sınırlı olan hizmet yerinden yönetim kuruluşları” için kullanılan teknik bir ifadedir.⁶⁹⁰ Ancak çeşitli kanunlarda kullanılan kamu kurumları ifadesiyle kanun koyucu çoğu kez sadece hizmet yerinden yönetim kuruluşlarını değil; merkezi idare ve yerel yönetimleri de kapsayacak şekilde tüm idari kuruluşları kastetmektedir.⁶⁹¹ Ceza Kanunu Koyucusu da TCK 244. maddesi için öngördüğü bu nitelikli halde, kamu kurum ve kuruluşları ifadesiyle sadece hizmet yerinden yönetim kuruluşları bakımından değil; “merkezi idare, yerel yönetimler ve hizmet yerinden yönetim kuruluşları da dahil olmak üzere tüm kamu kuruluşları” bakımından ağırlaştırıcı sebep öngörmüştür.⁶⁹²

⁶⁸⁹ Koca/ Üzülmmez, s. 920; Yaşar/ Gökcan/ Artuç, s. 7315.

⁶⁹⁰ Günday, Metin, **İdare Hukuku**, Ankara, İmaj Yayınevi, 2015, s. 532.

⁶⁹¹ Günday, s. 532.

⁶⁹² Akbulut, s. 206-207.

Doktrinde öngörülen ceza açısından sabit artırım sisteminin benimsenmesi eleştirilerek, ağırlaştırıcı sebep bakımından alt ve üst ceza sınırının belirlenmesinin daha isabetli olacağı ileri sürülmüştür. Çünkü sisteminin işleyişine veya verilerine müdahale edilen kurumlar, sistem ve verilerin önem derecesi, sebep olunan zarar cezanın belirlenmesinde dikkate alınmalıydı. Dolayısıyla hem ceza hem de kurumlar bakımından yapılan belirleme yerinde değildir.⁶⁹³

G. SUÇUN ORTAYA ÇIKIŞ BİÇİMLERİ

a. TEŞEBBÜS

TCK 35. maddesine göre bir kimse “işlemeyi kastettiği bir suçu elverişli hareketlerle doğrudan doğruya icraya başlayıp da elinde olmayan nedenlerle tamamlayamaz ise” teşebbüsten sorumlu olacaktır. Doktrindeki bir görüşe göre bu suçlar neticesiz suçlardır ve bu suçlara teşebbüs mümkün değildir.⁶⁹⁴ Ancak bizim de katıldığımız görüşe göre sisteme müdahale ve verilere müdahale niteliğindeki seçimlik hareketlerin icrasına elverişli hareketlerle doğrudan doğruya başlayan fail elinde olmayan nedenlerle neticeleri gerçekleştirememişse teşebbüsten sorumlu olacaktır.⁶⁹⁵ Örneğin bilişim sistemine, sistemin işleyişini bozmak için virüs gönderilmiş ancak sistemdeki anti virüs programı sayesinde sisteme bir şey olmamışsa fail TCK 244/1. maddesine teşebbüsten sorumlu olacaktır.⁶⁹⁶

TCK 244. maddesinde düzenlenen suçlar seçimlik hareketli olduğundan, seçimlik hareketlerden biri teşebbüs aşamasında kalmış ancak bir diğeri işlenmişse, bu durumda

⁶⁹³ Akbulut, s. 41.

⁶⁹⁴ Hafizoğulları/ Özen, s. 453.

⁶⁹⁵ Taşkın, s. 53; Erdoğan’a göre engelleme ve bozma suçun neticeleri olduğundan ve neticeli suçlar teşebbüs mümkün olduğundan bilişim sisteminin işleyişine müdahale suçuna teşebbüs mümkündür. Erdoğan, s. 202.

⁶⁹⁶ Erdoğan, s. 202.

tamamlanmış tek bir suç söz konusu olacak ve failin teşebbüsten değil tamamlanmış suçtan sorumluluğu doğacaktır.⁶⁹⁷

Sistemi bozmak, engellemek ya da veriler üzerinde ikinci fıkrada yazan hareketleri gerçekleştirmek için sisteme giren fail hareketine devam edebilecekken işlemeyi kastettiği suçtan vazgeçerse, gönüllü vazgeçme hükmü (TCK 36) gereği yalnızca sisteme girme suçundan (TCK 243) sorumlu olacaktır.⁶⁹⁸ Doktrinde bir görüş failin TCK 244. maddesindeki eylemleri tamamladıktan sonra vazgeçip, sistemi veya verileri eski haline geri döndürdüğünde de gönüllü vazgeçme hükümlerinin uygulanabileceğini ileri sürmüştür.⁶⁹⁹ Ancak burada artık fail hareketlerini tamamlayıp suçu gerçekleştirdiğinden, gönüllü vazgeçme hükümleri tatbik edilemez. Kanunda etkin pişmanlık hükmüne bu suç bakımından yer verilmediğinden, bu durum ancak TCK 62 gereğince takdiri indirim sebepleri bakımından göz önünde bulundurulabilir.⁷⁰⁰

b. İŞTİRAK

“Tek bir kişi tarafından işlenebilecek bir suçun, birden çok kişi tarafından birlikte gerçekleştirilmesi haline suça iştirak” denmektedir.⁷⁰¹ İştirake ilişkin genel kurallar (TCK 37-40) bu suçlar bakımından da uygulama alanı bulur, özellik arz eden bir durum söz konusu değildir.

TCK 244. maddesinde düzenlenen suçlar ani hareketli olduğundan, sisteme veya verilere müdahale edilmesiyle suç tamamlanır ve suç tamamlandıktan sonra bu suça iştirak mümkün değildir.

Hastane teşhis ve tedavi kayıtlarının bilişim sistemi üzerinden değiştirilerek, hastanın ölümüne neden olunması durumunda bir görüşe göre TCK 244/4. maddesi gereği

⁶⁹⁷ Mahmutoglu, s. 868; Meran, s. 582.

⁶⁹⁸ Kurt, s. 266; Yaşar/ Gökcan/ Artuç, s. 7320.

⁶⁹⁹ Kurt, s. 265-266.

⁷⁰⁰ Erdoğan, s. 233-234.

⁷⁰¹ Yalçın/ Köprülü, s. 513.

failin fiili başka bir suç olan insan öldürme suçuna vücut vereceğinden, fail sadece TCK 81. maddesi uyarınca cezalandırılacaktır.⁷⁰² Ancak bu görüşe katılmak mümkün değildir. Zira ölüm neticesini doğuran fiil, yanlış tedavinin uygulanması suretiyle ilgili sağlık görevlisi tarafından icra edileceğinden, sistemdeki kayıtları değiştiren kişinin dolaylı faillik müessesesi gereği TCK 81’den ve ayrıca verilere müdahale suçundan (TCK 244/2) cezalandırılması gerekir.

TCK 244. maddesini işleyen faile, TCK 245/A maddesinde sayılan şekilde yardım eden kimsenin durumunun özel olarak değerlendirilmesi gerekir. Bir kimsenin TCK 244. maddesindeki suçları işlemesi için TCK 245/A maddesinde sayılan suçu işleyen kimse, iştirak iradesiyle hareket etmemişse sadece TCK 245/A maddesinden; iştirak iradesiyle hareket etmiş ve işlenen fiil üzerinde ortak hakimiyet kurmuşsa hem TCK 244 hem TCK 245/A maddesinden sorumlu olacaktır. Eğer bu kişi bilişim sistemine müdahale veya verilere müdahale suçu bakımından sadece iştirak iradesiyle hareket etmiş ve örneğin suçun işlenmesi için yardım eden sıfatıyla sisteme girme suçunu işleyecek faile bunun için bir program satmışsa, TCK 244. maddesi bakımından yardım eden, TCK 245/A maddesi bakımından fail konumundadır. Failliğin şerikliğı nazaran asliliğı kuralı gereğince bu kimse sadece TCK 245/A maddesinden sorumlu olacaktır.

c. İÇTİMA

1. Genel Olarak

“Bir kimsenin, ceza kanununun aynı veya farklı hükmünü; tek veya birden çok fiille birçok defa ihlal etmesi” durumunda suçların içtimaı söz konusudur. Böyle bir durumda failin sorumluluğı tek bir suçtan ancak cezası ağırlaştırılarak belirlenecektir.⁷⁰³

⁷⁰² Kurt, s. 170.

⁷⁰³ Hafizogulları/ Özen, Genel Hükümler, s. 354.

TCK 244. maddesinde sayılan seçimlik hareketlerin ayrımını yapmak her zaman kolay olmamakta ve bir hareket suçun kanuni tanımında sayılan birden fazla kavramın kapsamında değerlendirilebilmektedir. Aynı fıkra da sayılan hareketler açısından bir sorun olmayacağı kanaatindeyiz zira suç seçimlik hareketli bir suç olarak öngörüldüğünden birden fazla hareketin gerçekleştirilmesi durumunda da tek suç işlenmiş sayılacaktır. Ancak tek bir hareketle farklı fıkralardaki hareketlerin gerçekleşmesi durumunda örneğin sistemi bozmak amacıyla verilerin silinmesi durumunda birinci ve ikinci fıkra açısından nasıl bir uygulamaya gidileceği sorununun çözülmesi gereklidir.

Doktrinde bir görüşe göre bilişim sisteminin işleyişine müdahale niteliğindeki eylemler verilere müdahale niteliğinde olduğundan ve TCK 244. maddesinin ikinci fıkrasının, birinci fıkranın işlenmesi için geçilmesi gereken suç olmasından ötürü iki fıkra arasında geçitli suç ilişkisi vardır.⁷⁰⁴ Buna göre ikinci fıkra yani verilere müdahale birinci fıkradaki suç içerisinde eridiğinden sadece birinci fıkradan hüküm kurulur.⁷⁰⁵ Ancak geçitli suç ilişkisinin söz konusu olabilmesi için; her iki suçun hukuki konularının aynı olması ve hafif suçun işlenmesinin daha ağır suçun işlenmesi için zorunluluk arz etmesi gerekir.⁷⁰⁶ Önceki sayfalarda anlatıldığı üzere birinci fıkra da düzenlenen bilişim sisteminin işleyişine müdahale suçunun hukuki konusu sistem üzerinde hak sahibi kişinin sistemi sağlıklı bir şekilde kullanmasına ilişkin menfaatken; ikinci fıkra da düzenlenen verilere müdahale suçunun hukuki konusu verilerin bütünlüğüdür. Ayrıca bilişim sisteminin işleyişinin engellenmesi veya bozulabilmesi için sistemdeki verilere müdahale etmek zorunluluk teşkil etmez. Örneğin bilişim sisteminin kablosunun çekildiği durumda sistemin işleyişi engellenmekte veya sistemin anakartına zarar verildiği durumda sistemin

⁷⁰⁴ Ketizmen, s. 137.

⁷⁰⁵ Yılmaz, s. 83.

⁷⁰⁶ İçel, İçtima, s. 47-48.

işleyişi bozulmakta ancak verilere müdahale edilmemektedir. Dolayısıyla iki fıkra arasında geçitli suç ilişkisi yoktur.

Doktrinde bir görüş burada failin kastına göre nitelendirmenin yapılması gerektiğini ileri sürmüştür.⁷⁰⁷ Başka bir görüşse bahse konu durumda fikri içtima kurallarının uygulanması gerektiğini savunmuştur.⁷⁰⁸ Bu görüşteki yazarlara göre tek bir fiille iki farklı suç olduğundan fikri içtima kuralı gereği daha ağır cezayı gerektiren suçtan cezalandırma yapılır.⁷⁰⁹

Doktrinde başka bir görüşse burada sadece TCK 244/1. maddesinde düzenlenen sistemin işleyişine müdahale suçunun oluştuğunu ileri sürmüştür. Bu görüşe göre TCK 244/2. maddesindeki verilere müdahale suçunun oluşabilmesi için sistemin işleyişine müdahale söz konusu olmamalıdır.⁷¹⁰ Verilere müdahale neticesinde sistemin işleyişi engellenmiş ya da bozulmuşsa artık TCK 244/2'den değil; TCK 244/1'den sorumluluk söz konusu olacaktır.⁷¹¹ Biz de bu görüşe iştirak ediyoruz.

Önceki bölümde de açıkladığımız üzere TCK 243. ve 244. maddeleri arasındaki ilişki konusunda doktrinde farklı fikirler ortaya atılmıştır. Ancak biz burada gerçek içtima ilişkisi olduğunu ve fail hakkında her suç için ayrı hüküm kurulması gerektiğini düşünmekteyiz.⁷¹²

5846 S FSEK 2. maddesinde bilgisayar programları ilim ve edebiyat eserlerinden sayıldıktan sonra Kanunun 71. maddesinde bir eseri hak sahibi kimsenin yazılı izni olmaksızın çoğaltma, değiştirme, dağıtma, umuma iletme ve yayımlama suç olarak öngörülmüştür. Bilgisayar programları da veri niteliğinde olduğundan bu programlara

⁷⁰⁷ Ancak yazar burada işletim yazılımındaki dosyaların silinmesi halinde artık failin kastının sistemin işleyişini bozmak olduğunun kabul edilmesi gerektiğini ifade etmiştir. Kurt, s. 167.

⁷⁰⁸ Erdağ, s. 290; Erdoğan, s. 236; Akbulut, s. 38.

⁷⁰⁹ Akbulut, s. 44.

⁷¹⁰ Koca/ Üzülmüş, s. 920.

⁷¹¹ Tezcan/ Erdem/ Önok, s. 1169; Parlar, s. 26; Karagülmez, s. 213.

⁷¹² Benzer yönde görüş için bkz. Meran, s. 368.

müdahale hem TCK 244/2 hem de FSEK 71. maddelerini ihlal niteliğinde olabilir. Bu durumda özel kanun olduğundan, FSEK uyarınca hüküm kurulacaktır.⁷¹³

Elektronik İmza Kanunu'nda (EİK) bazı suçlar öngörülmüştür. EİK 16. maddesinde⁷¹⁴ “*imza oluşturma verilerinin izinsiz kullanımı*”; EİK 17. maddesinde⁷¹⁵ “*elektronik sertifikalarda sahtekarlık*” fiilleri suç olarak öngörülmüştür. EİK’de düzenlenen bu suçları oluşturan fiiller, aynı zamanda TCK 244. maddesinde düzenlenen bilişim sistemine müdahale veya verilere müdahale suçlarına vücut verebilir. Bu durumda EİK özel kanun olduğundan, işlenen suçlar bakımından öncelikle uygulama alanı bulacaktır.⁷¹⁶

Yargı kararlarında elektronik veri ve belgelerle ilgili sahtecilik eylemlerinde, resmi belgede sahtecilik suçunun oluşup oluşmayacağı tartışmalıdır. “*Mali müşavir olan sanığın hiçbir iş yerinde çalışmayan kişileri çalışıyor göstermek için şifre ve imza kullanarak Sosyal Güvenlik Kurumuna ait sisteme girerek e-bildirge oluşturma durumunda*” Yargıtay 8. CD⁷¹⁷ TCK 204. maddesinin; Yargıtay 11. CD⁷¹⁸ TCK 244/2. maddesinin oluştuğuna kanaat getirmiştir.⁷¹⁹

⁷¹³ Erdoğan, s. 243.

⁷¹⁴ İmza oluşturma verilerinin izinsiz kullanımı

Madde 16- (Değişik: 23/1/2008 – 5728/525 md.)

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.

⁷¹⁵ Elektronik sertifikalarda sahtekarlık

Madde 17- (Değişik: 23/1/2008 – 5728/526 md.)

Tamamen veya kısmen sahte elektronik sertifika oluşturanlar veya geçerli olarak oluşturulan elektronik sertifikaları taklit veya tahrif edenler ile bu elektronik sertifikaları bilerek kullananlar, iki yıldan beş yıla kadar hapis ve yüz günden az olmamak üzere adli para cezasıyla cezalandırılır. Yukarıdaki fıkra da belirtilen suçlar elektronik sertifika hizmet sağlayıcısı çalışanları tarafından işlenirse bu cezalar yarısına kadar artırılır.

⁷¹⁶ Başlar, Yusuf, Elektronik İmza Kanunu'nda Düzenlenen Bilişim Suçları, s. 16.

⁷¹⁷ 12.12.2013 E. 2013/31911, K. 2013/29069.

⁷¹⁸ 27.11.2017 E. 2015/8801, K. 2017/8230.

⁷¹⁹ Özsoy, s. 333-334.

Doktrinde de elektronik belgenin TCK bakımından belge sayılarak, belgede sahtecilik suçlarına konu olup olamayacağı tartışmalıdır. Bazı yazarlar, belgeden söz edilebilmesi için yazılı kâğıt veya maddi varlığın zorunlu olduğunu, ayrıca kanunilik ilkesi gereğince bilişim sistemindeki verilerin sahtecilik suçlarının konusu olabilmesi ve ceza kanunun korumasından faydalanabilmesi için bunun kanunda açıkça düzenlenmesi gerektiğini ileri sürmektedir. Kısacası bu yazarlara göre elektronik ortamdaki evraklar üzerinde değişiklik yapılması veya bir bilişim sistemindeki verilerin değiştirilmesi suretiyle yanıltıcı belgelerin hazırlanması durumu belgede sahtecilik suçu içerisinde değerlendirilemeyecektir.⁷²⁰ Doktrindeki karşıt görüşe göre güvenli imzalı elektronik belgeler, klasik anlamda belgenin taşınması gereken tüm unsurlara sahip olduğundan sahtecilik suçuna konu olabilecek yani TCK anlamında belge sayılmaları gerekir.⁷²¹ TCK’da her ne kadar verilerin belgede sahtecilik suçuna konu olabileceğine dair açık bir hüküm bulunmasa da aksi yönde yani verilerin belgede sahtecilik suçuna konu olamayacağına dair de bir hüküm yoktur. Ayrıca EİK 5. maddesinde “*güvenli elektronik imza, elle atılan imza ile aynı hukukî sonucu doğurur*” denilerek elektronik belgelerin de fiziki belgeler gibi kabul edileceği belirtilmiştir. Sonuç olarak güvenli elektronik imzalı belgeler belge sayılmak için zorunlu her unsura sahip olduğundan, buna dair açık bir hüküm olmasa da sahtecilik suçuna konu olabileceğinin kabulü kıyas yasağı ve biçimsel kanunilik ilkesiyle çelişmemektedir.⁷²²

Bilişim sistemlerinde bulunan verilerin ve belgelerin, günümüz teknolojik şartlarında belgede sahtecilik suçlarının koruma kapsamı dışında bırakılması, her türlü veri işlemin artık bilişim sistemleri aracılığıyla elektronik ortamda gerçekleştirildiği

⁷²⁰ Arslan, Çetin/ Baştürk İhsan: Belgede Sahtecilik Suçunun Konusu Olarak Elektronik Ortamdaki Veriler, **EÜHFD**, C. 8, S. 2, 2013, s. 204.

⁷²¹ Gözel, Arif: Belgede Sahtecilik Suçlarının Konusu Olarak Belge ve Elektronik Belge, **SDÜHFD**, C. 5, S. 1, 2015, s. 189.

⁷²² Akın, Gülfer: Belgede Sahtecilik Suçlarının Konusu Olarak Elektronik/ Dijital Belge, **Bilişim Hukuku Dergisi**, C. 3, S. 1, 2021, s. 101.

düşünüldüğünde zamanın ihtiyaçlarıyla bağdaşmamaktadır. Kanun gerekçesi bağlayıcı olmadığından ve kanun metninde sadece belge denildiğinden bilişim sistemlerindeki verilerin ve elektronik belgelerin, belgede sahtecilik suçlarına konu olabileceği ve bu suçların düzenlendiği maddelerin korumasından faydalanabilecekleri kabul edilmelidir.⁷²³

Bu görüşe paralel olarak, Adalet Bakanlığı Kanunlar Genel Müdürlüğünün Temmuz 2015'te yayınladığı kanun tasarısı taslağında TCK 244. maddesine yeni bir fıkra eklenmesi suretiyle ikinci fıkrada sayılı seçimlik hareketlerin işlenmesi aracılığıyla sahte belge düzenlenmesi durumunda ayrıca belgede sahtecilik suçundan da hüküm kurulacağı belirtilmiştir.⁷²⁴ Dolayısıyla güvenli elektronik imzanın bulunması şartıyla verilerin sahtecilik suçuna konu olabileceği kabul edilmelidir. Güvenli elektronik imza bulunmayan verilerse belge niteliğinde olmayacağından belgede sahteciliğe değil ancak şartların bulunması durumunda TCK 244/2. maddesi çerçevesinde korunacaktır.⁷²⁵

Yargıtay Ceza Genel Kurulu da bir kararında gerçeğe aykırı elektronik işe giriş bildirgesi düzenlenmesini evrakta sahtecilik olarak değerlendirmiştir.⁷²⁶

⁷²³ Gözel, s. 156; Akın, s. 95.

⁷²⁴ Gözel, s. 192.

⁷²⁵ Gözel, s. 164.

⁷²⁶ “gerçeğe aykırı elektronik işe giriş bildireleri düzenlediği olayda; suç tarihinde yürürlükte bulunan Sosyal Sigorta İşlemleri Yönetmeliği'nin 11 ve 15. maddeleri gereğince elektronik ortamda düzenlenmesi gereken işe giriş bildirelerinin 5510 Sayılı Kanun'un 100. maddesi gereğince adli ve idari makamlar nezdinde resmî belge niteliğinde olacağı ve elektronik ortamda düzenlenecek bu belgeler üzerinde yapılacak sahtecilik eylemlerinin de resmî belgede sahtecilik suçunu oluşturacağı öngörülmüş ve Yerel Mahkemece sanık hakkında TCK'nın 204. maddesinin birinci fıkrasında düzenlenen resmî belgede sahtecilik suçundan mahkûmiyet hükmü kurulmuş ise de aynı Kanun'un 244. maddesinin ikinci fıkrasındaki "Bir bilişim sistemindeki verileri bozan, yok eden, değıştiren veya erişilmez kılan, sisteme veri yerleştiren, var olan verileri başka bir yere gönderen kişi, altı aydan üç yıla kadar hapis cezası ile cezalandırılır" şeklindeki düzenleme karşısında sanığın eyleminin aynı zamanda bilişim sistemine veri yerleştirme suçunu da oluşturduğu, TCK'nın 244. maddesinin ikinci fıkrasındaki bu düzenlemenin elektronik belgelerde yapılacak sahtecilik eylemlerine ilişkin özel norm niteliğinde olduğu ve özel normun önceliği ilkesi gereğince de sanık hakkında genel normun değil özel normun uygulanması gerektiği hususları göz önünde bulundurulduğunda, sanığın eyleminin TCK'nın 204. maddesinin birinci fıkrasında yer alan resmî belgede sahtecilik suçuna göre özel norm niteliğinde olan aynı Kanun'un 244. maddesinin ikinci fıkrasındaki bilişim sistemine veri yerleştirme suçunu oluşturduğu kabul edilmelidir.” YCGK E. 2017/8-1122, K. 2020/381, K.T. 29.09.2020.

2. Bileşik Suç

TCK 42. maddesine göre “*Biri diğerinin unsurunu veya ağırlaştırıcı nedenini oluşturması dolayısıyla tek fiil sayılan suça bileşik suç denir. Bu tür suçlarda içtima hükümleri uygulanmaz.*” Bilişim sisteminin işleyişine veya verilere müdahale suçu bileşik suç değildir. Çünkü bu suçlar bakımından farklı suçların bir araya gelip yeni suçun unsuru olmaları veya suçların yan yana gelerek birinin diğerinin ağırlaştırıcı nedeni olması söz konusu değildir.

Bilişim sisteminin işleyişine müdahale veya verilere müdahale suçu başka bir suçun unsurunu ya da nitelikli halini oluşturuyorsa TCK 42. maddesi gereği artık bileşik suç söz konusu olacak ve sadece o düzenlemeden sorumluluk doğacaktır. Yani hem TCK 244’ten hem de diğer suçtan sorumluluk söz konusu olmayacaktır. TCK 244/4. maddesindeki suç bileşik suçtur. Zira TCK 244. maddesinin birinci ve ikinci fıkrasındaki hareketler bu suç için unsur niteliğindedir. Dolayısıyla TCK 42. maddesi gereği ayrıca TCK 244/1 veya 2’den cezalandırma yapılmayacak sadece TCK 244/4. maddesinden ceza verilecektir.⁷²⁷

3. Zincirleme Suç

Sistemin işleyişine müdahale veya verilere müdahale suçları açısından zincirleme suç hükümlerinin uygulanması mümkündür.⁷²⁸ Buna göre TCK 43/1. maddesi gereğince “*bir suç işleme kararının icrası kapsamında değişik zamanlarda bir kişiye karşı aynı suçun birden fazla işlenmesi durumunda*” tek ceza verilecek ve ceza belli oranda artırılacaktır. Örneğin sistemdeki verileri değiştirmek amacıyla farklı zamanlarda aynı kişinin bilişim sisteminden o kişiye ait verileri silen kimsenin sorumluluğu TCK 43/1. maddesine göre belirlenecektir.

⁷²⁷ Koca/ Üzülmüş, s. 930.

⁷²⁸ Meran, s. 582; Taşkın, s. 54.

Bir kimsenin tek bir maille birden fazla kişiye virüs göndererek, bu kişilerin bilişim sistemlerinin işleyişini bozması durumunda, TCK 43/2. maddesinde düzenlenen “*aynı suçun birden fazla kişiye karşı tek bir fiille işlenmesi*” durumu söz konusu olacaktır. Bu durumda failin cezası TCK 43/1. maddesine göre belirlenecektir.

4. Fikri İçtima

TCK 44. maddesi gereği “*İşlediği bir fiil ile birden fazla farklı suçun oluşmasına sebebiyet veren kişi, bunlardan en ağır cezayı gerektiren suçtan dolayı cezalandırılır.*” Bilişim sisteminin işleyişinin engellenmesi veya bozulması suretiyle TCK 124. maddesi (haberleşmenin engellenmesi suçu) de gerçekleştirilmiş olabilir. Haberleşme için kullanılan bir sistemin virüs aracılığıyla çalışmasının engellenmesi durumunda hem TCK 244 hem TCK 124. (“*haberleşmenin engellenmesi*”) maddelerindeki suçlar gerçekleşir.⁷²⁹ Fail tek bir fiille hem haberleşmeyi engellemiş hem de sistemin işleyişine veya verilere müdahale etmişse fikri içtima kuralı uygulama alanı bulacak ve daha ağır cezanın öngörüldüğü TCK 244. maddesinden hüküm kurulacaktır.⁷³⁰

Mala zarar verme suçu ve TCK 244/1. maddesi arasındaki içtima ilişkisi doktrinde tartışmalıdır.⁷³¹ Doktrinde bir görüş buradaki problemin genel norm-özel norm ilişkisi çerçevesinde çözülebileceğini savunmaktadır ve TCK 244. maddenin TCK 151. maddeye göre özel norm olduğunu iddia etmektedir.⁷³² Ancak özel norm-genel norm ilişkisinden bahsedilebilmesi için özel normun genel normun taşıdığı tüm unsurları içermesi ayrıca bu unsurların yanında farklı bir unsur içermesi gerekmektedir. Yani bu unsur olmasaydı fiil, genel norma göre zaten cezalandırılabilirdi diyorsak özel norm-genel norm ilişkisi

⁷²⁹ Özbek/ Doğan/ Bacaksız, s. 986.

⁷³⁰ Erdoğan, s. 203.

⁷³¹ Veriler mal olmadığından, TCK 151 ve 244. maddeleri arasındaki ilişkinin tespiti ilk fıkra özelinde yapılacaktır.

⁷³² Yazar burada aynı hukuki değeri koruyan iki farklı madde olduğunu ve özel koruma sağlayan TCK 244. maddesinin olaya uygulanması suretiyle bu sorunun çözülebileceğini savunmaktadır. Mahmutoglu, s. 869.

vardır. Fakat TCK 151 ve TCK 244. maddelerinde düzenlenen suçlar çok farklı unsurlar ihtiva ettiğinden bu iki suç arasında özel norm-genel norm ilişkisi yoktur. Zira bilişim sisteminin işleyişini engellemek veya bozmak için sistemin soyut unsurlarına yönelik müdahale TCK 151. maddesi çerçevesinde değerlendirilemeyecektir.⁷³³

Doktrindeki başka bir görüşe göre bu iki suçu ayırma konusunda failin kastı belirleyicidir. Nitekim gerek suçların maddi konularının gerek suçların hukuki konularının farklı olması nedeniyle iki maddede aslında farklı şeyler düzenlenmektedir.⁷³⁴ Dolayısıyla failin kastı mağdurun bir malvarlığı değeri olan bilişim sisteminin fiziki varlığına zarar vermekse TCK 244. maddesi değil; TCK 151. maddesi uygulanacaktır.⁷³⁵ Failin kastı bilişim sisteminin işleyişini engellemek, bozmak amacıyla sistemin fiziki varlığına zarar vermekse, TCK 244. maddesi uygulanacaktır.⁷³⁶ Ancak burada kastın belirlenmesi failin iç dünyasına ilişkin bir değerlendirme olduğundan her zaman doğru sonuçlara götürmeyebilir. Dolayısıyla bu görüşe katılmıyoruz.

Suçun maddi konusunun bilişim sisteminin soyut unsurları olduğunu savunan görüşe göre; TCK 244. maddesinin maddi konusunu teşkil eden sistem ve veriler klasik anlamda mal kavramı içerisinde değerlendirilemez.⁷³⁷ Dolayısıyla bilişim sisteminin soyut unsurlarına yönelik müdahale TCK 244. maddesi; donanıma yönelik müdahalelerse TCK 151. maddesi kapsamındadır.⁷³⁸

Bizim de katıldığımız görüşe göre bilişim sistemine fiziki bir saldırının varlığı halinde sistemin işleyişinin bozulması söz konusu olduğu gibi mülkiyete dair bir unsur da zarara uğratılmaktadır. Dolayısıyla sistemin donanım yani fiziki unsurlarına hasar verildiği durumda, tek fille TCK 151 ve TCK 244/1. maddelerindeki suçlar birlikte

⁷³³ Hafizoğulları/ Özen, s. 453.

⁷³⁴ Taşkın, s. 55; Soyaslan, s. 707.

⁷³⁵ Soyaslan, s. 699.

⁷³⁶ Orta, s. 117.

⁷³⁷ Dülger, s. 346.

⁷³⁸ Hafizoğulları/ Özen, s. 453.

işlenmiş olacağından fikri içtima kuralı gereği daha ağır cezayı gerektiren TCK 244/1. maddesinden hüküm kurulacaktır.⁷³⁹ Yani bilişim sisteminin donanım veya yazılım unsuruna yönelik, sistemin işleyişine müdahale niteliğindeki fiiller TCK 244/1. maddesinin uygulama alanında değerlendirilecektir.⁷⁴⁰

Bir kimse başkasına ait verilerin de bulunduğu kendi bilişim sistemine fiziki bir zarar vermek suretiyle verilere de zarar vermişse sadece TCK 244/2. maddesi gereği sorumluluğu söz konusu olacaktır. Çünkü TCK 151. maddesindeki suçun işlenebilmesi için başkasına ait bir mala zarar verilmesi gerekir.⁷⁴¹

TCK 244/2. maddesinde geçen “*bilişim sistemindeki verilerin başka yere gönderilmesi*” seçimlik hareketi aynı zamanda TCK 136. maddesinde düzenlenen “*kişisel verileri, hukuka aykırı olarak bir başkasına verme, yayma veya ele geçirme*” suçuna da vücut vermektedir. Dolayısıyla “*verilerin başka yere gönderilmesi*” seçimlik hareketi bakımından TCK 244 ve TCK 136. maddeleri arasında fikri içtima ilişkisi söz konusu olabilir.⁷⁴² Bu durumda daha ağır bir ceza öngörüldüğünden TCK 136. maddesine göre failin cezası belirlenecektir.

Bir bilişim sistemindeki verilere müdahale edilerek sahte belge düzenlenmesi halinde nasıl bir uygulama yapılacağı hususunda öğretide farklı fikirler ortaya atılmış. Bir görüş bilişim sistemindeki verilerin değiştirilmesi veya sisteme veri eklenmesi suretiyle sahte bir belgenin düzenlenmesine sebep olan failin sorumluluğunun TCK 244 ve TCK 212. maddeleri arasındaki fikri içtima ilişkisi gereğince belirleneceğini savunmaktadır.⁷⁴³ Başka bir görüşse, bilişim sistemine veri ekleyerek veya sistemdeki mevcut verileri

⁷³⁹ Akbulut, s. 27; Kurt, s. 165.

⁷⁴⁰ Erdoğan’a göre failin amacının iyi bir şekilde tespit edilmesi gerekir. Eğer failin kastı sadece mala zarar vermeyse fikri içtima kuralına gidilmez ve sadece mala zarar verme suçundan hüküm kurulur. Ancak failin kastı sistemin işleyişinin engellenmesi veya bozulmasına yönelikse fikri içtima kuralı uygulanır. Erdoğan, s. 206.

⁷⁴¹ Akbulut, s. 45.

⁷⁴² Erdoğan, s. 237; Akbulut, s. 46.

⁷⁴³ Erdoğan, s. 237-238; Akbulut, s. 46.

değiştirerek, bir belgenin gerçeğe aykırı bir şekilde düzenlenmesini veya değiştirilmesini sağlayan failin hem belgede sahtecilikten hem de TCK 244/2. maddesinden cezalandırılacağını savunmaktadır.⁷⁴⁴ Biz de bu görüşe iştirak ederek gerçek içtima kuralı uyarınca ayrı ayrı iki suçtan ceza verilmesi gerektiğini savunuyoruz.

H. YAPTIRIM, SORUŞTURMA, KOVUŞTURMA

TCK 244/1. maddesinde düzenlenen sistemin işleyişine müdahale suçu için yaptırım olarak “*bir yıldan beş yıla kadar hapis cezası*” öngörülmüştür. TCK 244/2. maddesinde düzenlenen verilere müdahale suçu için “*altı aydan üç yıla kadar hapis cezası*” öngörülmüştür. TCK 244/3. maddesinde düzenlenen suçun nitelikli hali için verilecek cezanın yarı oranında artırılacağı belirtilmiştir.

TCK 244. maddesi için öngörülen yaptırımlar caydırıcılık sağlayamaması dolayısıyla eleştirilmektedir.⁷⁴⁵ Öngörülen bu cezaların alt sınırları gerek bu suçların işlenme oranlarının fazla olması gerekse suçlarla verilen zararların maliyetinin çok büyük miktarları bulması dolayısıyla yetersiz bulunmaktadır.⁷⁴⁶ Ayrıca bu suçlar aracılığıyla çok büyük maddi zararlara yol açılabildiğinden, mala zarar verme suçuna benzer olarak hapis cezasının yanında adli para cezasının öngörülmesi gerektiği de ifade edilmektedir.⁷⁴⁷

İlk iki fıkrada gösterilen suçlar karşılığı öngörülen cezaların alt sınırları altı ay ve bir yıl olduğundan, hâkimin cezayı alt sınırdan belirlemesi durumunda TCK 50/1’e göre hapis cezasının adli para cezasına ya da diğer bir tedbire dönüştürülmesi mümkündür. Fakat bu durumda hapis cezasının ertelenmesi söz konusu olmayacaktır.⁷⁴⁸

Mahkemece kurulan hüküm sonucu faile iki yıldan daha az hapis cezasının verilmesi halinde diğer koşulların da bulunması halinde CMK 231. maddesi gereğince

⁷⁴⁴ Mahmutoğlu, s. 870.

⁷⁴⁵ Akbulut, s. 47.

⁷⁴⁶ Koca/ Üzülmüş, s. 921.

⁷⁴⁷ Akbulut, s. 52.

⁷⁴⁸ Meran, s. 583.

hükmün açıklanması geriye bırakılabileceği gibi TCK 51. maddesi gereğince hapis cezasının ertelenmesi de mümkündür.⁷⁴⁹

Sistemin işleyişine müdahale suçu, verilere müdahale suçundan daha ağır nitelikte görüldüğünden, birinci fıkrada ikinci fıkra nazaran daha ağır bir ceza öngörülmüştür. Doktrinde bir görüşe göre sisteme müdahale niteliğindeki bir hareket için verilere müdahale niteliğindeki bir harekete göre daha fazla ceza öngörülmesi yerinde bir düzenleme olmamıştır. Zira sisteme müdahale kablonun prizden çekilmesi suretiyle dahi işlenebiliyorken sistemdeki verilere müdahale çok daha uzmanlık gerektirebildiğinden, suç politikası açısından sakıncalı bir düzenlemedir. Dolayısıyla verilere müdahale niteliğindeki eylemlere ilişkin daha fazla ceza veya verilerin niteliğine göre bir ağırlaştırıcı neden öngörülmesi düşünülebilirdi.⁷⁵⁰ Gerçekten de verilere müdahale niteliğindeki fiiller, sisteme müdahale niteliğindeki fiillerden çok daha vahim sonuçlar doğurabilmektedir. Fakat her somut olayda durum böyle olmayabilir, sistemin işleyişine müdahale daha vahim sonuçlar doğurabilir. Dolayısıyla burada verilere müdahale durumunda daha fazla ceza öngörülmesi yerine; sistemde yer alan verilerin sistemin kendisinden çok daha değerli olduğu haller için ikinci fıkrada öngörülen cezanın artırılması konusunda düzenleme yapılması daha isabetli bir çözüm olacaktır.⁷⁵¹

TCK 244. maddesinde düzenlenen suçlar resen soruşturulan, kovuşturulan suçlardır. Görevli mahkeme 5235 S Kanun 11. ve 12. maddeleri uyarınca asliye ceza mahkemeleridir. 30.11.2021 tarihli Resmi Gazete yayımlanan HSK'nın 1229 numaralı kararı gereğince 15.12.2021 tarihinden itibaren görev yapacak Bilişim İhtisas Mahkemeleri belirlenmiştir.⁷⁵² Karara göre “*iki asliye ceza mahkemesi bulunan yerlerde*

⁷⁴⁹ Erdoğan, s. 207.

⁷⁵⁰ Yazıcıoğlu, s. 409.

⁷⁵¹ Karagülmez, s. 220.

⁷⁵² Doktrinde bir görüşe göre özel uzmanlık mahkemelerin kurulması, mahkemelerin yetki ve görevlerine ilişkin karmaşaya yol açacağından bilişim suçlarıyla alakalı teknik konularda bilirkişiye başvurulması daha yerinde bir tercih olacaktır. Ünver, s. 145

2; üç, dört veya beş asliye ceza mahkemesi bulunan yerlerde 3; altı, yedi, sekiz veya dokuz asliye ceza mahkemesi bulunan yerlerde 6; on veya daha fazla asliye ceza mahkemesi bulunan yerlerde 8; yirmi beş veya daha fazla asliye ceza mahkemesi bulunan yerlerde 20 ve 21; otuz beş veya daha fazla asliye ceza mahkemesi bulunan yerlerde 20, 21, ve 22 numaralı asliye ceza mahkemeleri ihtisas mahkemesi olarak” görevlendirilmiştir.

CMK 12. maddesi gereğince yetkili mahkeme suçun işlendiği yer mahkemesidir. Yetkili mahkemenin belirlenmesiye bilişim alanında suçlarda zaman ve mekân sınırının olmaması dolayısıyla her zaman kolay olmamaktadır. Şayet müdahale edilen sistem veya veriler, fiilin işlendiği yerde bulunuyorsa yetkili mahkemenin belirlenmesi konusunda bir sorun çıkmamaktadır. Sorun bilhassa ağlar aracılığıyla gerçekleştirilen sisteme veya verilere müdahale suçlarında ortaya çıkmaktaydı. Zira ağların kaldırmış olduğu coğrafi sınırlar olmaksızın dünyanın bir ucundan, diğer ucuna işlenen bilişim suçlarında hareket başka yerde, netice başka yerde gerçekleşmektedir.⁷⁵³ İşte böyle durumlarda suçun nerede işlenmiş sayılacağı başka bir ifadeyle suçun işlenmesinde araç olarak kullanılan sistemin bulunduğu yer mi yoksa müdahale edilen sistemin veya verilerin bulunduğu yer mi suçun işlendiği yer sayılacağı sorunu karşımıza çıkmaktaydı.⁷⁵⁴ Bu sorunu çözmek için 7331 S Kanunla 08.07.2021 tarihinde CMK 12. maddesine eklenen altıncı fıkra gereğince “Bilişim sistemlerinin, banka veya kredi kurumlarının ya da banka veya kredi kartlarının araç olarak kullanılması suretiyle işlenen suçlarda mağdurun yerleşim yeri mahkemeleri de yetkilidir.” Yani artık failin fiili işlediği yer mahkemesi ve mağdurun bulunduğu yer mahkemesi yetkili olacağından, birden fazla yetkili mahkeme söz konusudur.

⁷⁵³ Bir görüş burada hareketin nerede işlendiğinin tespit edilebildiği durumlarda, suçun hareketin gerçekleştirildiği yerde işlendiğinin; hareketin nerede icra edildiğinin belirlenmediği durumlardaysa neticenin meydana geldiği yer mahkemesinin yetkili mahkeme kabul edilmesi gerektiğini savunmaktaydı. Özbek/ Doğan/ Bacaksız, s. 986.

⁷⁵⁴ Hem suçun işlenmesinde araç olarak kullanılan bilişim sisteminin bulunduğu yerin hem de üzerinde suçun işlendiği bilişim sisteminin bulunduğu yerin suçun işlendiği yer olarak kabul edilmesi gerektiğini savunan görüş için bkz. Mahmutoğlu, s. 860.

TCK 66. maddesi gereğince “beş yıldan fazla olmamak üzere hapis veya adli para cezasını gerektiren suçlarda sekiz yıl” geçmesiyle kamu davası düşeceğinden bilişim sistemine veya verilere müdahale suçları için dava zamanaşımı sekiz yıldır.

II. BİLİŞİM SİSTEMİ ARACILIĞIYLA HAKSIZ YARAR SAĞLAMA SUÇU

A. GENEL OLARAK

Teknolojik gelişmeler sonucunda ekonomik değerlerin bilişim sistemlerinde veri olarak temsil edilmesi ve bu veriler üzerinde işlem yapılabilmesi, ekonomik değerlerin temsili değişimini mümkün kılmış bu durumsa veri olarak temsil edilen ekonomik değerlerin bilişim sistemi aracılığıyla haksız müdahalelere maruz kalmasına neden olmuştur.⁷⁵⁵ Bilişim sistemi aracılığıyla haksız yarar sağlama suçunda veri olarak temsil edilen malvarlığına dahil değerlerin bilişim sistemine veya verilere müdahale edilmesi suretiyle haksız bir şekilde elde edilmesi söz konusudur.⁷⁵⁶

765 S TCK dönemi 525 b/2. maddesi⁷⁵⁷ bilişim sistemi aracılığıyla haksız yarar sağlama suçunun karşılığını oluşturmaktaydı.⁷⁵⁸ Söz konusu maddenin uygulama alanına yürürlükteki TCK 142/2-e, TCK 158/1-f, TCK 245 maddeleri de dahil olduğundan, maddenin kapsamı oldukça geniştir. ETCK 525 b/2 maddesinde suçun maddi unsuruna yönelik herhangi bir sınırlama getirilmemesi suçların ve cezaların kanuniliği ilkesinin bir gereği olan belirlilik ilkesini ihlal edici nitelik taşımaktaydı.⁷⁵⁹ Bu durum, 5237 S TCK’da suçun maddi unsurunun sisteme müdahale ve verilere müdahale niteliğindeki hareketler suretiyle gerçekleştirilebileceğinin öngörülmesiyle engellenmiştir.

⁷⁵⁵ Ketizmen, s. 144-145.

⁷⁵⁶ Ketizmen, s. 145.

⁷⁵⁷ Madde: “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.”

⁷⁵⁸ Açıkgöz, s. 64.

⁷⁵⁹ Ketizmen, s. 176-177.

TCK 244/4. maddesi “*Yukarıdaki fıkralarda tanımlanan fiillerin işlenmesi suretiyle kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlamanın başka bir suç oluşturmaması halinde, iki yıldan altı yıla kadar hapis ve beşbin güne kadar adli para cezasına hükmolunur.*” şeklinde düzenlenmiştir.

“*Bilişim sistemi aracılığıyla haksız yarar sağlama suçu*”, TCK 244. maddesinde ilk iki fıkra da sayılan hareketlerin gerçekleştirilmesi suretiyle işlenebilen bir suç olarak tanımlandığından, doktrinde dördüncü fıkranın hukuki niteliğine ilişkin farklı görüşler ortaya çıkmıştır. Bir görüşe göre dördüncü fıkra, temel suçun düzenlendiği ilk iki fıkra ya bağlı düzenlendiğinden, esasen sisteme ve veriye müdahale suçlarının daha ağır cezayı gerektiren nitelikli halidir.⁷⁶⁰ Ancak madde metni incelendiğinde her ne kadar tipik hareket tanımlaması ilk iki fıkra ya atıf yapılmak suretiyle yapılsa da bu hareketler aracılığıyla haksız yarar sağlama fiili tipik hareket olarak öngörülmüştür. Yani suçun fiil unsuru sadece sisteme veya verilere müdahale niteliğinde olmaktan çıkmış ve yeni bir fiil haline gelmiştir. Suça etki eden sebepler olarak adlandırılan suçun nitelikli hallerinde fiil unsuru aynı kalmakta ancak mağdurun veya failin kişiliği, fiilin işleniş biçimi gibi sebeplerle cezanın daha ağır veya hafif olarak öngörülmesi söz konusudur. Ayrıca TCK 244/4. maddesi için failin kastı sadece sisteme veya verilere müdahale olmayıp; haksız yarar sağlamaya yönelik olmalıdır. Hakeza dördüncü fıkra da düzenlenen bu suç hukuki konusu itibariyle 244/1-2. maddesinde düzenlenen suçlardan farklıdır.⁷⁶¹ Kısacası dördüncü fıkra da düzenlenen suç ilk iki fıkra da düzenlenen suçlardan farklı maddi, manevi unsur ve hukuki konuya sahip olduğundan bu suçların aynı madde başlığı altında düzenlenmesi yerinde bir düzenleme olmamıştır. Dolayısıyla bu suç müstakil bir suç olarak değerlendirilmelidir.⁷⁶²

⁷⁶⁰ Kurt, s. 161; Orta, s. 118; Özbek/ Doğan/ Bacaksız, s. 978.

⁷⁶¹ Yazıcıoğlu, s. 410.

⁷⁶² Açıkgöz, s. 62; Apaydın, s. 27; Erdoğan, s. 247; Koca/ Üzülmüş, s. 921.

Türkiye AKSSS'ye taraf olmanın yükümlülüğü olarak mevzuatını uyumlu hale getirmek için Sözleşmenin 8. maddesinde⁷⁶³ düzenlenen “bilgisayarla bağlantılı dolandırıcılık” başlıklı suçu TCK 244/4. maddesinde düzenlemiştir.⁷⁶⁴ AKSSS 8. maddesinde suçun, maddi yarar sağlamak için hile veya sahtekarlık niyetiyle başkasının zararına olacak şekilde işlenmesi öngörülmüş; TCK'da ise Sözleşmeden farklı olarak suçun maddi yarar sağlamak amacıyla hile veya sahtekarlık niyetiyle başkasının zararına olacak şekilde işlenmesine tipik fiilde yer verilmemiştir.⁷⁶⁵

Madde metninde failin fiilinin “başka bir suç oluşturmaması halinde” maddede gösterilen cezaya hükmedileceği öngörülmüştür. Bu ifade bu hükmün tali norm niteliğini ortaya koymaktadır.⁷⁶⁶ Dolayısıyla sisteme müdahale veya verilere müdahale yoluyla haksız çıkar sağladığında, bu fiilin örneğin hırsızlık, dolandırıcılık gibi başka bir suça vücut verip vermediğine bakılarak uygulanacak madde belirlenmesi yapılmalıdır. Eğer fiil başka maddedeki suç tanımına giriyorsa bu maddeden; girmiyorsa TCK 244/4'ten cezaya hükmedilmelidir. Kısacası TCK 244/4. maddesi sisteme veya verilere müdahale etme suretiyle haksız yarar elde etme fiiline uygulanacak asıl hüküm değildir; fiil başka suçlar bakımından tipiklik arz ediyorsa öncelikle o madde hükmü uygulama alanı bulacaktır.⁷⁶⁷

Madde gerekçesinde madde metninden farklı olarak “*fiilin daha ağır bir cezayı gerektiren başka bir suç oluşturmaması gerekir*” denilerek fikri içtima ilişkisinin geçerli olacağından bahsedilmiş. Ancak gerekçenin bağlayıcı olmaması dolayısıyla madde metnindeki ifadeye göre değerlendirme yapılacak ve cezanın daha ağır olup olmadığına

⁷⁶³ Madde-8 Bilgisayarla Bağlantılı Dolandırıcılık

“Taraflardan her biri, aşağıda belirtilenler, kasten ve haksız yere gerçekleştirildiği zaman, bir başka şahsın mal kaybına sebebiyet verdiğinde, bunların kendi iç hukukunda cezai suç olarak tanımlanması için gerekli olabilecek yasama tedbirlerini ve diğer tedbirleri kabul edecektir.

Şahısların kendilerine veya başkasına haksız yere maddi menfaat sağlamak için hile veya sahtekarlık niyetiyle;

a) Bilgisayar sistemlerine veri girişi yapmak, verileri değiştirme, silme veya engelleme;

b) Bir bilgisayar sisteminin işleyişine herhangi bir müdahalede bulunma.”

⁷⁶⁴ Açıkgöz, s. 65; Taşkın, s. 56.

⁷⁶⁵ Erdoğan, s. 250; Açıkgöz, s. 66.

⁷⁶⁶ Koca/ Üzülmüş, s. 922; Ketizmen, s. 178.

⁷⁶⁷ Koca, s. 97.

bakılmaksızın fiilin başka bir suça vücut verip vermediğine göre ceza belirlenecektir.⁷⁶⁸

Madde metniyle gerekçe arasındaki uyumsuzluğun giderilmesi gereklidir.⁷⁶⁹

B. HUKUKİ KONU

Doktrinde bir görüşe göre suçun hukuki konusu “*bilişim sistemleri kullanılarak, başkasının zararına, haksız çıkar sağlanıp bilişim ortamının güvensiz kılınmasının önlenmesine ilişkin ferdi-kamusal yarardır.*”⁷⁷⁰ Ancak önceki bölümlerde de ifade edildiği üzere bilişim suçları düzenlendikleri bölümden bağımsız değerlendirilmelidir. Zira bu suçlar “Topluma Karşı Suçlar” bölümünde düzenlense de aslında kişisel menfaatleri ihlal etmektedir.

Bilişim sistemleri aracılığıyla haksız yarar sağlama suçunun öngörülmesiyle bu sistemlere veya verilere müdahale edilmesi suretiyle insanların malvarlığı değerlerine yönelik haksız saldırıların engellenmesi amaçlanmaktadır.⁷⁷¹ Dolayısıyla bu suçun ihdas edilmesiyle korunması amaçlanan asıl değer malvarlığı değerleridir.⁷⁷² Suçun maddi unsuru ilk iki fıkradan yola çıkılarak kaleme alınsa da maddi unsura haksız yarar sağlama da eklendiğinden, dördüncü fıkranın hukuki konusu ilk iki fıkradan farklı hale gelmekte ve bu suçla aslında bilişim sistemleri aracılığıyla mal varlığı değerlerine yönelik saldırılar engellenmeye çalışılmaktadır.⁷⁷³

C. MADDİ KONU

“*Suçun maddi konusu suçun üzerinde işlendiği şey veya kişidir.*” Doktrinde bir görüş, suçun maddi konusunun bilişim sisteminin işleyişi ve veriler olduğunu ileri

⁷⁶⁸ Taşkın, s. 57; Ketizmen, s. 177; Karagülmez, s. 218.

⁷⁶⁹ Karagülmez, s. 217; Taşkın, s. 58.

⁷⁷⁰ Hafizoğulları/ Özen, s. 457.

⁷⁷¹ Erdoğan, s. 251.

⁷⁷² Koca/ Üzülmüş, s. 927; Parlar, s. 25; Özbek/ Doğan/ Bacaksız, s. 970.

⁷⁷³ Açıkgöz, s. 69.

sürmüştür.⁷⁷⁴ Ancak bu suç, bilişim sistemine veya verilere müdahale edilerek haksız çıkar sağlama suretiyle işlendiğinden, suçun maddi konusu haksız çıkardır.⁷⁷⁵ Doktrinde bazı yazarlar, bu çıkarın kişinin ekonomik durumunda artışa sebep olan bir menfaat olması gerektiğini; bu yönüyle failin ya da başkasının malvarlığının aktif değerlerinde artışa veya pasif değerlerinde azalmaya sebep olan her değerın suçun konusu olabileceğini savunmaktadırlar.⁷⁷⁶ Bu yarar “*kişinin işe alınması, terfi etmesi veya ihaleyi alması*” gibi hallerde de söz konusudur. Manevi olarak elde edilen, ekonomik olarak değeri ölçülemeyen menfaat veya yararlar bu suçun konusu olamaz. Kısacası yalnızca maddi çıkarların bu suçun maddi konusu olabileceğini savunmaktadırlar.⁷⁷⁷ Aksi görüşse burada kanun koyucunun maddi olup olmadığını belirtmeksizin haksız çıkar ifadesini kullanmasından yola çıkarak, failin kendisi için önemli gördüğü bir menfaati elde etmesi halini de (örneğin sistem üzerinden sınav sorularının çalınması, notların yükseltilmesi durumunda da haksız manevi bir yarar sağlandığından) bu suç kapsamında değerlendirmektedir.⁷⁷⁸

TCK 244/4. maddesi tali norm olarak öngörüldüğünden yani ancak fiil hırsızlık, dolandırıcılık, güveni kötüye kullanma gibi suçlara vücut vermediğinde uygulama alanı bulabilecek bir madde olduğundan ve bu maddelerde maddi haksız çıkar sağlama fiilleri tipik fiil olarak öngörüldüğünden, TCK 244/4’ün maddi konusu da maddi haksız çıkarlardır. Yani bu suç hırsızlık, dolandırıcılık, güveni kötüye kullanma gibi suçların oluşmaması durumunda haksızlık teşkil eden fiilin cezasız kalmaması için getirildiğinden, suçun maddi konusu da bu suçlarla aynı nitelikte yani maddi olmalıdır.⁷⁷⁹ Ayrıca haksız çıkarın manevi nitelikte olabileceğinin kabulü halinde dördüncü fıkranın

⁷⁷⁴ Yılmaz, s. 88.

⁷⁷⁵ Koca/ Üzülmmez, s. 927; Taşkın, s. 58; Açıkgöz, s. 75.

⁷⁷⁶ Koca, s. 98.

⁷⁷⁷ Koca/ Üzülmmez, s. 927; Açıkgöz, s. 90; Tezcan/ Erdem/ Önok, s. 1170-1171.

⁷⁷⁸ Kurt, s. 175; Yazıcıoğlu, s. 410; Yaşar/ Gökcan/ Artuç, s. 7316; Soyaslan, s. 709; Apaydın, s. 28; Erdoğan, s. 250; Taşkın, s. 58; Meran, s. 573; Parlar, s. 27.

⁷⁷⁹ Açıkgöz, s. 90.

uygulama alanı ilk iki fıkranın uygulama alanını daraltacak şekilde genişletilmiş olur zira her suçun işlenmesinde failin elde edebileceği manevi bir yarar vardır. Örneğin intikam amacıyla başkasının bilişim sisteminin işleyişinin engellenmesi halinde de failin manevi bir çıkarı söz konusudur ancak bu fiil dördüncü fıkra kapsamında değerlendirmemelidir.⁷⁸⁰ Ayrıca suçun yaptırımını olarak hem hapis cezasının hem de adli para cezasının öngörüldüğü suçlarda, amaç suçla elde edilen maddi çıkar için kazanç müsaderesinin uygulanamaması halinde bu çıkarın failden alınmasını sağlamak olduğundan, dördüncü fıkra da her iki türde yaptırım öngörülmesi elde edilen haksız çıkarın maddi nitelikte olması gerektiği şeklinde yorumlanabilir.⁷⁸¹ Kısacası bu suçun maddi konusu maddi nitelikteki haksız çıkarlardır.

Bilişim sistemleri kullanılarak elde edilen menfaatin haksız olması yani bu menfaatin elde edilmesine hukuken izin verilmemesi gerekir.⁷⁸² Hukuken tasvip edilen bir yararın elde edilmesi durumunda zaten maddi konu yokluğundan işlenemez suç söz konusudur.

Haksız çıkar, doğrudan failin kendisi yararına elde ettiği bir yarar olabileceği gibi üçüncü bir kimse yararına elde edilmiş bir çıkar da olabilir. Ancak yararın her ne kadar mağdurun rızası olmasa da mağdurun yararına elde edilmesi durumunda bu suç oluşmayacaktır zira suçun unsurlarından haksız çıkar sağlanmamıştır.⁷⁸³ Doktrindeki karşıt görüşe göreyse fail işlediği fiil sonucu çıkarı mağdur yararına elde etmiş olsa dahi kanunda “kendisi veya başkası” demek suretiyle başkası açısından bir sınırlama getirilmediğinden suç gerçekleşmiş sayılmalıdır.⁷⁸⁴ Biz ilk görüşe yani lehine haksız çıkar sağlanan başkasının, mağdur olamayacağı görüşüne iştirak etmekteyiz. Zira aksinin

⁷⁸⁰ Açıköz, s. 91.

⁷⁸¹ Akbulut, s. 234.

⁷⁸² Yaşar/ Gökcan/ Artuç, s. 7316.

⁷⁸³ Yaşar/ Gökcan/ Artuç, s. 7316.

⁷⁸⁴ Erdoğan, s. 254.

kabulünde mağdurun hem suçtan zarar gören hem de suçtan fayda sağlayan kişi olduğunun kabulü bizce mantıklı değildir.

Haksız çıkar doğrudan bir faydanın sağlanması örneğin para transfer edilmesi şeklinde veya dolaylı bir faydanın sağlanması örneğin ücretli bir hizmetten başkasının şifresini öğrenerek yararlanma ve bedeli 3. kişiye ödetme şeklinde olabilir.⁷⁸⁵

D. FAİL

TCK 37. maddesine göre “*suçun kanuni tanımında yer alan fiili gerçekleştiren*” kimse faildir. Cezai sorumluluğun şahsiliği ilkesi gereğince bir kimse ancak kendi fiillerinden sorumlu olacağından, organları aracılığıyla işlemlerde bulunabilen tüzel kişiler suçun faili olamayacaktır.

Bilişim sistemi aracılığıyla haksız yarar elde etme suçunun faili herkes olabilir.⁷⁸⁶ Bilişim sistemlerinin kullanılabilmesi için teknik bilgiyi gerektirmesi, suçu özgü suç haline getirmeyecektir. Bilgiye erişimin çok kolay hale geldiği günümüzde, toplumun her kesimi tarafından kullanılan bu sistemlere dair yeterli bilgisi olan herkes tarafından bu suç işlenebilecektir.

Fail “*sistemin işleyişini engelleyerek veya bozarak ya da verileri bozarak, yok ederek, değiştirerek, erişilmez kılarak, sisteme veri yerleştirerek, verileri başka yere göndererek*” haksız yarar sağlayan kimsedir.

E. MAĞDUR

Doktrinde bir görüşe göre mağdur haksız çıkar sağlanmak için müdahalede bulunulan bilişim sistemi veya veriler üzerinde hak sahibi kimsedir.⁷⁸⁷ Başka bir görüşe göreyse suçun mağduru “*bilişim sisteminin kullanılmasından doğrudan zarar gören*

⁷⁸⁵ Ketizmen, s. 146.

⁷⁸⁶ Taşkın, s. 58; Açıköz, s. 71.

⁷⁸⁷ Erdoğan, s. 253.

*kimse ve bilişim ortamının güvenliğini sağlamakla yükümlü kamu idaresidir”.*⁷⁸⁸ Ancak suçun mağduru ceza normuyla korunun hukuki değerin sahibi kimse olduğundan, TCK 244/1 ve 2. maddelerindeki seçimlik hareketlerin icra edilmesi suretiyle malvarlığında azalma yaşanan kişiler bu suçun mağdurudur.⁷⁸⁹ Zira suçla ihlal edilip ceza normuyla korunan değer mal varlığı değerleridir.

Doktrinde bir görüşe göre işleyişi bozulan veya engellenen sistem ya da müdahale edilen veri sahipleriyle malvarlığında azalma gerçekleşen kişilerin farklı kişiler olması durumunda, bilişim sistemi veya veri sahibi de bu suçun mağduru kabul edilmelidir.⁷⁹⁰ Ancak suçla ihlal edilen değerin doğrudan sahibi olmadıklarından bu kişiler mağdur değil; suçtan zarar gören olabilir.

Bir bankaya ait hesaplarda, müşterilerden birinin hesabında oynama yapılarak bir miktar meblağın failin kendi hesabına aktarılmasında her ne kadar hesap müşteriye ait ise de verilerin sahibi ve paranın zilyedi banka olduğundan bu durumda mağdurun banka olacağı kuşkusuzdur.⁷⁹¹

F. SUÇUN UNSURLARI

a. MADDİ UNSUR

Kanuni tanımında çok hareketli bir suç⁷⁹² olarak öngörülen TCK 244/4. maddesindeki suçu, TCK 244/1 ve 2. fıkrasındaki hareketlerin gerçekleştirilmesi suretiyle fail kendisi veya başkası lehine haksız çıkar sağlayarak işlemektedir.⁷⁹³ Burada fail haksız menfaat sağlamak için ilk iki fıkradaki hareketleri icra etmektedir.⁷⁹⁴

⁷⁸⁸ Hafızoğulları/ Özen, s. 457.

⁷⁸⁹ Açıkgöz, s. 76.

⁷⁹⁰ Koca/ Üzülmüş, s. 927; Açıkgöz, s. 77.

⁷⁹¹ Yazıcıoğlu, s. 232/233.

⁷⁹² Koca, s. 98.

⁷⁹³ Koca/ Üzülmüş, s. 928.

⁷⁹⁴ “1.5 milyar lira eksik tahakkuk ve tahsilata neden olduğu, bu durumun, sanık tarafından bilgisayar kayıtlarında sayaç çarpanları değiştirilerek eksik fatura düzenlenmesinden kaynaklandığının belirtildiği”

Doktrinde bir görüşe göre bu suç seçimlik hareketli bir suçtur. Bu görüşe göre suç, birinci veya ikinci fıkrada yazılı seçimlik hareketlerin gerçekleştirilmesi suretiyle haksız çıkar elde edilerek işlenebileceğinden “*bilişim sistemleri aracılığıyla haksız çıkar sağlama suçu*” seçimlik hareketli bir suç olarak öngörülmüştür.⁷⁹⁵ Doktrinde başka bir görüşe göreyse suçun kanuni tanımında ilk iki fıkra atf yapıldığından ve bu fıkralarda da harekete değil neticeye yer verildiğinden bu suç serbest hareketli bir suçtur. suç ilk iki fıkrada yer verilen neticeleri gerçekleştirmeye elverişli her türlü fiil işlenerek haksız çıkar elde edilmesi suretiyle işlenebilir.⁷⁹⁶ Ancak daha önce de ifade ettiğimiz üzere maddede sayılı hareketler netice değildir. Bu hareketlerin neticesi, bilişim sisteminin işlevsiz hale gelmesi veya verilerin kullanılamaz hale gelmesi olduğundan, hareketler netice olarak değerlendirilemez.

Bilişim sistemi aracılığıyla haksız yarar elde etme suçunun hangi hareketlerle işleneceği maddede öngörüldüğünden, bu suç bağlı hareketli bir suçtur.⁷⁹⁷ Maddede sayılan hareketlerden bir veya birkaçının yapılarak, haksız menfaatin failin veya başkasının tasarruf alanına sokulmasıyla veya haksız çıkar üzerinde tasarrufta bulunma imkanına kavuşmalarıyla suç tamamlanır.⁷⁹⁸ Suçun maddi konusu aynı olmak koşuluyla TCK 244/1 veya 2. fıkralarındaki seçimlik hareketlerden birden fazlasının gerçekleştirilmesi suretiyle haksız çıkar elde edilmesi durumunda tek suç vardır.⁷⁹⁹

Bilişim sistemleri aracılığıyla haksız yarar sağlama suçu neticeli bir suçtur.⁸⁰⁰ TCK 244. maddesinin ilk iki fıkrasında sayılan seçimlik hareketler sonucu fail kendisi veya başkası lehine haksız çıkar elde etmiş olmalıdır. Başka bir ifadeyle gerçekleştirilen

Yargıtay’ın ETCK 525/b maddesinden hüküm kurduğu kararda TCK 244/4. maddesi gerçekleşmektedir. Yargıtay 4. CD. E. 2000/1068 K. 2000/1771 T. 28.2.2000: Kurt, s. 169.

⁷⁹⁵ Apaydın, s. 29.

⁷⁹⁶ Erdoğan, s. 252-253.

⁷⁹⁷ Koca/ Üzülmüş, s. 928; Açıkgöz, s. 78.

⁷⁹⁸ Koca/ Üzülmüş, s. 928.

⁷⁹⁹ Açıkgöz, s. 79.

⁸⁰⁰ Yılmaz, s. 88.

seçimlik hareketler ve elde edilen haksız çıkar arasında nedensellik bağı olmalı ki failin sorumluluğu gündeme gelsin.⁸⁰¹

Bilişim sistemleri aracılığıyla haksız yarar sağlama suçu, haksız çıkarın failin veya başkasının tasarruf alanına geçmesiyle veya haksız çıkar üzerinde failin veya başkasının tasarrufta bulunma imkanını elde etmesiyle tamamlanır⁸⁰² Kısacası haksız yararın elde edilmesiyle suç tamamlanacaktır.⁸⁰³

Failin kendisi veya başkası yararına haksız çıkar sağlama yeterli olup, mağdurun mutlaka zarara uğratılması gerekmemektedir.⁸⁰⁴ Doktrinde bir görüş burada haksız çıkar sağlanması sonucu bir zararın doğmaması ihtimalini mümkün görmediğinden⁸⁰⁵ suçun tehlike suçu değil; zarar suçu olduğunu savunmaktadır.⁸⁰⁶ Karşıt görüşe göreyse haksız bir çıkarın elde edilmesiyle herhangi bir zararın doğması maddede aranmadığından başka bir ifadeyle suçun kanuni tanımında tipik fiilin gerçekleştirilmesi için ayrıca mağdurun bir zarara uğratılması aranmadığından bu suç tehlike suçudur.⁸⁰⁷ Ancak mağdurun zarara uğratılmasının zorunlu olmaması bu suçun zarar suçu olarak değerlendirilmesine engel değildir yani bu suç bir zarar suçudur.⁸⁰⁸

Suç üçüncü fıkra da sayılan kurum ve kuruluşların bilişim sistemlerine veya verilerine müdahale edilerek işlendiğinde de dördüncü fıkra uygulanacaktır.⁸⁰⁹ Ancak burada üçüncü fıkra dördüncü fıkranın nitelikli hali değildir. Nitekim üçüncü fıkra ilk iki fıkradaki suçların nitelikli hali olarak öngörülmüştür. Dolayısıyla “*bilişim sistemleri aracılığıyla haksız çıkar sağlama suçu*” banka veya kredi kurumuna ya da kamu kurumu

⁸⁰¹ Açıkgöz, s. 89.

⁸⁰² Açıkgöz, s. 94.

⁸⁰³ Açıkgöz, s. 74.

⁸⁰⁴ Yaşar/ Gökcan/ Artuç, s. 7317; Soyaslan, s. 709.

⁸⁰⁵ Yazara göre suçun oluşması için zararın varlığı şarttır. Erdoğan, s. 254.

⁸⁰⁶ Taşkın, s. 58; Yılmaz, s. 87.

⁸⁰⁷ Apaydın, s. 30.

⁸⁰⁸ Koca/ Üzülmüş, s. 928; Açıkgöz, s. 75.

⁸⁰⁹ Hafizoğulları/ Özen, s. 458; Kurt, s. 244.

veya kamu kuruluşuna karşı işlendiğinde üçüncü fıkra gereği artırım yapılmaksızın sadece dördüncü fıkradaki cezadan hüküm kurulacaktır.⁸¹⁰

b. MANEVİ UNSUR

TCK 244/4. maddesindeki suç ancak kasten işlenebilir.⁸¹¹ Fail birinci ve ikinci fıkradaki fiilleri işlemek suretiyle kendisi veya başkası lehine haksız çıkar sağladığını bilerek ve isteyerek hareket etmelidir. Sağlanan yararın haksızlığı kast kapsamında olduğundan fail elde ettiği yararın haksız olduğunu bilmelidir.⁸¹²

Doktrinde bir görüş burada “*kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlaması*” ifadesi dolayısıyla özel kastın arandığını savunmaktadır.⁸¹³ Ancak bahse konu ifade suçun maddi unsurunu yani fiili oluşturmakta olup, failin özel bir saikle hareket etmesi aranmamıştır. Kısacası bu suç genel kastla işlenebilen bir suçtur.⁸¹⁴

Failin kendisi veya başkası için sağladığı yararın haksız olduğunu bilmesi gerektiğinden bu suç ancak doğrudan kastla işlenebilir.⁸¹⁵ Buradaki haksızlık bilinci, maddi unsura ilişkin bir bilgi olduğundan kast içerisinde değerlendirilmelidir.⁸¹⁶ Çıkarın haksız olduğu bilgisi kast içerisinde değerlendirildiğinden bu suç olası kastla işlenemez.⁸¹⁷

“*Bilişim sistemleri aracılığıyla haksız çıkar sağlama*” suçunun kanunda açıkça taksirle işlenebileceği öngörülmediğinden, bu suç taksirle işlenemez. Yani dikkat ve özen yükümlülüğüne aykırı bir biçimde TCK 244. maddesinin ilk iki fıkrasındaki hareketleri

⁸¹⁰ Açıkgöz, s. 104-105.

⁸¹¹ Yaşar/ Gökcan/ Artuç, s. 7318.

⁸¹² Koca/ Üzülmüş, s. 929.

⁸¹³ Parlar, s. 27; Taşkın, s. 59; Karagülmez, s. 214; Yılmaz, s. 89.

⁸¹⁴ Soyaslan, s. 710; Açıkgöz, s. 99; Erdoğan, s. 257.

⁸¹⁵ Koca/ Üzülmüş, s. 929; Suçun olası kastla işlenebileceği görüşünü savunan yazarlar için bkz. Yaşar/ Gökcan/ Artuç, s. 7318.

⁸¹⁶ Koca, s. 98.

⁸¹⁷ Açıkgöz, s. 100; Aksi görüşse suçun olası kastla da işlenebileceğini ileri sürmektedir: Apaydın, s. 31.

gerçekleştirmek suretiyle kendisi veya başkası lehine haksız yarar sağlayan kimse cezalandırılmayacaktır.

c. HUKUKA AYKIRILIK

Kanun hükmü ve amirin emrinin icrası (TCK 24), ilgilinin rızası (TCK 26/2)⁸¹⁸ ve hakkın kullanılması (TCK 26/1)⁸¹⁹ bu suçla bağdaşan hukuka uygunluk nedenleridir.

İlgilinin rızası hukuka uygunluk sebebinde, rıza vermeye yetkili kimsenin bu rızayı göstermesi gerektiğinden, her zaman bu rıza sistem veya veri sahibinden alınmak zorunda değildir. Doktrinde bir görüşe göre burada rızayı sistem üzerinde hak sahibi kimse/ sistemin ilgilisi göstermelidir.⁸²⁰ Ancak rızayı gösterecek kimse suçla zarara veya tehlikeye uğratılan değer veya hakkın sahibi olduğundan, rızayı göstermesi gereken kimse bu suç bakımından haksız elde edilen menfaatin esas sahibi yani suçun mağduru kimsedir. Ancak her zaman sistem veya veri sahibiyle maddi çıkarın gerçek sahibi kimse aynı kişiler olmayabileceğinden, rıza göstermesi gereken kimse her somut olaya göre ayrı ayrı değerlendirilmelidir. Zira maddi çıkarın gerçek sahibinin sistem veya veri sahibinden farklı kimse olması durumunda sistem veya veri malikinin rızası fiili hukuka uygun hale getirmeyecektir.⁸²¹ Dolayısıyla her somut olay özelinde ayrı değerlendirme yapılarak geçerli bir rızanın bulunup bulunmadığı hususunda karar verilmelidir.

G. SUÇUN ÖZEL GÖRÜNÜŞ ŞEKİLLERİ

a. TEŞEBBÜS

Neticeli bir suç olan bilişim sistemleri aracılığıyla haksız yarar elde etme suçuna teşebbüs mümkündür. Doktrinde bir görüşe göre, tipik hareketler sonucu haksız bir çıkar sağlanmamışsa teşebbüsten söz edilemez ancak fiil, TCK 244/1 ve 2. maddeleri veya

⁸¹⁸ Koca/ Üzülmüş, s. 929; Parlar/ Hatipoğlu, s. 3479.

⁸¹⁹ Açıkgöz, s. 102.

⁸²⁰ Taşkın, s. 59.

⁸²¹ Açıkgöz, s. 103.

TCK 243. maddesindeki tipik fiille örtüşüyorsa artık bu maddelerden sorumluluk doğacaktır.⁸²² Ancak bu görüşe katılmak mümkün değildir. Suç haksız yararın elde edilmesiyle tamamlandığından fail maddede sayılan hareketleri icra etmesine rağmen elinde olmayan nedenlerle netice gerçekleşmemiş veya suçun icrasına elverişli hareketlerle başlamasına rağmen fiilin icrası bitmemişse teşebbüsten sorumluluk doğacaktır.⁸²³

Doktrinde bir görüşe göre haksız çıkarın elde edilmesi ifadesinden anlaşılması gereken menfaatin fiziken elde edilmesi olmayıp; failin zilyetinde olmasıdır. Dolayısıyla suçun tamamlanması için haksız çıkarın fiziken ele geçirilmesi aranmayacaktır.⁸²⁴ Ancak burada zilyetlik de aranmamalıdır. Bilişim sistemleri aracılığıyla haksız yarar sağlama suçu, haksız çıkarın failin veya başkasının tasarruf alanına geçmesiyle veya haksız çıkar üzerinde failin veya başkasının tasarrufta bulunma imkanını elde etmesiyle tamamlanır⁸²⁵

“*Bilişim sistemi aracılığıyla haksız yarar sağlama suçunun*”, TCK 244/1. ve 2. fıkralarında belirtilen hareketlerle işleniyor olması sebebiyle hangi suçun oluştuğunun veya hangi suça teşebbüs olduğunu tespit için failin kastının belirlenmesi önem teşkil etmektedir.⁸²⁶ Şayet fail haksız çıkar sağlamak kastıyla hareket etmiş ancak bu çıkarı elde edememişse TCK 244/4. maddesine teşebbüsten sorumlu olacaktır. Ancak failin kastı sadece sisteme veya verilere müdahale etmeye yönelikken ayrıca haksız bir çıkar elde edilmişse, tamamlanmış TCK 244/1 veya 2. maddesinden sorumlu tutulmalıdır.⁸²⁷

TCK 244/4. maddesini gerçekleştirmek için suçun icra hareketlerine başlayan failin, “*suçun icra hareketlerinden gönüllü vazgeçmesi veya kendi çabasıyla suçun*

⁸²² Özbek/ Doğan/ Bacaksız, s. 983

⁸²³ Yaşar/ Gökcan/ Artuç, s. 7316.

⁸²⁴ Yargıtay da aynı görüşü paylaşmaktadır. (11. CD 12.05.2009/ 3700-6207.) Ancak yazarlar ne kadar zilyetliğin yeterli olduğunu savunsa da örnek gösterilen Yargıtay kararında zilyet fail değil bankadır. Dolayısıyla zilyetlik yerine tasarruf imkanını elde etmenin yeterli görülmesi daha isabetli bir tercih olacaktır. Yaşar/ Gökcan/ Artuç, s. 7316.

⁸²⁵ Açıkgöz, s. 94.

⁸²⁶ Yaşar/ Gökcan/ Artuç, s. 7320; Açıkgöz, s. 110.

⁸²⁷ Koca/ Üzülmüş, s. 929; Açıkgöz, s. 110.

tamamlanmasını ya da neticenin gerçekleşmesini önlemesi” halinde TCK 36. maddesinin (gönüllü vazgeçme) uygulanması mümkündür. Bu durumda fail TCK 244/4. maddesine teşebbüsten sorumlu olmayacak ancak fiilin tamamlanan kısmı TCK 244/1 veya 2. maddesinde düzenlenen suçları oluşturuyorsa bundan sorumlu olacaktır.⁸²⁸

b. İŞTİRAK

Suç iştirak bakımından özellik arz etmediğinden iştirake ilişkin genel kurallar uygulama alanı bulacaktır. Bilişim sistemleri aracılığıyla haksız yarar sağlama suçunda iştirakin her türlü şekli mümkündür.⁸²⁹

Dolaylı fail olarak bu suçun işlenmesi mümkündür. Dolaylı fail cebir veya tehditle suçu işletmişse TCK 28 ve TCK 37/2. maddeleri uyarınca TCK 244/4. maddesinden dolaylı fail sıfatıyla sorumlu olacaktır.⁸³⁰ Bilişim sistemi aracılığıyla haksız yarar sağlama fiilinin sistem veya verileri kontrolle görevli kimsenin aldatılması aracılığıyla işlenmesi durumunda dolaylı fail olarak sorumluluğun hangi maddeden doğacağı doktrinde tartışmalıdır. Burada yetkili kimse aldatıldığından, sisteme veya verilere müdahale söz konusu olmadığından dolaylı failin sorumluluğu TCK 157. maddesinden doğacaktır.⁸³¹

TCK 245/A maddesinde bilişim alanındaki suçların işlenmesi için yardım niteliği taşıyabilecek fiillerin suç olarak öngörülmesi söz konusudur. TCK 245/A maddesinin uygulama alanı “*Bilişim Alanında Suçlar*” bölümündeki suçlar ve bilişim sistemlerinin araç olarak kullanıldığı suçlarla sınırlı tutulmuştur. Bir kimsenin TCK 244/4. maddesindeki suçu işlemesi için TCK 245/A maddesinde sayılan suçu işleyen kimse, iştirak iradesiyle hareket etmemişse sadece TCK 245/A maddesinden sorumlu olacaktır. Eğer bu kişi “*bilişim sistemi aracılığıyla haksız yarar sağlama suçu*” bakımından sadece

⁸²⁸ Açıkgöz, s. 111.

⁸²⁹ Açıkgöz, s. 111.

⁸³⁰ Açıkgöz, s. 113.

⁸³¹ Hileli hareketler bilişim sistemleri kullanılarak icra edilmişse nitelikli halden; bilişim sistemi kullanılmadan kandırma söz konusuysa suçun temel halinden hüküm kurulacaktır. Açıkgöz; s. 73.

iştirak iradesiyle hareket etmiş ve örneğin suçun işlenmesi için yardım eden sıfatıyla sisteme girme suçunu işleyecek faile bunun için bir program satmışsa, TCK 244. maddesi bakımından yardım eden, TCK 245/A maddesi bakımından fail konumundadır. Failliğin şerikliğe nazaran asliliği kuralı gereğince bu kimse sadece TCK 245/A maddesinden sorumlu olacaktır. Fakat TCK 245/A maddesinde sayılan seçimlik hareketler “*bilişim sistemi aracılığıyla haksız yarar sağlama suçu*” açısından zorunluysa başka bir ifadeyle bu hareketi gerçekleştiren TCK 244/4 maddesi bakımından müşterek fail haline gelmişse, fail hem TCK 245/A maddesi hem de TCK 244/4 maddesini ihlal etmiştir. Bu durumunda doktrinde bir görüşe göre fikri içtima kuralı gereğince daha ağır cezanın öngörüldüğü TCK 244/4. maddesinden hüküm kurulmalıdır. Yazara göre TCK 244/4. maddesinin tali norm olarak öngörülmesi bu suçla haksız çıkar elde etmeye yönelik olmayan suçlar arasında fikri içtima kuralının uygulanmasına engel değildir.⁸³² Ancak bağımsız olarak cezalandırılan hazırlık hareketi niteliğindeki fiiller TCK 244/4. maddesinde düzenlenen suç için tipik değildir. TCK 244/4 ve 245/A maddelerinde tipik hareketler farklı olduğundan, iki madde arasında fikri içtima ilişkisi söz konusu değildir. Dolayısıyla TCK 244/4. maddesinin işlenmesi için araç temin eden kimse, fiil üzerinde ortak hakimiyet kurmuşsa hem TCK 244/4. maddesinden hem de TCK 245/A maddesinden sorumlu olacaktır.

Başkası için haksız çıkar elde edildiği durumlarda, lehine çıkar sağlanan kimse bu durumu biliyor ve hatta suçu işlemesi için faili azmettirmişse şerik olarak sorumlu olacaktır. Ancak bu kişi elde edilen çıkarın haksız olduğunu bilmiyorsa, çıkarın haksız olduğu bilgisi kast içerisinde değerlendirildiğinden, TCK 30/1. maddesi gereği şerik olarak sorumluluğu doğmayacaktır.⁸³³

⁸³² Açığöz, s. 113.

⁸³³ Açığöz, s. 113.

c. İÇTİMA

1. Genel olarak

Bilişim sistemi aracılığıyla haksız yarar sağlama suçunun öngörülme sebebi; eşya olarak kabul edilmeyen ekonomik değeri haiz verilere yönelik haksız menfaat elde etmek amacıyla gerçekleştirilen fiillerin, mal varlığını korumak için öngörülmüş diğer suçlar bakımından kanuni tipe uygun olmaması dolayısıyla bu değerlere yönelik fiillerin yaptırımsız kalmasını önlemektir.⁸³⁴

Doktrinde bir görüşe göre, TCK 243. maddesi bu suç bakımından geçit suç niteliği taşıdığından faile sadece TCK 244/4. maddesinden ceza verilecektir.⁸³⁵ Ancak önceki bölümlerde de açıklandığı üzere TCK 243. maddesi, TCK 244. maddesindeki suçlar için geçilmesi zorunlu bir suç değildir. Dolayısıyla bir bilişim sistemine girilmesi suretiyle TCK 244/4. maddesi ihlal ediliyorsa; gerçek içtima kuralı gereğince fail hakkında hem TCK 243 hem de TCK 244/4. maddelerinden hüküm kurulacaktır. Doktrinde bir başka görüşe TCK 244/4. maddesinin işlenmesi bakımında bilişim sistemine girme suçunun işlenmesinin zorunluluk arz etmesi sebebiyle tek fiille hem TCK 243'ün hem de TCK 244/4'ün gerçekleştiğini dolayısıyla fikri içtima kurallarının uygulanması gerektiğini ve failin yalnızca TCK 244/4'ten cezalandırılması gerektiğini savunmaktadır.⁸³⁶ Ancak bilişim sistemine girme TCK 244/4. maddesinin işlenebilmesi için zorunluluk arz etmediğinden, bilişim sistemine girilerek TCK 244/4. maddesinin gerçekleştirildiği örneklerde fikri içtima değil; gerçek içtima kuralı uygulanmalıdır.

“Bilişim sistemi aracılığıyla haksız çıkar sağlama suçu” ile TCK 158/1-f, TCK 142/2-e, TCK 163, TCK 245 ve 5411 S. Bankacılık Kanunu 160. maddesi arasında asli-

⁸³⁴ Açıkgöz, s. 117.

⁸³⁵ Parlar, s. 28; Soyaslan, s. 710.

⁸³⁶ Koca/ Üzülmüş, s. 930.

tali norm ilişkisi vardır.⁸³⁷ Asli norm- tali norm ilişkisi görünüşte içtima ilişkisi arz ettiğinden⁸³⁸, fikri içtima ilişkisi uygulanmayacaktır. Yani fiil hem TCK 244/4 hem de yukarıda sayılan suçlar bakımından tipiklik arz ediyorsa, TCK 244/4. maddesinin tali norm olması dolayısıyla gerçekleşen diğer suçtan hüküm kurulacaktır.

Öncelikle TCK 244/4 ve TCK 142/2-e maddesinde düzenlenen bilişim sistemleri aracılığıyla hırsızlık suçu arasındaki ilişki incelendiğinde, hırsızlık suçunun kanuni tanımında tipik fiil “*zilyedinin rızası olmadan başkasına ait taşınır bir malı, kendisine veya başkasına bir yarar sağlamak maksadıyla bulunduğu yerden alma*” şeklinde tanımlanmıştır.⁸³⁹ Buna göre hırsızlık suçunun maddi konusu taşınır bir malken; verilerin kanunda taşınır bir mal olarak tanımlanmaması dolayısıyla “*suçta ve cezada kanunilik ilkesi*” ve “*kıyas yasağı*” gereğince veriler TCK 142/2-e maddesinin konusu olamayacaktır.⁸⁴⁰ Bilişim sistemlerine veya verilere müdahale edilerek haksız yarar elde edilmesi durumunda, ekonomik değeri olan veriler taşınır mal olmadığından TCK 244/4. fıkrası uygulama alanı bulacaktır.⁸⁴¹

Doktrindeki karşıt görüşe göreyse TCK 142/2-e maddesiyle getirilen bu nitelikli hal ile bilişim sistemlerinin kullanılması suretiyle verilerin değil; taşınabilir şeylerin çalınması kastedildiğinden, bilişim sistemi kullanılarak bir kimsenin banka hesabından kendisine veya başka bir kimseye ait banka hesabına para aktarılması TCK142/2-e maddesine vücut verecektir.⁸⁴² Yani TCK 244. maddesinde sayılan sisteme veya verilere

⁸³⁷ Açıkgöz, s. 118-139.

⁸³⁸ İçel, İçtima, s. 209.

⁸³⁹ Hırsızlık suçunun oluşması için taşınabilir bir malın fiziken bulunduğu yerden alınması gerektiğinden bu suçun bilişim sistemleri aracılığıyla nasıl işlenebileceği muğlaktır. Kanun gerekçesinde de buna dair bir açıklama getirilmemiştir. Doktrinde bazı yazarlar bilişim sistemleri aracılığıyla hırsızlık suçunun bir iki örnek dışında mümkün olmadığı yönündedir. Yazıcıoğlu, s. 398.

⁸⁴⁰ Yazıcıoğlu, s. 398.

⁸⁴¹ Özbek, Veli Özer, Banka ve Kredi Kartlarının Kötüye Kullanılması Suçu, s. Örneğin gerçek hayatta ekonomik değere sahip bir bilgisayar oyunundaki “item”in ele geçirilmesi durumunda Yargıtay 13. CD TCK 244/4’ten hüküm kurulması gerektiğine karar vermiştir. 13. CD E. 2015/2174, K. 2016/10469. Açıkgöz, s. 96-97.

⁸⁴² Parlar, s. 106; Taşkın, s. 347-348.

müdahale niteliğindeki hareketlerin icra edilmesi suretiyle taşınır bir malın bulunduğu yerden alınarak haksız bir yarar sağlanması halinde TCK 142/2-e maddesinde düzenlenen hırsızlık suçunun nitelikli hali gerçekleşmiş olacaktır.⁸⁴³ Bu sebeple malvarlığı değeri teşkil etmeyen verilerin çalınması değil; taşınır malların bulunduğu yerden alınması bu suçu oluşturacaktır. Verilerin çalınması suretiyle haksız yarar elde edilmesi durumunda fiil başka bir suç teşkil etmiyorsa TCK 244/4. maddesinden hüküm kurulacaktır.⁸⁴⁴

Yine bu görüşe sahip bazı yazarlar ancak ekonomik değere sahip verilerin hırsızlık suçuna konu olabileceğini kabul etmektedir.⁸⁴⁵ Bu görüşe göre bilişim sistemlerinin kullanılması suretiyle ekonomik bir değeri olan verilerin transferi ancak ekonomik değeri olan verilerin dış dünyada maddi varlığı bulunan taşınır bir malı temsil etmesi durumunda TCK 142/2-e maddesine sebep olabilecektir. Başka bir ifadeyle dış dünyada maddi bir varlığı olan taşınır mallara fiziki herhangi müdahale olmadan, bu malları temsil eden verilere müdahale edilmesi suretiyle ekonomik değer tasarruf alanına sokulması suretiyle TCK 142/2-e maddesi işlenmektedir. Dolayısıyla örneğin internet bankacılığı işlemleriyle başkasının hesabından kendi hesabına haksız transfer yapan fail, TCK 142/2-e maddesinde düzenlenen bilişim sistemleri aracılığıyla hırsızlık suçunu işlemiştir.⁸⁴⁶ Ancak dış dünyada maddi bir varlığı temsil etmeyen ancak ekonomik değeri olan verilere müdahale TCK 142/2-e maddesinin uygulama alanına girmemektedir. Örneğin internet üzerinden haksız bir şekilde bir telefonda diğerine kontör gönderilmesi TCK 142/2-e kapsamına değil; TCK 244/4. maddesi kapsamına girmektedir.⁸⁴⁷

Başkasının internet bankacılığı kullanılarak kendisi veya bir başkasının hesabına para transferi yapılması durumunda hangi suçun oluştuğu konusunda Yargıtay 6. ve 11.

⁸⁴³ Ketizmen, s. 181.

⁸⁴⁴ Parlar, s. 109.

⁸⁴⁵ Karagülmez, s. 195.

⁸⁴⁶ Koca/ Üzülmüş, s. 923.

⁸⁴⁷ Yargıtay 13. CD. K.T. 30.01.2013, E. 2011/26435 K. 2013/1955 kararı da bu yöndedir. Koca/ Üzülmüş, s. 925.

CD arasında görüş ayrılığı vardı. Yargıtay 6. CD TCK 142/2-e'den hüküm kurarken; 11. CD TCK 244/4'den hüküm kurmaktaydı.⁸⁴⁸ Bu olayların Yargıtay Ceza Genel Kuruluna taşınması ardından Genel Kurul'un 27.04.2009 tarihli (E. 2009/11-193, K. 2009/268) kararıyla transfere konu olan şeyin veri değil, verilerin temsil ettiği taşınır mal niteliğindeki para olduğu gerekçesiyle olayın TCK 142/2-e maddesi çerçevesinde değerlendirilmesine hükmedilmiştir. Bu durum doktrini de ikiye bölmüş bir görüş⁸⁴⁹ Yargıtay Ceza Genel Kurulu gibi internet bankacılığı kullanılarak para transferi yapılması durumunda, transfere konu olan veri değil, verilerin temsil ettiği taşınır mal niteliğindeki para olduğu düşüncesinden hareketle bilişim sistemleri kullanılması aracılığıyla hırsızlık suçu oluştuğunu savunmaktadır.⁸⁵⁰ Karşıt görüşlerden biri transfere konu taşınır mal niteliğinde olmayan veri olduğundan, verilerin değiştirilmesi suretiyle haksız çıkar elde edilmesi dolayısıyla⁸⁵¹ bir başka görüşse verilerin başka yere gönderilmesi suretiyle haksız çıkar elde edilmesi dolayısıyla fiili TCK 244/4 çerçevesinde değerlendirmektedir.⁸⁵²

Öncelikle belirtmek gerekir ki YCGK kararı sonrası verilerin taşınır mal olarak kabul edilmesi TCK 244/4. maddesinin⁸⁵³ uygulama alanını çok daraltmıştır.⁸⁵⁴ Ceza hukukunda geçerli olan biçimsel kanunilik ilkesi uyarınca suç teşkil eden fiillerin kanunda açıkça öngörülmesi gerekir. Hırsızlık suçunun kanuni tanımında açıkça taşınır mal ifadesi kullanıldıktan sonra verilere müdahale niteliğindeki hareketleri hırsızlık suçu

⁸⁴⁸ Koca/ Üzülmüş, s. 924.

⁸⁴⁹ Mahmutoglu; yazara göre kamu davasına konu olayda TCK 244. maddesinin birinci veya ikinci fıkrasındaki seçimlik hareketlerden biri gerçekleştirilmediğinden olay TCK 244/4 kapsamında değerlendirilemez. S. 881

⁸⁵⁰ Koca/ Üzülmüş, s. 923.

⁸⁵¹ Paranın üçüncü bir kişinin veya failin hesabına geçmesiyle suç tamamlanmaktadır. Zira TCK244/4. maddesinde maddi çıkar üzerinde tasarruf imkanını elde etmeyle suç tamamlanacağından paranın hesaptan çekilmesi aranmaz. Açıkgoz, s. 128-129.

⁸⁵² Özbek/Doğan/Bacaksız, s. 983; Özen/ Baştürk, s. 139.

⁸⁵³ Bilişim sistemi kullanılarak banka hesapları arası para transferi yapmak TCK 142/2-e maddesini oluştururken; bir hesaptaki verinin azaltılarak diğerinin artırılması halinde (örneğin bir hesaptaki belli miktar paranın 0 tl'ye düşürülüp, başka bir hesaptaki para miktarının o miktarda artırılması) TCK 244/4. maddesi oluşmaktadır. YARGITAY 11. CD E. 2002/5711 K. 2002/8416. Kurt, s. 169.

⁸⁵⁴ Yılmaz, s. 94-95.

kapsamında değerlendirmek, TCK 2/3. maddesinde düzenlenen “kıyasa yol açacak biçimde genişletici yorum yapma” yasağına aykırıdır. Zira veriler klasik anlamda taşınır malların sahip olduğu hiçbir özelliğe sahip değilken kanunda da böyle bir kabule yer verilmemiştir. Bu sebeplerle kanunda açıkça verilerin taşınır mal sayılacağına dair bir hüküm olmadıkça verilere müdahale niteliğindeki hareketlerin TCK 142/2-e maddesinde düzenlenen hırsızlık suçuna vücut vermeyeceği görüşüne iştirak ediyoruz.

Doktrinde bir görüşe göre haksız çıkarın elde edildiği zamanın tespiti suçun tespiti açısından önemlidir. Taşınır malın elde edilmesiyle haksız çıkar sağlanıyorsa hırsızlık; taşınır malın bulunduğu yerden alınmasından önce haksız çıkar sağlanıyorsa TCK 244/4 gerçekleşmiştir.⁸⁵⁵

Doktrinde bir görüşe göre ATM'lere banka kartı kullanmaksızın, fiziksel etkide bulunarak ATM'den para çekilmesi durumunda “*bilişim sistemi aracılığıyla hırsızlık suçu*” oluşacaktır.⁸⁵⁶ Ancak TCK 142/2-e maddesinde bilişim sistemine karşı hırsızlık değil; bilişim sisteminin kullanılması suretiyle hırsızlık suçu nitelikli hal olarak öngörülmüştür. Dolayısıyla bilişim sistemlerine fiziksel müdahale yoluyla TCK 244/1. maddesi gerçekleştirilebileceğinden burada hırsızlık suçundan ziyade TCK 244/4 oluşacaktır.

Sanal paranın bilişim sistemine veya verilere müdahale edilmek suretiyle haksız bir şekilde elde edilmesi durumunda maddi bir çıkar elde edildiğinden sorumluluk TCK 244/4. maddesi çerçevesinde doğacaktır.⁸⁵⁷

TCK 244/4. maddesiyle nitelikli dolandırıcılık hallerinden biri olan TCK 158/1-f maddesi arasındaki ilişkisinin de incelenmesi önem arz etmektedir. “*Bilişim sistemleri aracılığıyla haksız yarar sağlama suçu*”, “*bilişim sistemlerinin araç olarak kullanılması*

⁸⁵⁵ Ketizmen, s. 181-182

⁸⁵⁶ Koca/ Üzülmüş, s. 923; Ketizmen, s. 181.

⁸⁵⁷ Açıkgöz, s. 96.

suretiyle dolandırıcılık suçuna” göre tali normdur. Dolandırıcılık suçunun bilişim sistemleri kullanılarak gerçekleştirilebilmesi için dolandırıcılık suçunun unsurlarının gerçekleşmesi gerekir. Buna göre failin bilişim sistemlerini kullanmak suretiyle “*hileli davranışlarla bir kimseyi aldatıp, onun veya başkasının zararına olarak, kendisine veya başkasına bir yarar sağlaması*” halinde TCK 158/1-f maddesinden sorumluluğu doğacaktır.

Bilişim sistemine karşı hileli hareketlerde bulunularak sistemin aldatılması suretiyle haksız çıkar sağlanması hali TCK 244/4. maddesi kapsamında⁸⁵⁸; kişilere karşı hileli hareketlerle haksız çıkar sağlanması haliyse TCK 158/1-f maddesi kapsamında değerlendirilmelidir. Yani TCK 244/4. maddesinin uygulanabilmesi için kişilere karşı hileli herhangi bir hareket gerçekleştirilmemelidir.⁸⁵⁹ TCK 158/1-f maddesinin gerçekleşmesi için hileli davranışlarla aldatmanın sadece ve mutlaka bilişim sistemi araçlarıyla yapılmalıdır.⁸⁶⁰

Yargıtay da bilişim sistemleri kullanılması suretiyle işlenen dolandırıcılık suçuyla TCK 244/4. maddesindeki suç hileli davranışın bir insana karşı yapılıp yapılmadığına göre ayırmaktadır. Buna göre hileli davranışlar bir bilişim sistemi kullanılarak gerçek bir kimseye karşı icra ediliyor ve bu fiil nedeniyle fail haksız bir kazanç elde ediyorsa nitelikli dolandırıcılık suçu; hileli hareket etmeksizin TCK 244/1 ve 2. fıkralarında sayılan hareketler aracılığıyla bilişim sistemi kullanılarak haksız yarar sağlanıyorsa TCK 244/4. maddesindeki suç oluşmaktadır.⁸⁶¹

Doktrinde bir görüş dolandırıcılık suçunda hileli hareketlerle aldatılması gereken kimsenin insan olması sebebiyle bilişim sistemlerinin aldatılması durumunda dolandırıcılık suçu bakımından tipikliğin gerçekleşmemesi dolayısıyla bilişim sistemleri

⁸⁵⁸ Kurt, s. 171.

⁸⁵⁹ Yaşar/ Gökcan/ Artuç, s. 7316.

⁸⁶⁰ Korkmaz, s. 1428.

⁸⁶¹ Koca/ Üzülmaz, s. 926.

aracılığıyla dolandırıcılık suçunun işlenemeyeceğini ileri sürmüştür.⁸⁶² Ancak bilişim sistemleri aracılığıyla insanların da hileli hareketlerle kandırılması mümkün olduğundan TCK 158/1-f maddesi gerçekleştirilebilecek bir suçtur.⁸⁶³ Hileli hareketlerle failin kandırılmasında bilişim sistemlerinin araç olarak kullanılması ve fail ile kandırılan kimsenin yüz yüze gelmemiş, herhangi bir şekilde irtibat kurmamış olması durumunda TCK 158/1-f maddesinde düzenlenen nitelikli hal gerçekleşmiş olacaktır.⁸⁶⁴ Örneğin online alışveriş sitesi gibi bir site oluşturup insanların alışveriş yapmasının sağlanması sonucu haksız yarar elde edilmesi durumunda TCK 244. maddesinde sayılan hareketler olmaksızın gerçek kişiler hileli davranışlarla aldatılmakta ve nitelikli dolandırıcılık suçu gerçekleştirilmektedir.⁸⁶⁵ Ancak Yargıtay fail ile aldatılan kimse arasında herhangi bir şekilde irtibat kurulması halinde de bu nitelikli halden hüküm kurulması yönünde bazı kararlar vermiştir.⁸⁶⁶

TCK 158/1-f maddesinde düzenlenen nitelikli halin uygulanabilmesi için fail bilişim sistemini araç olarak kullanarak hileli davranışlarda bulunmalı, hileli hareketlerin yöneltildiği kimseyle fail arasında herhangi başka bir irtibat kurulmaksızın aldatılan kimse bilişim sistemine güven duyarak tasarrufta bulunmalıdır. Örneğin failin internet sitesi üzerinden verdiği sahte bir ilan için ayrıca telefonla arayarak mağduru ikna etmesi durumunda aldatma tamamen bilişim sistemi aracılığıyla gerçekleştirilmediğinden TCK 158/1-f değil; 158/1-g'deki ağırlaştırıcı hal uygulanacaktır.⁸⁶⁷

Doktrinde bilgi güncellemesi bahanesiyle banka adına müşterilere mail gönderip onlardan bilgilerini alıp hesaplarından haksız çıkar sağlama durumunu TCK 158/1-f maddesi kapsamında değerlendiren yazarlar vardır.⁸⁶⁸ Ancak dolandırıcılık suçunun

⁸⁶² Ünver, s. 98; Özbek, Banka ve Kredi Kartları, s. 1059; Taşkın, s. 348-349.

⁸⁶³ Açıkgöz, s. 119.

⁸⁶⁴ Korkmaz, s. 1424.

⁸⁶⁵ Ketizmen, s. 183.

⁸⁶⁶ Örneğin 15. CD E. 2014/2393, K. 2016/5769 K.T. 02.06.2016.

⁸⁶⁷ Korkmaz, s. 1427.

⁸⁶⁸ Karagülmez, s. 194; Mahmutoglu, s. 885.

oluşması için aldatılan kimsenin kendi rızasıyla malvarlığı üzerinde tasarrufta bulunması gerekir. Bu yöntemde hileli davranışlar, aldatılan kimseden banka bilgileri alınmak için kullanılmakta ve elde edilen bilgilerle daha sonra fail kendine yarar sağlamaktadır. Dolandırıcılık suçu açısından tipiklik gerçekleşmediğinden başka bir ifadeyle aldatılan kimse kendi rızasıyla malvarlığı üzerinde bir tasarrufta bulunmadığından TCK 158/1-f maddesinden değil;⁸⁶⁹ TCK 244/4. maddesinden hüküm kurulmalıdır.

Bilişim sistemi niteliğindeki bir otomatın sunduğu hizmetten otomatın işleyişine veya sistemindeki verilere müdahale etmek suretiyle bedel ödmeden yararlanılması sonucu haksız bir menfaat sağlanması durumunda hem TCK 244/4 hem de TCK 163. maddesi gerçekleştirilmektedir. Ancak TCK 244. maddesi tali norm olduğundan, böyle bu durumda olaya asli norm olarak TCK 163. maddesi uygulanacaktır.⁸⁷⁰

TCK 163/2. maddesindeki fiilin işlenmesiyle TCK 244/4. maddesinin gerçekleştirilemeyeceği kanaatindeyiz. Zira TCK 163/2. maddesinde şifreli veya şifresiz yayınlardan yararlanma fiili işlenirken herhangi bir bilişim sisteminin işleyişi engellenmediğinden, bozulmadığından veya verilere müdahale niteliğinde bir fiil icra edilmediğinden bu iki fıkra arasında herhangi bir içtima ilişkisi söz konusu değildir.⁸⁷¹ Ancak şifreli veya şifresiz yayınlardan yararlanmak için bilişim sistemine girilmesi söz konusu olabilir. Örneğin kablosuz internetten şifresi kırılmak suretiyle faydalanma durumunda bir bilişim sistemine girme söz konusudur. Bu durumda elektromanyetik dalgalarla kullanılan kablosuz internetten bedel ödenmeksizin yararlanılması karşılıksız yararlanma suçuna vücut verecektir.⁸⁷² Böyle bir örnekte fail hakkında gerçek içtima

⁸⁶⁹ Korkmaz, s. 1428.

⁸⁷⁰ Açıkgöz, s. 131.

⁸⁷¹ Kablosuz internetin şifresinin kırılması başka bir ifadeyle bilişim sistemine girme suçu, TCK 163/2. maddesindeki suçun hareketleri kısmi ayniyet teşkil ettiğinden fikri içtima kuralı gereğince en ağır cezanın öngörüldüğü TCK 163/2'den hüküm kurulmalıdır. Açıkgöz, s. 132.

⁸⁷² Açıkgöz, s. 132.

kuralı gereğince hem TCK 243. maddesinden hem de TCK 163/2. maddesinden ceza hükmü kurulmalıdır.

TCK 163/3. maddesindeki suçun bir bilişim sistemine müdahale edilmesi suretiyle işlenmesi durumunda, TCK 244/4. maddesindeki suç da gerçekleşmektedir. Örneğin elektrik dağıtımını gerçekleştiren şirketin bilişim sistemine müdahale ederek tüketim miktarının belirlenmesini önleyen kişi, ayrıca borcun çıkmasını engelleyerek haksız bir maddi çıkar elde ettiğinden, failin fiili hem TCK 244/4. maddesi için hem de TCK 163/3. maddesi için tipiktir. Ancak TCK 244/4'ün tali norm olarak öngörülmesi dolayısıyla olaya TCK 163/3. maddesi uygulanacaktır.⁸⁷³

Kredi kartının fiziki olarak ele geçirilmediği ancak kart bilgilerinin ele geçirilerek kullanılması durumunda doktrinde bir görüş TCK 245'te kartın fiziken kullanılması gerektiği düşüncesinden hareketle cezai sorumluluğu TCK 244/3 veya 4. fıkraları çerçevesinde değerlendirmektedir.⁸⁷⁴ Ancak kredi kartı, banka kartından farklı olarak 5464 S. Kanun gereği *“fiziki varlığı bulunmayan kart numarası”* şeklinde de tanımlandığından, kart bilgisinin ele geçirilerek örneğin online alışveriş yapılması suretiyle haksız yarar elde edildiği durumda *“kartın bağlı olduğu hesabın bulunduğu bilişim sistemindeki verilerin alışveriş yapılan internet sitesine gönderilmesi söz konusu olduğundan”* fiil TCK 244/4 ve TCK 245/1. maddelerinin her ikisini de ihlal etmektedir. Fakat TCK 244/4. maddesi tali norm olarak ihdas edildiğinden, TCK 245/1. maddesinden hüküm kurulacaktır.⁸⁷⁵

⁸⁷³ Açıkgöz, s. 133.

⁸⁷⁴ Özbek, Banka veya Kredi Kartı, s. 1032.

⁸⁷⁵ Açıkgöz, s. 135.

Doktrinde bir görüş TCK 245 ve TCK 244/4. maddeleri arasında özel- genel norm ilişkisi olduğunu ve TCK 245. maddesinin özel norm olduğunu savunmaktadır.⁸⁷⁶ Ancak iki madde arasındaki ilişki asli- tali norm ilişkisidir.

5464 S. Kanunda banka kartı fiziksel varlığı olan bir kart olarak tanımlandığından, kartın elde edilmeden, kart bilgilerinin kullanılarak haksız çıkar elde edildiği örneklerde bir görüş kartın fiziksel olarak kullanılmasını aradığından TCK 245/1. maddesindeki kanuni tipe uygun eylemin gerçekleşmediğini dolayısıyla sorumluluğun TCK 244/4. maddesinden doğabileceğini ileri sürmüştür.⁸⁷⁷ Başka bir görüşse banka kartı bilgilerinin kart elde edilmeden kullanılarak haksız çıkar elde edilmesi durumunda TCK 245. maddesinden sorumluluğun doğacağını ifade etmektedir.⁸⁷⁸ TCK 245/1. maddesinde banka kartının ele geçirilmesi arandığından ve 5464 S. Kanunda banka kartının fiziki bir kart olduğu ifade edildiğinden, kartın elde edilmeden kart bilgilerinin kullanılarak haksız çıkar elde edilmesi halinde TCK 245. maddesi bakımından tipik fiil söz konusu olmadığından, TCK 244/4. maddesinden hüküm kurulmalıdır.

Doktrinde bir görüşe göre banka veya kredi kartının kullanılarak örneğin ATM'den para çekilmesi durumunda, kart sahibinin banka bilişim sistemindeki hesabında veriler değiştiğinden TCK 244/4 maddesi ve 245/1. maddesi aynı anda gerçekleşmektedir. Ancak TCK 244/4. maddesi tali norm olduğundan olaya TCK 245/1. maddesi uygulanmalıdır.⁸⁷⁹

5411 S Bankacılık Kanunu 160. maddesinde bankacılık zimmeti banka yönetim kurulu başkan ve üyeleri ile diğer mensuplarının “*Görevi nedeniyle zilyetliği kendisine devredilmiş olan veya koruma ve gözetimiyle yükümlü olduğu para veya para yerine geçen evrak veya senetleri veya diğer malları kendisinin ya da başkasının zimmetine*

⁸⁷⁶ Baş, s. 262.

⁸⁷⁷ Erdoğan, s. Açıkgöz, s. 136.

⁸⁷⁸ Ketizmen, s. 187; Karagülmez, s. 301-302.

⁸⁷⁹ Açıkgöz, s. 136.

geçirmesi” şeklinde tanımlanmıştır. Banka görevlisinin kendisine görevi dolayısıyla verilen bilişim sistemini kullanarak, kendisi veya başkası hesabına para aktarması her ne kadar TCK 244/4. maddesi bakımından tipik olsa da bu normun tali norm niteliği dolayısıyla fail bankacılık zimmeti suçundan sorumlu olacaktır.⁸⁸⁰

2. Bileşik Suç

TCK 244/1 ve 2. fıkralarında tanımlanan suçlar, “*bilişim sistemleri aracılığıyla haksız yarar sağlama suçunun*” unsuru olduğundan, “*bilişim sistemi aracılığıyla haksız yarar sağlama suçu*” bileşik suç niteliğindedir.⁸⁸¹ Yani fail “*bir bilişim sisteminin işleyişini bozarak veya engelleyerek ya da sistemdeki verileri bozarak, yok ederek, değiştirerek, erişilmez kılarak sisteme veri yerleştirerek ya da var olan verileri başka yere göndererek*” kendisi veya başkası yararına haksız çıkar sağladığında ortada tek fiil, tek suç vardır.⁸⁸² TCK 42. maddesi gereğince ayrıca TCK 244/1 veya 2. maddesinden cezalandırma yapılmayacak sadece TCK 244/4. maddesinden hüküm kurulacaktır.⁸⁸³

3. Zincirleme Suç

Zincirleme suç hükümlerinin TCK 244/4. maddesi bakımından uygulanması mümkündür.⁸⁸⁴ Bilişim sistemi aracılığıyla haksız yarar sağlama kararının icrası kapsamında değişik zamanlarda aynı kişiye karşı TCK 244. maddesinin ilk iki fıkrasında yazan hareketleri gerçekleştirmek suretiyle farklı haksız yararlar elde ederse, fail hakkında TCK 43/1. maddesi gereğince belli oranda artırım yapılarak tek cezaya hükmedilecektir. Ayrıca bu suçun tek fiille birden fazla kişiye karşı işlenmesi durumunda

⁸⁸⁰ Koca, s. 97-98.

⁸⁸¹ Koca/ Üzülmöz, s. 921-922; Yazar/ Gökcan/ Artuç, s. 7315-7316; Açıkgöz, s. 114; Erdoğan, s. 262.

⁸⁸² Koca/ Üzülmöz, s. 922.

⁸⁸³ Koca/ Üzülmöz, s. 930.

⁸⁸⁴ Yaşar/ Gökcan/ Artuç, s. 7321; Soyaslan, s. 710.

da TCK 43/2. maddesi gereğince belli oranda artırım yapılarak tek cezaya hükmedilecektir.⁸⁸⁵

4. Fikri içtima

Dördüncü fıkra fiilin başka bir suç oluşturmaması halinde bu fıkra uyarınca cezaya hükmolunacağı ifade edilmiştir. Burada fikri içtimaya ilişkin genel kuraldan ayrılarak, farklı bir durum yaratılmış ve fiilin daha az cezayı gerektiren başka bir suçu oluşturmada dahi cezalandırmanın daha az cezayı gerektiren hükme göre yapılacağı belirtilmiştir.⁸⁸⁶ TCK 244. maddesinin gerekçesinde “...bir ve ikinci fıkralarda tanımlanan fiillerin işlenmesi suretiyle kişinin kendisine veya başkasına yarar sağlaması, ceza yapturumu altına alınmıştır. Ancak, bu fıkra hükmüne istinaden cezaya hükmedilebilmesi için, fiilin daha ağır cezayı gerektiren başka bir suç oluşturmaması gerekir.” denilmek suretiyle aslında fikri içtima kuralı tekrar edilmeye çalışılmış ancak madde metni her nasılsa “başka bir suç oluşturmaması halinde” şeklinde kanunlaştırılmıştır. Gerekçe madde metnine dahil olmadığından, bağlayıcı değildir. Dolayısıyla madde metnine göre hüküm kurma yoluna gidilecektir.

Getirilen bu düzenlemeyle aslında asli norm-tali norm ilişkisi kurulmuştur ve bilişim sistemleri aracılığıyla haksız yarar sağlama suçu oluşabilecek kanun boşluğunu engellemek amacıyla tali norm niteliğinde düzenlenmiştir.⁸⁸⁷ Başka bir deyişle TCK 244/4. maddesi tali norm olduğundan asli normun önceliği ilkesi gereği TCK 244/4. maddesi ancak fiil başka bir suç teşkil etmiyorsa uygulanabilecektir.⁸⁸⁸ Fiil başka bir suça vücut veriyorsa o suçtan hüküm kurulacaktır.⁸⁸⁹ TCK 244. maddesinin gerekçesinde “Bu bakımdan, fiilin örneğin dolandırıcılık, hırsızlık, güveni kötüye kullanma veya zimmet

⁸⁸⁵ Erdoğan, s. 265.

⁸⁸⁶ Meran, s. 582.

⁸⁸⁷ Özbek/ Doğan/ Bacaksız, s. 979.

⁸⁸⁸ Mahmutoğlu, s. 879.

⁸⁸⁹ Koca/ Üzülmüş, s. 930.

suçunu oluşturmaları halinde, bu fıkra hükmüne istinaden cezaya hükmedilmeyecektir.” denilmek suretiyle de aslında fıkranın tali niteliği vurgulanmıştır. TCK 244/4. maddesi bilişim sistemleri aracılığıyla haksız yarar sağlama durumunda öncelikle uygulanacak bir hüküm değil; tersine boşluk kalmaması için ihdas edilmiş bir norm olduğundan⁸⁹⁰ fikri içtima kuralının uygulanması bu suç bakımından mümkün değildir.⁸⁹¹

Ancak doktrindeki aksi görüşe göre “*bilişim sistemi aracılığıyla haksız yarar sağlama suçunun*” tali norm olarak öngörülmesi, bu suçla başka bir suçun fiillerin örtüşmesi durumunda iki suç arasında fikri içtima kuralının uygulanmayacağı şeklinde yorumlanamaz. TCK 244/4. maddesinin metninde “haksız çıkar sağlama”nın başka bir suça vücut vermemesi arandığından, haksız bir çıkar elde etmenin söz konusu olmadığı suçlarla TCK 244/4 arasında fikri içtima ilişkisi kurulabilecektir.⁸⁹² Dolayısıyla TCK 243 ve TCK 244/4 maddeleri arasında fikri içtima ilişkisi vardır. Nitekim fail bilişim sistemleri aracılığıyla haksız yarar elde etmek için sisteme girdiğinde iki suçun icra hareketleri kısmen örtüştüğünden fikri içtima kuralı gereği fail en ağır cezayı öngören suçtan (TCK 244/4) sorumlu olacaktır.⁸⁹³ TCK 136 ve TCK 228/3 ile TCK 244/4 arasında da fikri içtima ilişkisi vardır.⁸⁹⁴ FSEK kapsamında bilgisayar programları eser olarak nitelendirilmiştir. Bu programlar da verilerden oluştuğundan bu programlara müdahale, verilere müdahale niteliğindedir. FSEK 71/1. maddesinde düzenlenen bilgisayar programını değiştirmek, bilişim programını çoğaltmak, dağıtmak, iletmek, yayımlamak fiilleri TCK 244/4. maddesi açısından da tipik nitelikte olduğundan iki madde arasında fikri içtima ilişkisi olabilir. FSEK’te haksız çıkar sağlama aranmamış ancak suçun icra hareketleri her iki suça da vücut veriyorsa yani suçların maddi unsuru olan fiiller kısmen

⁸⁹⁰ Koca, s. 97.

⁸⁹¹ Parlar, s. 28; Soyaslan, s. 711; Meran, s. 583.

⁸⁹² Açıkgöz, s. 117.

⁸⁹³ Açıkgöz, s. 141.

⁸⁹⁴ Açıkgöz, s. 141-144.

aynıysa fikri içtima kuralı gereği en ağır cezadan hüküm kurulur.⁸⁹⁵ Ancak bu görüşe katılmak mümkün değildir zira fikri içtima ilişkisinin söz konusu olabilmesi için fiilin bir bütün olarak her iki suç bakımından tipik olması aranmalıdır. Dolayısıyla fikri içtima kuralının TCK 244/4. maddesi bakımından uygulanması mümkün değildir.

Doktrinde bir görüşe göre bilişim sistemleri aracılığıyla haksız yarar sağlama suçunu işlemek isteyen failin fiili yarım kalmış ve netice meydana gelmemişse fiil hem TCK 244/1-2’yi hem de TCK 244/4’e teşebbüsü meydana getirdiğinden yani tek bir fiille kanunun farklı maddeleri ihlal edildiğinden fikri içtima kuralı gereği fail daha ağır cezayı gerektiren suçtan ceza alacaktır.⁸⁹⁶ Ancak böyle bir yorumun mümkün olmadığını düşünüyoruz. Zira failin kastı baştan itibaren TCK 244/4’ün işlenmesine yöneliktir ve bilişim sistemi aracılığıyla haksız yarar elde etme suçunun fiil unsurunun bir kısmını TCK 244/1 ve 2. fıkralarında sayılan hareketlerin oluşturması bu iki suç arasında fikri içtima ilişkisi olduğunu göstermez.

I. YAPTIRIM, SORUŞTURMA, KOVUŞTURMA

“Bilişim sistemleri aracılığıyla haksız çıkar sağlanma suçunun” müeyyidesi olarak “iki yıldan altı yıla kadar hapis ve beş bin güne kadar adli para cezasına” hükmolunacağı öngörülmüştür. Hapis cezası ve adli para cezası, seçimlik olarak öngörülmediğinden her iki ceza birlikte uygulanacaktır. Koşulların olması halinde hapis cezasının ertelenmesi mümkündür ancak bu hal adli para cezasının infazını engellemeyecektir. CMK 231. maddesi gereği HAGB uygulanması mümkün değildir.

⁸⁹⁵ Ancak burada her bilişim sistemi programı eser olarak kabul edilmediğinden fikri içtima ilişkisi her durumda geçerli değildir. Eser niteliğine sahip olup olmadığı FSEK’e göre tespit edilecek eser niteliği taşımayan programlar için fikri içtima ilişkisi geçerli olmayacak ve sadece TCK 244/4 işlenmiş sayılacaktır. Açığöz, s. 144.

⁸⁹⁶ Yaşar Gökcan/ Artuç, s. 7320.

HAGB ancak tek tip cezanın öngörüldüğü veya adli para cezasının hapis cezasına seçimlik olarak öngörüldüğü durumlarda uygulanabilir.⁸⁹⁷

Adli para cezasının alt sınırı maddede gösterilmediğinden, TCK 52. maddesi gereği beş gün alt sınır olacaktır. Bilişim sistemi aracılığıyla haksız yarar sağlama suçu açısından nitelikli hale ve etkin pişmanlık hükümlerine yer verilmemesi yerinde bir tercih olmamıştır.⁸⁹⁸

TCK 66. maddesi gereğince beş yıldan fazla olmamak üzere hapis veya adli para cezasını gerektiren suçlarda sekiz yıl geçmesiyle dava zamanaşımı dolacağından, bilişim sistemi aracılığıyla haksız yarar elde edilmesi suçuna ilişkin kamu davası sekiz yılın geçmesiyle düşecektir.

TCK 244/4. maddesi resen soruşturulacak ve kovuşturulacak bir suçtur, uzlaştırma kapsamında değildir. 5235 S Kanunun 11. ve 12. maddeleri gereğince görevli mahkeme, Asliye Ceza Mahkemeleridir. 30.11.2021 tarihli Resmi Gazete yayımlanan HSK'nın 1229 numaralı kararı gereğince 15.12.2021 tarihinden itibaren görev yapacak Bilişim İhtisas Mahkemeleri belirlenmiştir.⁸⁹⁹ Karara göre “*iki asliye ceza mahkemesi bulunan yerlerde 2; üç, dört veya beş asliye ceza mahkemesi bulunan yerlerde 3; altı, yedi, sekiz veya dokuz asliye ceza mahkemesi bulunan yerlerde 6; on veya daha fazla asliye ceza mahkemesi bulunan yerlerde 8; yirmi beş veya daha fazla asliye ceza mahkemesi bulunan yerlerde 20 ve 21; otuz beş veya daha fazla asliye ceza mahkemesi bulunan yerlerde 20, 21, ve 22 numaralı asliye ceza mahkemeleri ihtisas mahkemesi olarak*” görevlendirilmiştir.

⁸⁹⁷ Centel/ Zafer, s. 859.

⁸⁹⁸ Mal varlığına karşı suçlar ve TCK 245. maddesi için etkin pişmanlık hükmüne yer verilmişken; TCK 244/4. maddesi için etkin pişmanlık hükmüne yer verilmemiştir. Akbulut, s. 265.

⁸⁹⁹ Doktrinde bir görüşe göre özel uzmanlık mahkemelerin kurulması, mahkemelerin yetki ve görevlerine ilişkin karmaşaya yol açacağından bilişim suçlarıyla alakalı teknik konularda bilirkişiye başvurulması daha yerinde bir tercih olacaktır. Ünver, s. 145

CMK 12. maddesi gereğince yetkili mahkeme “suçun işlendiği yer mahkemesidir”. Ayrıca 7331 S Kanunla 08.07.2021 tarihinde CMK 12. maddesine eklenen altıncı fıkra gereğince “Bilişim sistemlerinin, banka veya kredi kurumlarının ya da banka veya kredi kartlarının araç olarak kullanılması suretiyle işlenen suçlarda mağdurun yerleşim yeri mahkemeleri de yetkilidir.” Yani artık hem suçun işlendiği yer mahkemesi hem de mağdurun bulunduğu yer mahkemesi yetkili olacağından, birden fazla yetkili mahkeme söz konusudur.



SONUÇ

Kişisel bilgisayarların ve bilhassa bilişim sistem ağlarından internetin kullanımının yaygınlaşması insan yaşamını eğitimden askeri faaliyetlere, eğlence hayatından ticari hayata kadar neredeyse her alanda etkilemiş; zaman ve mekân sınırları kaldırılarak dünya küresel bir köy haline gelmiştir. Teknolojik gelişmelerle birlikte hayatımızın vazgeçilmez bir parçası haline gelen bilişim sistemleri de insanlar tarafından kötüye kullanılmaya başlamış, bu durum ise bilişim alanından yeni kanuni düzenlenmelerin ihdas edilmesi ihtiyacını ortaya çıkarmıştır. Kanun koyucu artık hayatın her alanında kullanım alanı bulan ve dolayısıyla gerek yeni anti-sosyal fiillerin işlendiği gerekse mevcut suç tiplerinin işlenmesi için yeni bir alan yaratması sebebiyle bilişim sistemleri aracılığıyla veya bu sistemlere karşı işlenen fiilleri yaptırıma bağlamak istemiştir. Her türlü işlemin bilişim sistemleri aracılığıyla kolayca ve kısa bir sürede yapılması, bu sistemlerin kullanım oranını artırmıştır. Bu durumsa insanların sistemlerin ve sistemlerdeki verilerin güvenliğine, sistemlerin sağlıklı bir şekilde işleyişine ilişkin haklı çıkarlarının korunması gerekliliğiyle bazı fiillerin suç olarak öngörülmesi sonucunu doğurmuştur.

Bilişimin ayrı bir disiplin olması ve bu alanda icat edilen teknolojilerin teknik bilgi ve uzmanlık gerektirmesi dolayısıyla bu teknolojilere karşı veya bu teknolojiler aracılığıyla işlenen suçlarda soruşturmanın ve kovuşturmanın etkili bir biçimde yürütülebilmesi için muhakeme sürecinde yer alan kolluk görevlilerinden savcı ve hakimlere kadar her bir süjenin bilişim teknolojileriyle ilgili eğitilmeleri ve bilhassa bu alanda uzmanlaşmış ceza mahkemelerin kurulması ehemmiyet arz etmektedir. Bu çerçevede Türkiye’de kolluk kuvvetlerinde özel birim (siber suçlarla mücadele daire başkanlığı) kurulmuştur. Ayrıca Nisan 2021’de yayınlanan İnsan Hakları Eylem Planında bilişim suçlarıyla ilgili ihtisas mahkemelerinin kurulacağı ifade edilmiştir. Buna paralel

olarak HSK'nın 1229 numaralı kararı gereğince 15.12.2021 tarihinden itibaren görev yapacak Bilişim İhtisas Mahkemeleri belirlenmiştir.

Bilişim suçları daha çok yeni bir alan sayılabileceğinden, bu suçlarla mücadelede ve bu suçların muhakemesinde görevli yetkili ve merciler bilişim teknolojileri konusunda gerekli teknik bilgiye ve uzmanlığa sahip değillerdir. Ayrıca suçların delillerini ortaya koyabilmek başlı başına ayrı bir sorundur zira bilişim teknolojilerinin faillere sağlamış olduğu anonimlik ve suçun sanal ortamda işlenmesi dolayısıyla delillerinin geleneksel suçlardan farklılık arz etmeleri suç delillerinin toplanmasını zorlaştırmaktadır. Bilişim suçlarında delilleri elde etmenin zorluğu adli bilişimin önem kazanmasına yol açmıştır. Bilişim teknolojilerinin çok teknik bir alan olması bilişim alanında suçlar konusunda çalışan insanların da teknik bilgiye ve uzmanlığa sahip olmasını gerektirir.

Bilişim alanında suçlara ilişkin, özellikle AKSSS'ye uyum sağlamak amacıyla gerçekleştirilen kanun değişiklikleri, bilişim suçlarına karşı mücadelede isabetli adımlar olmuştur. Ancak yapılan düzenlemeler ve değişiklikler bazı noktalarda yetersiz kalmış veya yerinde olmamıştır. Öncelikle “*Bilişim Alanında Suçlar*” bölümünün “*Topluma Karşı Suçlar*” kısmında düzenlenmesi isabetsizdir. Çünkü bilişim suçlarıyla asıl kişilerin bireysel menfaatleri ihlal edilmektedir. Bu suçların mağduru kişiler olduğundan, bu suçların “*Kişilere Karşı Suçlar*” bölümünde düzenlemesi daha yerinde bir tercih olacaktır.

Malvarlığına karşı suçlarda hukuki alacağın tahsili amacıyla hareket edilmesi halinde öngörülen hafifletici sebebin bilişim suçlarında da öngörülmesi gerekirdi. Örneğin satın aldığı bilgisayar programının parasını ödemeyen kimsenin bilgisayarına girerek bu programı silen program satıcısının fiili için cezasında indirim öngörülmemesi yerinde bir tercih değildir.

Her ne kadar bilişim sistemine girilmesinin müstakıl bir suç haline getirilmesi olumlu bir deęişiklik olarak nitelendirilse de kanun koyucu, 765 S. TCK'da yer alan verilerin ele geçirilmesi suçunu 5237 S. TCK'da düzenlememiştir. Ele geçirilen veriler kişisel veri niteliğindeyse, verilerin TCK 136. maddesi bağlamında korunduęu; verilerin sistemden ortadan kaldırılarak ele geçirilmesi durumunda, verilerin TCK 244/2. maddesi bağlamında koruma altında olduęu söylenebilir. Fakat bu suçlar açısından tipiklięin gerçekleşmedięi durumlarda veriler korumasız kalmaktadır. Bu eksiklięin giderilmesi gerekir. Ayrıca TCK 243. maddesinde düzenlenen teknik araçlarla veri nakillerinin izlenmesi suçunun farklı bir maddede kaleme alınması daha isabetli bir tercih olacaktır.

AKSSS'nin 7. maddesinde devletlere bilgisayarla ilgili sahtecilik eylemlerinin müeyyide altına alınmasına ilişkin bir yükümlölük getirilmiş ancak Ceza Kanunu Koyucusu bu yükümlölüęe uygun hareket etmemiştir. Günümüzde resmi ve özel evrakların bilgisayarlar aracılığıyla hazırlandığı ve hatta elektronik belgelerin kullanıldığı bir ortamda bu belgeler üzerinde bilgisayar aracılığıyla yapılan müdahaleleri sahtecilik suçuyla deęil verileri deęiştirme ve yok etme suçuyla cezalandırılması yerinde bir tercih olmamıştır. Söz konusu 7. madde kapsamındaki fiiller TCK 244/2. maddesi ve evrakta sahtecilik suçları (TCK 204 vd) kapsamında deęerlendirilebilecek olsa da AKSSS'nin getirdiğı yükümlölük gereğince bilgisayarlarla gerçekleştirilen sahtecilik fiillerinin TCK'da yaptırıma bağlanması gerekir.

TCK 244. maddesindeki suçlar, özgü suç olarak öngörölmemiş ancak kamu görevlileri, banka ve kredi kurumu çalışanları için cezayı ağırlaştırıcı neden öngörölerek nitelikli hal bakımından özgü suç yaratılabilirdi. Zira sayılan kimseler kurum bilgisayarlarına rahatlıkla erişim sağlayabildiğinden, TCK 244. maddesini ihlal etmeleri daha kolay olacaktır

Verilere müdahalenin düzenlendiği TCK 244. maddesinin ikinci fıkrasında “*sisteme veri yerleştirme ve var olan verileri başka yere gönderme*” hareketlerine yer verilmesi yerinde bir düzenleme olmamıştır. Zira “*sisteme veri yerleştirme ve verileri başka bir yere gönderme*” hareketlerinde sistemdeki mevcut verilere yönelik bir müdahale söz konusu değildir. Fail sisteme veri yerleştirirken veya verileri başka yere gönderirken sistemdeki mevcut verilere müdahale etmemekte ancak sisteme müdahale etmektedir. Nitekim veri yerleştirme hareketiyle verileri değiştirmek; verileri başka sisteme göndermek hareketiyle verileri bozma, yok etme kastediliyorsa bu hareketler zaten madde metninde yer aldığından gereksiz bir tekrara gidilmiş olacaktır. Bu sebeple verilere müdahale niteliği taşımayan bu hareketlerin bu fıkra düzenlenmesi doğru bir tercih olmamıştır. Bu hareketler sistemin işleyişini engelliyor ya da bozuyorsa sisteme müdahale olarak değerlendirilmeli ancak sisteme müdahale söz konusu değilse farklı bir suç olarak düzenleme altına alınmalıdır

YCGK kararı sonrası verilerin taşınır mal olarak kabul edilmesi, ceza hukukunda geçerli olan “*biçimsel kanunilik ilkesi*” ve “*kıyas yasağına*” aykırıdır. Hırsızlık suçunun kanuni tanımında açıkça taşınır mal ifadesi kullanıldıktan sonra verilere müdahale niteliğindeki hareketleri hırsızlık suçu kapsamında değerlendirmek, TCK 2/3. maddesinde düzenlenen kıyasa yol açacak biçimde genişletici yorum yapmaktır. Zira veriler klasik anlamda taşınır malların sahip olduğu hiçbir özelliğe sahip değilken kanunda da böyle bir kabule yer verilmemiştir. Bu sebeplerle kanunda açıkça verilerin taşınır mal sayılacağına dair bir hüküm olmadıkça verilere müdahale niteliğindeki hareketlerin TCK 142/2-e maddesinde düzenlenen hırsızlık suçuna vücut vermeyeceği görüşüne iştirak ediyoruz.

KAYNAKÇA

Açıkgöz, Emre İkbâl, **Bilişim Sistemi Aracılığıyla Haksız Yarar Sağlama Suçu (TCK m. 244/4)**, Ankara, Adalet Yayınevi, 2020.

Akbulut, Berrin, **Bilişim Alanında Suçlar**, 2. B., Ankara, Adalet Yayınevi, 2017.

Akbulut, Berrin, “Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme”, **Selçuk Üniversitesi Hukuk Fakültesi Dergisi**, C. 24, S. 2, 2016, ss. 7-55.

Akın, Gülfer, “Belgede Sahtecilik Suçlarının Konusu Olarak Elektronik/ Dijital Belge”, **Bilişim Hukuku Dergisi**, C. 3, S. 1, 2021, ss. 76-138.

Apaydın, Cengiz, “Bilişim Sistemindeki Verileri Yok Etme, Bozma, Erişilmez Kılma, Değiştirme, Hukuka Aykırı Olarak Verileri Yerleştirme veya Gönderme Suçu ile Bu Suretle Hukuka Aykırı Yarar Elde Etme Suçunun Değerlendirilmesi”, **Terazi Hukuk Dergisi**, C. 10, S. 111, 2015, ss. 14-41.

Apaydın, Cengiz, “Bilişim Sisteminin İşleyişini Engelleme ve Bozma Suçları”, **Ceza Hukuku Dergisi**, C. 10, S. 29, 2015, ss. 205-264.

Arslan, Çetin/ Baştürk İhsan, “Belgede Sahtecilik Suçunun Konusu Olarak Elektronik Ortamdaki Veriler”, **EÜHFD**, C. 8, S. 2, 2013, ss. 195-219.

Artuk, Mehmet Emin / Gökçen, Ahmet/ Alşahin, Emin / Çakır, Kerim, **Ceza Hukuku Genel Hükümler**, 15. B., Ankara, Adalet Yayınevi, 2019.

Baş, Eylem, **Banka veya Kredi Kartlarının Kötüye Kullanılması Suçu**, Ankara, Yetkin Yayınevi, 2015.

Başlar, Yusuf, “Elektronik İmza Kanunu’nda Düzenlenen Bilişim Suçları”, **ABÜHFD**, C. 4, S. 7, 2016, ss. 41-64.

Bourgeois, Davis T./ Smith , James L./ Wang, Shouhong/ Mortatı, Joseph, **Information Systems for Business and Beyond**, 2014.

Casey, Eoghan, **Digital Evidence and Computer Crime: Forensic Science, and the Internet**, 2000.

Centel, Nur/ Zafer, Hamide, **Ceza Muhakemesi Hukuku**, 17. B., İstanbul, Beta Yayınevi, 2020.

Çetin, Muhammet Sefa, Yargıtay Kararları Işığında Bilişim Sistemine Girme veya Kalma Suçu, **TAAD**, S. 45, 2021, ss. 1-28.

Değirmenci, Olgun, 2004 Türk Ceza Kanunu’nun Bilişim Suçları Bakımından Değerlendirilmesi, **TBBD**, S. 58, 2005, ss. 195-208.

Değirmenci, Olgun, **Ceza Muhakemesinde Sayısal (Dijital) Delil**, Ankara, Seçkin Yayınevi, 2014.

Doğan, Koray, **Neticesi Sebebiyle Ağırlaşmış Suçlar**, 2. B., Ankara, Adalet Yayınevi, 2015.

Dönmezer, Sulhi / Erman, Sahir, **Nazari ve Tatbiki Ceza Hukuku (Cilt II)**, 13. B., İstanbul, Der Yayınları, 2019.

Dülger, Murat Volkan, **Bilişim Suçları ve İnternet İletişim Hukuku**, 9. B., Ankara, Seçkin Yayınevi, 2020.

Eker, Ö. Umut, “Türk Ceza Hukukunda Bilişim Suçları Eski TCK Bağlamında Hukukumuzda Yer Alan İlk Düzenlemeler ve 5237 Sayılı Yeni Türk Ceza Kanunu’nun İlgili Hükümlerinin Yorumu”, **TBBD**, C. 19, S. 62, 2006, ss. 101-131.

Ekici Şahin, Meral/ Koruculu, Irmak, “Bilişim Sistemine Girme Suçu: Suçun Kamu Personeli ve Özel Sektör Çalışanlarına Tahsis Edilen Bilgisayarlarla İşlenmesine İlişkin Bir Değerlendirme”, **DEÜHFD**, C. 21, ÖZEL S. 2019, ss. 585-626.

Erdağ, Ali İhsan, “Bilişim Alanında Suçlar (Türk ve Alman Ceza Hukukunda)”, **GÜHFD**, C. 14, S. 2, 2010, ss. 275-303.

Erdoğan, Yavuz, “Bilişim Sistemine Girme ve Kalma Suçu”, **DEÜHFD**, C. 12, Özel S. 2010, ss. 1363-1433

Erem, Faruk, “Bilgisayar Suçları ve Türk Ceza Kanunu”, **TBBD**, 1993, ss. 178-186.

Ergün, İsmail, “**Siber Suçların Cezalandırılması ve Türkiye’de Durum**”, Ankara, Adalet Yayınevi, 2008.

Ersoy, Yüksel, “Genel Hukuki Koruma Çerçevesinde Bilişim Suçları”, **AÜSBFD**, C. 49, S. 3, 1994, ss. 149-183.

Gözel, Arif, “Belgede Sahtecilik Suçlarının Konusu Olarak Belge ve Elektronik Belge”, **SDÜHFD**, C. 5, S. 1, 2015, ss. 143-201.

Günday, Metin, **İdare Hukuku**, 9. B., Ankara, İmaj Yayınevi, 2015.

Hafizoğulları, Zeki / Özen, Muharrem, **Türk Ceza Hukuku Genel Hükümler**, 8. B., Ankara, US-A Yayınevi, 2015.

Hafizoğulları, Zeki/ Özen, Muharrem, **Türk Ceza Hukuku Özel Hükümler Toplama Karşı Suçlar**, 3. B., Ankara, US-A Yayınevi, 2017.

İçel, Kayıhan, “Avrupa Konseyi Siber Suç Sözleşmesi Bağlamında Avrupa Siber Suç politikasının Ana İlkeleri”, **İÜHFM**, C. 59, S. 1-2, 2001, ss. 3-10.

İçel, Kayıhan, “Görünüşte Birleşme (İçtima) İlkeleri ve Yeni Türk Ceza Kanunu”, **İstanbul Ticaret Üniversitesi Sosyal Bilimler Dergisi**, S. 14, 2008, ss. 35-49.

İçel, Kayıhan, **Suçların İçtimaı**, İstanbul, İstanbul Üniversitesi Yayınları, 1972.

İhtiyaroğlu, Uğur, “Bilişim Sistemine Girme Suçunun Yargı Kararları Bağlamında İncelenmesi”, **HHFD**, C. 10, S. 2. 2020, ss. 406-440.

Karagülmez, Ali, **Bilişim Suçları Soruşturma ve Kovuşturma Evreleri**, Ankara, Seçkin Yayınevi, 2011.

Karakehya, Hakan, “Türk Ceza Kanunu’nda Bilişim Sistemine Girme Suçu”, **TBBD**, S. 81, 2009, ss. 1-24.

Katoğlu, Tuğrul, “Ceza Hukukunda Suçun Mağduru Kavramının Sınırları”, **AÜHFD**, C. 61, S. 2, 2012, ss. 657-694.

Kayaer, Nebahat, “Türk Hukukunda Bilişim Sistemine Girme Suçu”, **Ceza Hukuku Dergisi**, C. 14, S. 39, 2019, ss. 83-128.

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

Koca, Mahmut/ Üzülmmez, İlhan, **Türk Ceza Hukuku Genel Hükümler**, 13. B., Ankara, Seçkin Yayınevi, 2020

Koca, Mahmut/ Üzülmmez, İlhan, **Türk Ceza Hukuku Özel Hükümler**, 7. B., Ankara, Adalet Yayınevi, 2020.

Koca, Mahmut, “Hukukumuzda TCK’nun 244. Maddesi Kapsamında Bilişim Sistemini Engelleme, Bozma, Verileri Yok Etme veya Değiştirme Suçu”.

Korkmaz, Fülya, “Dolandırıcılık Suçunun Bilişim Sistemlerinin Araç Olarak Kullanılması Suretiyle İşlenmesi”, **AÜHFD**, C. 69, S. 3, 2020, ss. 1415-1436.

Köksal, Aydın, **Adı Bilgisayar Olsun**, İstanbul, Cumhuriyet Kitapları, 2010.

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

Mahmutoğlu, Fatih Selami, “Karşılaştırmalı Hukuk Bakımından İnternet Søjelerinin Ceza Sorumluluğu”, **İÜHFM**, C. 59, S. 1-2, ss. 39-49.

Mahmutoğlu, Fatih Selami, “Türk Ceza Kanunu’nda Yer Alan Bilişim Alanındaki Suçlar ve Karşılaşılan Sorunların Yargı Kararları Işığında Değerlendirilmesi”, **İÜHFM**, C. 71, S. 1, 2013, ss. 855-889.

Meran, Necati, **Yeni Türk Ceza Kanunu’nda Sahtecilik-Malvarlığı-Bilişim Suçları ile Ekonomi ve Ticaret Alanında Suçlar**, 2. B., Ankara, Seçkin Yayınevi, 2008.

Orta, Mesut, **Bilişim Suçları ve Elektronik Delillerin Toplanması, Muhafazası, Değerlendirilmesi, Sunulması (Adli Bilişim)**, Ankara, Yetkin Yayınevi, 2015.

Önok, Murat, “Avrupa Konseyi Siber Suç Sözleşmesi Işığında Siber Suçlarla Mücadelede Uluslararası İşbirliği”, **Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi**, Prof. Dr. Nur Centel’e Armağan, C. 19, S. 2, 2013, ss. 1229-1269.

Özbek, Veli Özer/ Doğan, Koray / Bacaksız, Pınar, **Türk Ceza Hukuku Özel Hükümler**, 16. B., Ankara, Seçkin Yayınevi, 2021.

Özbek, Veli Özer, “Banka ve Kredi Kartlarının Kötüye Kullanılması Suçu (TCK m. 245)”, **DEÜHFD**, C. 9, Özel S. 2007 ss. 1019-1063.

Özbek, Veli Özer, “İnternet Kullanımında Ortaya Çıkabilecek Bazı Ceza Hukuku Sorunları”, **DEÜHFD**, C. 4, S. 1, 2002, ss.101-158.

Özen, Muharrem / Baştürk, İhsan, **Bilişim-İnternet ve Ceza Hukuku**, Ankara, Adalet Yayınevi, 2011.

Özgenç, İzzet: **Türk Ceza Hukuku Genel Hükümler**, Ankara 2019.

Özsoy, Nevzat, “Yargıtay Kararları Işığında Doğrudan Bilişim Suçları (TCK 243 ve 244)” **Yaşar Hukuk Dergisi**, C.1 S. 2, 2019, ss. 295-352.

Parlar, Ali, **Türk Ceza Hukukunda Bilişim Suçları**, 3. B., Ankara, Bilge Yayınevi, 2015.

Parlar, Ali / Hatipoğlu, Muzaffer, **Türk Ceza Kanunu Yorumu**, 3. B., Ankara, Seçkin Yayınevi, 2010.

Sokullu Akıncı, Füsun: “Avrupa Konseyi Siber Suç Sözleşmesinde Yer Alan Maddi Ceza Hukukuna İlişkin Düzenlemeler ve Özellikle İnternette Çocuk Pornografisi”, **İÜHFM**, C. 59, S. 1-2, 2001, ss. 11-38.

Soyaslan, Doğan, **Ceza Hukuku Özel Hükümler**, 7. B., Ankara, Yetkin Yayınevi, 2014.

Tanrıkulu, Cengiz, **Ceza Muhakemesi Hukukunda Bilişim Sistemlerinde Arama ve Elkoyma**, Ankara, Adalet Yayınevi, 2014.

Taşkın, Şaban Cankat, “Bilişim Hukuku Uluslararası Uyuşmazlıkları”, **TBBD**, S. 85, 2009, ss. 332-372.

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

Tezcan, Durmuş / Erdem, Mustafa Ruhan/ Önok, Rıfat Murat, **Teorik ve Pratik Ceza Özel Hukuku**, 18. B., Ankara, Seçkin Yayınevi, 2020.

Tezcan, Durmuş, “Bilgisayar Karşısında Özel Hayatın Korunması”, **Anayasa Yargısı 8 (Anayasa Mahkemesinin 29.Kuruluş Yıldönümü Sempozyumu, Ankara, 25-27 Nisan 1991)**, ss. 385-392.

Tezcan, Durmuş, “Bilişim Suçlarında Uluslararası Adli Yardımlaşma”, **Yaşar Hukuk Dergisi**, C. 1, S. 2, 2019, ss. 287-294.

Tiedemann, Klaus (Çev. Feridun YENİSEY), “Bilgisayarlarla İşlenen Suçların Ceza Hukuku Yönünden İncelenmesi”, **İÜHF**, C. 41, S. 1-2, 1975, ss. 319-332.

Toroslu, Nevzat / Toroslu, Haluk, **Ceza Hukuku Genel Kısım**, 25. B., Ankara, Savaş Yayınevi, 2019.

Ünver, Yener, “Türk Ceza Kanunu’nun ve Ceza Kanunu Tasarısı’nın İnternet Açısından Değerlendirilmesi”, **İÜHF**, C. 59, S. 1-2, 2001, ss. 51-153.

Yalçın, Türkan / Köprülü, Timuçin, **Ceza Hukuku Genel Hükümler Uygulamalı Çalışmaları**, 7. B., Ankara, Savaş Yayınevi, 2020.

Yaşar, Osman/ Gökcan, Hasan Tahsin/ Artuç, Mustafa, **Yorumlu Uygulamalı Türk Ceza Kanunu (C. 5)**, 2. B., Ankara, Adalet Yayınevi, 2014.

Yazıcıoğlu, Yılmaz, **Bilgisayar Suçları Kriminolojik Sosyolojik ve Hukuki Boyutları ile**, İstanbul, Alfa Yayınevi, 1997.

Yazıcıoğlu, Yılmaz, “Yeni Türk Ceza Kanunundaki Bilişim Suçlarının Genel Değerlendirilmesi” **Yeditepe Hukuk Fakültesi Dergisi**, C. 2, S. 2, 2015.

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

Yılmaz, Sacit, “5237 Sayılı TCK’nın 244. Maddesinde Düzenlenen Bilişim Alanındaki Suçlar”, **TBBD**, S. 92, 2011, ss. 62-100.



ÖZET

Çalışmamızın konusunu TCK 243. maddesinde düzenlenen “Bilişim Sistemine Girme” ve TCK 244. maddesinde düzenlenen “Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme” suçları oluşturmaktadır. Üç bölümden oluşan çalışmamızın ilk bölümünde inceleme konusu suçların daha iyi anlaşılabilmesi için teknik kavramlar ve tanımlarına ilişkin açıklamaların yanında bilişim alanındaki suçlara ilişkin ulusal ve uluslararası düzenlemelerden bahsedilmiştir.

Çalışmanın ikinci bölümünde TCK 243. maddesinde düzenlenen “Bilişim Sistemine Girme” suçunun analitik incelenmesi yapılmıştır. Her ne kadar madde başlığı “Bilişim Sistemine Girme” olsa da TCK 243. maddesinde iki ayrı suça yer verilmiştir. Bu suçlar bilişim sistemine girme ve/veya bilişim sisteminde kalma ile veri nakillerinin teknik araçlarla izlenmesi suçlarıdır. Çalışmamızda bu suçların incelenmesine ayrı başlıklar altında yer verilmiş olup, sırasıyla suçların konusu, faili, mağduru, unsurları, özel görünüş biçimleri, muhakemesi ve yaptırımı incelenmiştir.

Çalışmanın son bölümünde TCK 244. maddesinde düzenlenen “Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme” suçunun analitik incelemesi yapılmıştır. TCK 244. maddesinde de tek bir suça yer verilmemiştir. Maddenin ilk fıkrasında bilişim sisteminin işleyişine müdahale, ikinci fıkrasında bilişim sistemindeki verilere müdahale ve dördüncü fıkrasında bilişim sistemi aracılığıyla haksız yarar sağlama suçları yaptırım altına alınmıştır. Bu suçlar da yukarıda bahsedilen sırayla çalışmamızda incelenmiştir.

ABSTRACT

The subject of our thesis is “The Crime of Entering Information System” regulated article 243 of TCK and “The Crime of System Blocking, Breaking, Data Destroying, Changing” regulated in article 244 of TCK. In the first part of our thesis, which consists of three parts, national and international regulations on information technology crimes are mentioned as well as explanations related to technical concepts and definitions in order to provide better understanding for the crimes, subject to our thesis.

In the second part of our thesis, analytical examination of “The Crime of Entering Information Technology System” regulated in TCK 243 was made. Although the title of the article is the crime of entering information technology system, two separate crimes are included in article 243 of TCK. These crimes are “The Crime of Entering Information System and/or Staying In The Information System and Monitoring The Data Transfers By Technical Means”. In our thesis, the examination of these crimes are given under different headings, and the subject, perpetrator, victim, elements, special appearance, judgement and sanction of the crimes are examined respectively.

In the last part of our thesis, an analytical examination of “The Crime of System Blocking, Breaking, Data Destroying, Changing” regulated in article 244 of TCK was made. Also article 244 of TCK is not included a single crime. In the first paragraph of the article, crime of interfering in running of information technology, in the second paragraph, crime of interfering in data in information system and in the fourth paragraph, providing unfair benefits through the information system are sanctioned. These crimes were also examined in our thesis in the order mentioned above.

TEŞEKKÜR

Yüksek lisans çalışmaların nedeniyle tarafıma “2210-A Genel Yurtiçi Yüksek Lisans Burs Programı 2020/1” kapsamında burs veren Türkiye Bilimsel ve Teknolojik Araştırma Kurumu (TÜBİTAK)’na teşekkür ederim.

