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

BİLİŞİM SİSTEMİNİ ENGELLEME, BOZMA, VERİLERİ YOK ETME VEYA DEĞİŞTİRME SUÇLARI

(TCK m.244)

Yüksek Lisans Tezi

İREM GEÇMEZ

İstanbul, 2019

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

BİLİŞİM SİSTEMİNİ ENGELLEME, BOZMA, VERİLERİ YOK ETME VEYA DEĞİŞTİRME SUÇLARI

(TCK m.244)

Yüksek Lisans Tezi

İREM GEÇMEZ

Danışman: Prof. Dr. Ahmet GÖKCEN

İstanbul, 2019

T.C.
MARMARA ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ MÜDÜRLÜĞÜ

TEZ ONAY BELGESİ

KAMU HUKUKU Anabilim Dalı KAMU HUKUKU Bilim Dalı TEZLİ YÜKSEK LİSANS öğrencisi İREM GEÇMEZ'nın BİLİŞİM SİSTEMİNİ ENGELLEME, BOZMA VERİLERİ YOK ETME VEYA DEĞİŞTİRME SUÇLARI (TCK M.244) adlı tez çalışması, Enstitümüz Yönetim Kurulunun 20.06.2019 tarih ve 2019-18/17 sayılı kararıyla oluşturulan jüri tarafından oy birliği / ~~oy çokluğu~~ ile Yüksek Lisans Tezi olarak kabul edilmiştir.

Tez Savunma Tarihi ...25.../...07.../...2019...

Öğretim Üyesi Adı Soyadı			**İmzası**
1.	Tez Danışmanı	Prof. Dr. AHMET GÖKCEN	
2.	Jüri Üyesi	Doç. Dr. MEHMET EMİN ALŞAHİN	
3.	Jüri Üyesi	Doç. Dr. ALİ EMRAH BOZBAYINDIR	

ÖZET

“Bilişim Sistemini Engelleme, Bozma, Verileri Yok Etme veya Değiştirme Suçları (TCK m.244)” başlıklı yüksek lisans çalışmamız, iki bölümden oluşmaktadır. Birinci bölümde, bilişim sistemiyle ilgili teknik kavramlar, bilgisayar, bilgisayarın unsurları, bilişim ve bilişim sistemi, bilişim sisteminin unsurları, internet ağından ve bulut bilişimden bahsedilmiştir. Bilişim hukuku, teknik kavramların sıkça kullanıldığı bir alan olduğundan, sorunlara çözüm üretmeden önce, sorunun ne olduğunun anlaşılması amacıyla öncelikle temel kavramlar tanımlanmaya çalışılmış ve günümüzde veri akışının en yoğun olduğu ağ olan internetten söz edilmiş ve internet kullanımına ilişkin birtakım istatistiksel verilere yer verilmiştir. Bu bilgilerin ardından bilişim suçu kavramından ve bu suçların genel özelliklerinden bahsedilerek, Türk Ceza Kanunu’nda düzenlenen bilişim suçları hakkında, tez konumuz ile ilişkili olduğundan genel bir bilgi verilmiştir. Ayrıca 7 Nisan 2016 tarihinde yürürlüğe giren, 6698 Sayılı Kişisel Verilerin Korunması Kanunu ile bilişim suçlarının işlenmesinde kullanılan yasak cihaz ve programlarla ilgili olarak ihdas edilen yeni suç tipi (TCK m.245/A) da bu bölümde genel olarak incelenmiştir.

İkinci bölümde tez konumuz olan bilişim sisteminin işleyişini engelleme, bozma, verileri yok etme veya değiştirme suçları madde içeriğinde üç farklı suç içerdiğinden *“bilişim sisteminin işleyişini engelleme veya bozma suçu”*, *“bilişim sistemindeki verileri bozma, yok etme, değiştirme veya erişilmez kılma, sistemde var olan verileri başka bir yere gönderme suçu*” ve *“bilişim sistemi aracılığıyla kendisinin ya da başkasının yararına haksız bir çıkar sağlama suçu”* şeklinde üç başlık altında detaylı bir şekilde incelenmiştir. İnceleme içerisinde bu düzenlemelerin uygulamadaki yansımalarını ortaya koymak amacıyla Yargıtay kararlarına da atıf yapılmıştır.

Tezin sonuç kısmında ise bütün bu inceleme ve analiz neticesinde bilişim sistemini engelleme, bozma, verileri yok etme veya değiştirme suçlarıyla hukuki anlamda daha etkili mücadele edebilmek amacıyla yapılması gereken düzenlemeler ve alınması gereken tedbirlere yönelik önerilerde bulunulmaya çalışılmıştır.

Anahtar Kelimeler : Bilgisayar, İnternet, Bilişim, Bilişim Suçu, Veri, Bilişim Sistemini Engelleme, Bilişim Sistemini Bozma, Verileri Yok Etme, Verileri Değiştirme

ABSTRACT

Our postgraduate study, which is titled Crimes of Information System Blocking, Disrupting, Data Deletion or Alteration (TPC Art.244), consists of two parts. In the first part, technical concepts of the information system, computer, computer elements, information, information system elements, internet network and cloud computing are touched upon. Since information technology law is a field where technical concepts are frequently used, before offering solutions to problems and in order to help understand what the problem is, firstly the fundamental concepts are defined, internet -which in today's world has the most data transfer traffic- is touched upon and some statistical data are presented regarding internet usage. After then, general information is provided about the concept and general features of cybercrime and cybercrimes which are regulated in Turkish Criminal Law, since it is related to our thesis subject. Furthermore, the new type of crime (TPC Art.245/A) related to forbidden devices and programs used in cybercrimes, which came to existence on April 7th 2016 through 6698 Numbered Law on the Protection of Personal Data, is analyzed in this part in general.

In the second part, since the crime of blocking, disrupting, data deletion or alteration of the functionality of information system consists of three different types of crime, they are elaborately analyzed in three parts as *"crime of blocking or disrupting the functionality of the information system",* "*crime of disrupting, deleting, altering data or rendering data inaccessible, transferring existent system data to another place"* and *"gaining unfair advantage for oneself or another person using the information system"*. In the analysis there are references made to the decisions of Court of Cassation so as to project the effect of these regulations in practical terms.

In the conclusion of this thesis, with the results from all research and analyses above, it is attempted to provide suggestions regarding regulations and precautions that need to be implemented to combat the crimes of blocking, disrupting, data deletion or alteration more effectively in the sense of law.

Keywords: Computer, Internet, Information, Cybercrime, Data, Blocking of Information System, Disrupting of Information System, Data Deletion, Data Alteration

BİLİŞİM SİSTEMİNİ ENGELLEME, BOZMA, VERİLERİ

YOK ETME VEYA DEĞİŞTİRME SUÇLARI

(TCK m.244)

İÇİNDEKİLER

Sayfa

KISALTMALAR LİSTESİ

ABD	Amerika Birleşik Devletleri
ATM	Otomatik Para Çekme Cihazı
BKM	Bankalar Arası Kart Merkezi
B	Baskı
bkz.	Bakınız
BKKKK	Banka Kartları ve Kredi Kartları Kanunu
C.	Cilt
CD.	Ceza Dairesi
CMK	Ceza Muhakemesi Kanunu
CGK	Yargıtay Ceza Genel Kurulu
çev.	Çeviren
D.	Daire
E.	Esas
E.T.	Erişim Tarihi
FBE	Fen Bilimleri Enstitüsü
IP	İnternet Protokolü
K	Karar
KANUN	Türk Ceza Kanunu
KİT	Kamu İktisadi Teşebbüsü
m.	Madde

MERSİS	Merkezi Sicil Kayıt Sistemi
R.G.	Resmi Gazete
S.	Sayı
s.	Sayfa
SBE	Sosyal Bilimler Enstitüsü
SPAM	İstenmeyen Elektronik Posta
TAKBİS	Tapu ve Kadastro Bilgi Sistemi
TBB	Türkiye Barolar Birliği
TBMM	Türkiye Büyük Millet Meclisi
TCK	5237 sayılı Yeni Türk Ceza Kanunu
TCY	Türk Ceza Yasası
TCKÖT	Türk Ceza Kanunu Ön Tasarısı
TDK	Türk Dil Kurumu
TMK	Terörle Mücadele Kanunu
TPC	Turkish Penal Code
TÜBİTAK	Türkiye Bilimsel ve Teknolojik Araştırma Kurumu
TÜİK	Türkiye İstatistik Kurumu
UYAP	Ulusal Yargı Ağı Projesi
vb.	ve benzeri
vd.	ve devamı
vs.	vesaire
VPN	Virtual Private Network (Sanal Özel Ağlar)

Y. Yıl

Yar. Yargıtay

YKD Yargıtay Kararları Dergisi

YTCK Yeni Türk Ceza Kanunu

YCGK Yargıtay Ceza Genel Kurulu

GİRİŞ

Günümüzde bilgi ve iletişim sistemlerinin yaygınlaşması bilgiye ulaşmayı kolaylaştırmış, birim zamanda yapılan işlerin hızını, verimliliğini ve bu doğrultuda bireylerin yaşam kalitesini artırmıştır. Bundan 20-30 yıl kadar önce yalnızca hayali kurulabilen teknolojik ürünler, bulut bilişim, robot teknolojisi, akıllı binalar, giyilebilir teknoloji, bitcoin (sanal para birimi) gibi kavramlar günlük hayatta duymaya alıştığımız kavramlar haline gelmiş, bilgisayar ise günden güne daha da "akıllanarak" hayatımızın vazgeçilmez bir unsuru olmuştur.

Hayatın her alanında olduğu gibi, bilişim ve teknoloji alanında da meydana gelen gelişmeler, insanların elinde iyi veya kötü olarak şekillenmektedir. Bu nedenle bu alanlarda meydana gelen gelişmeler, insan hayatında faydalı ve gerekli olmakla birlikte, sunduğu imkanların yanında yeni suç türlerinin ortaya çıkmasına neden olmuş, mevcut kanunlarımızın bilişim teknolojisindeki gelişmelerle paralel olarak yenilenememesi, kanun boşlukları ve madde metinlerindeki belirsizlikler, öngörülen cezaların caydırıcılık niteliğinden uzak olması, bu alandaki suçların diğer suçlara oranla daha kolay işlenmesi, büyük maliyetler gerektirmemesi ve işlenen suçlarda faillerin tespit edilmesinin zor olması gibi nedenlerle de bilişim alanında işlenen suç oranının günden güne artış göstermiş ve göstermeye devam etmektedir.

Ülkemizde bilişim alanındaki suçlar düzenlenirken ayrı bir kanun yapma yoluna gidilmemiş, mevcut ceza kanununa yeni hükümlerin eklenmesi yöntemi benimsenmiştir. Türk Ceza Kanununda bilişim suçları düzenlenirken, doğrudan bilişim suçları ve bilişim sistemleri aracılığıyla işlenen suçlar ayrımına yer verilmiştir. Doğrudan bilişim suçları, "Bilişim Alanında Suçlar" başlıklı onuncu bölümünde yer alan suçları kapsarken, bilişim sistemleri aracılığıyla işlenen suçlar ise klasik suçların, bu sistemlerin sağladığı kolaylıktan faydalanmak suretiyle işlenen şekillerini ifade etmektedir.

Bilişim sistemlerinin kullanımının yaygınlaşması ve bu alanda işlenen suçların hem çeşitliliğinin hem de suç işlenme oranlarının artması, bu alandaki eksikliklerin boyutunu ve yeni düzenlemelere olan ihtiyacı ortaya koymuştur. Bu sebeple çalışmamızda, bu alanda en sık işlenen suçlardan olan bilişim sisteminin işleyişini engelleme, bozma, verileri yok etme veya değiştirme suçları incelenmiştir.

"Türk Ceza Kanununda Bilişim Sistemini Engelleme, Bozma Verileri Yok Etme veya Değiştirme Suçları (TCK m. 244)" konulu çalışmamız iki ana bölüm ve sonuçtan oluşmaktadır.

Bu çalışmanın ilk bölümünde, bilişim alanının birçok teknik terim içermesi sebebiyle konunun anlaşılır kılınması için bilişim hukuku ile ilgili temel kavramlar, kısaca internetin gelişimi ve tarihi anlatılmıştır. Teknik terimlerin ardından bilişim suçu kavramı açıklanmış ve TCK'da "bilişim alanında suçlar" bölümünde yer alan ve tez konumuzla yakın ilişkili olan doğrudan bilişim suçlarına kısaca değinilmiştir.

İkinci bölümde tez konumuz değerlendirilmiş olup her suç ayrı başlık altında incelenmiş ve suçlarla ilgili Yargıtay kararlarına yer verilmiştir.

Sonuç bölümünde ise tez konusunun önemi ve bu suçların önlenmesi için yapılması gerekenler sunularak çalışma tamamlanmıştır.

Birinci Bölüm

BİLİŞİM SİSTEMİNE İLİŞKİN TEORİK ÇERÇEVE

I. BİLİŞİM SİSTEMİYLE İLGİLİ TEKNİK KAVRAMLAR

A. BİLGİSAYAR KAVRAMI

Bilişim, bilgisayar ve buna benzer aygıtlar ile bu aygıtlar arasındaki bağlantıyı kapsayan bir üst kavramdır[1]. Bu nedenle bilişim ve bilişim teknolojisi denildiğinde akla ilk gelen kavramlardan biri şüphesiz bilgisayardır[2].

Gün geçtikçe insanların öğrenmesi gereken bilgi miktarındaki artış nedeniyle bu bilgilerin toplanması ve işlenmesinde insanlara yardımcı olacak makinalara ihtiyaç duyulmuştur. Bu ihtiyacı karşılamak için de bilgisayarlar geliştirilmiştir. Bilgisayar, günlük hayatın her alanında kullanılmakla birlikte, verilerin aktarım hızı, yapılan işlemlerin doğruluğu ve uzun süre değişime uğramadan saklanabilmesi gibi sebeplerle kullanımı günden güne artmaktadır[3]. Bütün kamusal ve özel kuruluşlar da teknolojiye uyum sağlamak adına yalnızca güncel değil geçmiş zamanda oluşturulan ve klasik yöntemlerle saklanmaya çalışılan verileri de bilgisayar ortamına aktarmaya devam etmektedir[4].

Bilgisayarın hemen hemen her alanda kullanılıyor olması, bireylerin oldukça yüksek oranlarda temel bilgisayar kullanımına hâkim olması ve aktif internet kullanımın da günden

---

1 **Caner Yenidünya/Olgun Değirmenci,** Mukayeseli Hukukta ve Türk Hukukunda Bilişim Suçları**,** İstanbul, Legal Yayınevi, 2003, s.31; **Mahmut Koca/İlhan Üzülmez,** Türk Ceza Kanunu Özel Hükümler, Ankara, Seçkin Yayınevi, 2018, s.852; **Dilek Güler,** Bilişim Sistemine Girme Suçu, KTO Karatay Üniversitesi Hukuk Fakültesi Dergisi, C:3, S:2, 2018, s.15.

2 **Yavuz Erdoğan**, Türk Ceza Kanunu'nda Bilişim Suçları (Avrupa Konseyi Siber Suç Sözleşmesi ve Yargıtay Kararları İle), Legal Yayınları, 2012, s.8.

3 **Mehmet Burak Kızıltan,** 5237 Sayılı Türk Ceza Kanununda Bilişim Sistemine Girme, Sistemi Engelleme ve Bozma Suçları**,** Yayımlanmamış Yüksek Lisans Tezi, İstanbul Üniversitesi SBE, İstanbul, 2007, **s**.2. https://tez.yok.gov.tr/UlusalTezMerkezi/ (E.T: 25.11.2018).

4 **Furkan Yılmaz,** Türkiye'deki Bilişim Suçlarının Sosyolojik Bir Analizi: Tehditler ve Çözüm Stratejileri, Yayımlanmamış Yüksek Lisans Tezi, Anadolu Üniversitesi SBE, Eskişehir, 2015, s.7 https://tez.yok.gov.tr/UlusalTezMerkezi/ (E.T: 25.11.2018); **Yağmur Sönmez,** Günümüz İnternet Ortamında Bilişim Suçları ve Türkiye'deki İnternet Haber Sitelerine Yansımaları, Yayımlanmamış Yüksek Lisans Tezi, Marmara Üniversitesi SBE, İstanbul, 2018, s.25-26. https://tez.yok.gov.tr/UlusalTezMerkezi/ (E.T: 25.11.2018).

güne artması, getirdiği faydaların yanı sıra bilişim alanındaki suçlarının da artmasına neden olmuştur[5].

Geçmişten günümüze, teknolojik gelişmelerle birlikte bilgisayarın da değişime uğradığı göz önünde bulundurulduğunda, tanım yapmak riskli bir durum olsa da mevzuatta "*bilgileri otomatik işleme tabi tutan sistem*"[6] ve "*bilişim sistemi*[7]" kavramlarının yer alması sebebiyle bu kavramların kapsamının belirlenebilmesi için bilgisayarın genel bir tanımlamasının yapılması gerekmektedir[8].

İngilizce "*computing*" (hesaplama) kelimesinden türetilmiş *"computer"* yani bilgisayar kelimesi, "hesap yapmak" anlamında gelen ve Arapça kökenli bir kelime olan *"sayışmak"* kelimesinden türetilerek, Prof. Dr. Aydın KÖKSAL tarafından dilimize yerleştirilmiştir[9].

Bilgisayar teknolojisinin başlangıcı olarak kabul edilen ilk bilgisayar Amerika'da 1940'lı yıllarda 30 ton ağırlığında olan ve 180 metrekarelik alan üzerine kurulan ENIAC (Electronic Numerical Integratorand Computer) adlı bilgisayardır[10]. Ülkemizde, 1960 yılında Karayolları Genel Müdürlüğü tarafından ilk kez bilgisayar kullanılmış olup daha sonra üniversitelerde bilgisayar sistemleri kurulmuş ve 1970'li yılların sonundan itibaren bireysel ve kurumsal kullanımı yaygınlaşmıştır[11]. Günümüzde oldukça yaygın kullanımı olan ve ortalama 100-150 gr olan akıllı telefonların da bilgisayar niteliğinde olduğu düşünüldüğünde, meydana gelen gelişim ve değişimin boyutu da anlaşılmaktadır.

---

5 **Sönmez**, s.26.
6 765 Sayılı (Mülga) Türk Ceza Kanununda yer alan ifadedir.
7 5237 Sayılı Türk Ceza Kanununda yer alan ifadedir.
8 **Erdoğan,** Bilişim Suçları, s.4.
9 **Aydın Köksal**, Adı Bilgisayar Olsun, İstanbul, Cumhuriyet Yayınları, 2010, s.409 vd.
10 **Yenidünya/Değirmenci**, s.13.
11 **Müzeyyen Kadayıfçılar**, Bilgisayara Giriş, Ankara, Bil-Öm A.Ş. Yayıncılık, 1988, s.10.

Sözlükte yer alan tanıma göre bilgisayar, *"çok sayıda aritmetiksel ya da mantıksal işlemlerden oluşan bir işi, çalışması sırasında bir işletmenin işe karışması gerekmeksizin, önceden verilmiş bir izlenceye göre, özdevimli olarak yürüten bir veri işleyicidir."*[12].

Doktrinde bilgisayar çeşitli şekillerde tanımlanmış olup bunlardan bazıları şu şekildedir;

Artuk/Gökcen/Yenidünya; "*veri üretme ile veri iletişimi teknolojisini içeren, veriyi, bilgi işleme, depolama ve aktarma özelliklerine sahip bulunan cihazdır."*[13]

Akbulut; "*insanlar tarafından hazırlanıp yüklenen programlar yardımıyla bilgileri belirli bir düzende saklamak, işlenerek yeni sonuçlar üretmek, üretilen bilgileri başka yerlere iletmek, başka yerlerdeki bilgilere ulaşmak gibi amaçlarla kullanılan makinedir.*[14]"

Eralp; *"giriş birimleri ile dış dünyadan aldıkları veriler üzerinde aritmetiksel ve mantıksal işlemler yaparak işleyen ve bu işlenmiş bilgileri çıkış birimleri ile bize ileten, donanım ve yazılımdan oluşan elektronik bir makinedir.*[15]"

Kurt; *"programlara ve verilen komutlara göre işlem yapan, otomatik olarak çalışan, sıralı işlem yapan, verileri depolama, işleme tabi tutma, tasnif ve terkip etme, iletme özelliklerine sahip olan, elektronik ya da manyetik akımlarla çalışan, mantıklı sonuçlar üreten, programlanabilen, genel amaçlı kullanılabilme özelliklerine sahip elektronik cihazlardır*"[16].

Yenidünya/Değirmenci; *"dış ortamdan çeşitli yöntemlerle aldığı verileri, içeriğinde bulundurduğu programlar doğrultusunda depolayan, işleyen, bu verilerden yeni*

---

12 Türk Dil Kurumu Sözlüğü, http://tdk.gov.tr (E.T: 20.10.2018).
13 **Artuk/Gökcen/Yenidünya**, Türk Ceza Kanunu Şerhi, C:5., Ankara, Turhan Kitapevi, 2009, s.4641,4642.
14 **Berrin Akbulut,** Bilişim Alanında Suçlar, 2. Bası, Adalet Yayınevi, Ankara, 2017, s. 10,11; **Berrin Bozdoğan Akbulut**, "Bilişim Suçları", Selçuk Üniversitesi Hukuk Fakültesi Dergisi, Milenyum Armağanı, Konya, C.8, S:1-2, s.546.
15 **Özgür Eralp**, Hukukçular İçin Bilişim Terimleri Sözlüğü, Avbil Yayınları, Ankara, 2007, s.26.
16 **Kurt,** s. 31.

sonuçlar üreten, ürettiği sonuçları kullanıcıya sunan, bu suretle veri iletişimi sağlayan bir makinedir." [17].

Bilgisayar uzmanları tarafından yapılan tanımlamalardan bazıları da şunlardır;

Gültekin, "*belirli mantık düzeni içerisinde verilerin veya bilgilerin sağlanması, depolanması ve çeşitli işlemlerden geçirilerek amaca uygun halde verilmesini sağlayan makinalardır*."[18].

Kadayıfçılar; "*bilgisayar, giriş birimi ile alınan verileri yalın ya da karmaşık işlemlerden sonra çıkış birimlerinden kullanıcının gereksindiği biçimde sağlayan bir bilgi işlem aygıtıdır"*[19].

Kara; "*bir dizi işlemi ve fonksiyonu en az emek katkısı ile gerçekleştirebilmek için tasarlanmış bir araçtır"*[20].

Bu tanımlardan yola çıkılarak, bilgisayarın diğer elektronik aletlerden farkının, işlemleri belirli bir programa göre yapması yani programlanabilir olması ve verileri büyük bir hızla işleyebilmesi olduğu söylenebilecektir[21].

Bilgisayar, iki tabanlı (Binary) sayı sistemi olan (0) ile (1) rakamlarına dayanır ve bilgisayardaki bütün bu işlemler bu sayılar üzerinden gerçekleştirilir. Bellek yalnızca (0) ve (1) rakamlarını tanıdığından bilgisayar bütün bilgileri bu sayıların uygun kombinasyonuna dönüştürerek kaydeder ve yapılan işlemler sonucu elde edilen sonuçlar da yine bu ikili

---

17 **Olgun Değirmenci,** Bilişim Suçları, Yayınlanmamış Yüksek Lisans Tezi, Marmara Üniversitesi SBE, İstanbul, 2002, s.10 https://tez.yok.gov.tr/UlusalTezMerkezi/ (E.T: 25.11.2018); Yenidünya/Değirmenci, s.19.

18 **Nurbay Gültekin,** Bilgisayara Giriş Basic Programlama, Trabzon, Karadeniz Teknik Üniversitesi Yayınları, 1989, s.5.

19 **Kadayıfçılar**, s.15.

20 **Veli Kara**, Bilgisayara Giriş, Trabzon, Karadeniz Teknik Üniversitesi Yayınları, 1989 s.1.

21 **Erdoğan,** Bilişim Suçları, s.24.

sistemde elde edilir. Ancak bu şekilde verilen sonuç oldukça karışık olacağından elde edilen bilgiler harf ve rakamlara dönüştürülerek çıktı ortamına verilir[22].

Sonuç olarak bilgisayar, programlara ve komutlara göre işlem yapan, verileri işleyen ve bir düzen ve sıra içerisinde depolayan, tanımlanan ağ sayesinde bu verileri aktarabilen, hızlı, doğru ve mantıklı sonuçlar üreten ve bu işlemleri otomatik olarak yapabilen cihazlardır[23].

B. BİLGİSAYARIN UNSURLARI

Bilgisayarlar, verilen işi yapan, karmaşık devrelerden oluşan güçlü bir makine aksamı ve verilen işin insan müdahalesi olmadan nasıl yapılacağını belirleyen komut dizisi olarak iki temel unsurlardan yani donanım (hardware) ve yazılımdan (sotfware) oluşmaktadır[24]. Donanım, bilgisayarın görünen, fiziki parçalarına genel olarak verilen addır[25]. Yazılım ise fiziki olmayan ancak bilgisayarın çalışmasını sağlayan ve kodlardan oluşan bileşendir[26]. Yani bilgisayar sadece makina aksamından değil, makina ve yazılımdan oluşan bir aygıttır.

1. Donanım

Bilgisayarda gözle görülebilen, dışında ve içinde bulunan parçaların tamamına donanım (hardware) adı verilir. Başka bir deyiş ile donanım, bilgisayarda bulunan mekanik ve elektronik parçaların tamamıdır[27]. Modern bilgisayar sistemlerinin temel donanımları,

---

22 **Gültekin**, s.10; **Akbulut,** Bilişim Alanında Suçlar, s.10-11; **Yüksel Ersoy,** Genel Hukuki Koruma Çerçevesinde Bilişim Suçları, Prof. Dr. Yılmaz GÜNAY'a Armağan, Ankara Üniversitesi Siyasal Bilgiler Fakültesi Yayını, 1994, C.:49, No:3-4, s.150. http://www.politics.ankara.edu.tr/dergi/pdf/49/3/ersoyyuksel.pdf..

23 **Hüdaverdi Uçar,** 5237 Sayılı Türk Ceza Kanunu'nda Bilişim Suçları, Yayımlanmamış Yüksek Lisans Tezi, Çankaya Üniversitesi SBE, Ankara, 2014, s.3 https://tez.yok.gov.tr/UlusalTezMerkezi/ (E.T: 25.11.2018).

24 **Alp**, s.8.

25 **Dülger,** s.63.

26 **Demircan**, s.14.

27 **Cüneyt Gedikli/Gökhan Güven/Talip Torun**, Bilgisayar Teknolojileri ve İnternet, Ankara, Detay Yayıncılık, 2004, s.7.

mikro işlemci, dahili bellek, disk sürücü ve ağa bağlı diğer bilgisayarlarla veri aktarımını sağlayan diğer cihazlardan oluşur[28].

a. Mikro İşlemci

İngilizce'de Central Processor Unit (CPU) teriminin Türkçe'deki karşılığı olan mikro işlemci, ana işlemci ya da merkezi işlem birimi, giriş biriminden gelen veriler üzerinde aritmetik ve mantıksal işlemlerin denetlendiği ve işlem sonuçlarının geçici olarak saklandığı yer yani bilgisayarın beynidir[29]. Bilgisayarın çalışma hızını belirleyen temel parçalardan biri olup, çalışmasını düzenleyen ve programlardaki komutları işleyen temel ünitedir[30]. Mikro işlemci, aritmetik ve mantıksal işlemlerin yapıldığı aritmetik mantık birimi, işlemlerin istenilen şekil ve sırada yapılmasını sağlayan denetim birimi ve ana bellek biriminden oluşur[31].

b. Salt Okunur Bellek

İngilizce olan *"Rom – Read Only Memory"* terimi, Türkçe'ye "salt okunur bellek" şeklinde çevrilmiştir. Salt okunur bellek, bilgisayar üreticileri tarafından bilgisayarın çalışması için gerekli olan en temel komutların yüklendiği ve depolandığı birimdir[32]. Bu veriler salt okunur özellikte oldukları için silinmeleri, değiştirilmeleri ya da güç kesintisinden dolayı zarara uğramaları mümkün değildir[33].

c. Rastgele Erişimli Bellek

İngilizce "*RAM- Random Access Mamory"* teriminin Türkçe'deki karşılığı olan rastgele erişimli bellek; insanda beyin, makinede motor hangi görevi yapıyorsa bilgisayarda o görevi görmektedir. RAM, bilgisayar çalıştığı sürece faaliyetlerine devam eden, bilgisayara

---

28 **Mustafa Topaloğlu**, Bilişim Hukuku, Adana, Karahan Kitabevi, 2005, s.3.

29 **Kadayıfçılar**, s.18; **Yenidünya/Değirmenc**i, s.22-23; **Murat Volkan Dülger**, Bilişim Suçları ve İnternet İletişim Hukuku, Ankara, Seçkin Yayıncılık, 2017**,** s.63, Değirmenci, Bilişim Suçları, s.11.

30 **İzzet Tamer**, Bilgisayara Giriş, Ankara, SFS Grup Yayınevi, 2012 s.13.

31 **Gültekin,** 15.

32 **Fatma Burcu Nacar,** Avrupa Birliği Ülkeleri ve Türkiye'de Bilişim Suçlarının Ceza Hukukundaki Uygulamaları, Yayımlanmamış Yüksek Lisans Tezi, Atılım Üniversitesi SBE, Ankara, 2010, s.4 https://tez.yok.gov.tr/UlusalTezMerkezi/ (E.T: 25.11.2018); **Dülger**, s.63.

33 **Dülger**, s.63; **Yenidünya/Değirmenci,** s.23.

gelen gücün kesintiye uğraması halinde ihtiva ettiği bilgileri silen, erişimin ardışık olmadığı, rastgele düzenlendiği, ancak veri okuma hızının fazla olduğu bir bellektir[34]. Tıpkı bir insanın beyni gibi, bilgisayarın ihtiyacı olan her bilgi rastgele erişimli bellekte olmalıdır. Bir bilgisayarın belleği, bilgisayarın kapasitesine göre olmalıdır. Bu bellek, üzerine veriler yazılabilir, saklanabilir, değiştirilebilir ve silinebilir durumdadır[35].

d. Çevre Giriş ve Çıkış Birimleri

Bilgisayara veri girmek amacıyla kullanılan birimler giriş birimleridir[36]. Klavye, fare, DVD[37] okuyucular, mikrofon, dokunmatik yüzeyler, USB bellek aygıtları, disketler, tarayıcı gibi aygıtlar giriş birimi kapsamındadır.

Bilgisayardan elde edilen her türlü bilginin alındığı, ekran, yazıcı, ses sistemi, projeksiyon gibi aygıtlar da çıkış birimini oluşturmaktadır. Teknolojinin gelişmesi ile birlikte bilgisayarda yer alan giriş ve çıkış birimleri de gelişmekte ve değişmektedir[38].

2. Yazılım

İngilizce software teriminin Türkçe karşılığı olan yazılım, bilgisayarın soyut unsurunu oluşturmaktadır. Bilgisayarları diğer hesaplayıcı cihazlardan ayıran en önemli özellik işlem sırasını kendisinin belirlemesidir[39]. Bilgisayarlar, önceden belirlenmiş kurallara eksiksiz uyan ve programdan ayrılmayan, aynı zamanda mantıksal işlemler yapan makinalardır ve bu makina insan tarafından öngörülmeyen bir işlemi kendiliğinden

---

34 **Yenidünya/Değirmenci,** s.24, **Dülger,** s.63.

35 **Dülger,** s. 63; **Pallı,** s.12.

36 **Levent Kurt**, Tüm Yönleriyle Bilişim Suçları ve Türk Ceza Kanunundaki Uygulaması, Ankara, Seçkin Yayıncılık, 2005, s.34.

37 "DVD; Daire şeklindeki özel plastikten yapılan, üzerine lazer ışını teknolojisiyle mikroskobik çukurlar açılan ve bu sayede verilerin temel birimi olan "0" ve "1"ler yüklenebilen, sonradan bilgisayarların giriş-çıkış birimlerinden olan özel sürücü sayesinde yine lazer ışını teknolojisiyle okunabilen ve üzerine her türlü verinin işlenebildiği araçlardır." (**Dülger,** s.63).

38 **Dülger,** s.64.

39 **Uçar,** s.6**; Davut Özkul,** Bilişim Sistemi Kavramı ve Bilişim Sistemlerinin Denetimi, Sayıştay Dergisi, S:44-45, 2002, s.15.

yapabilecek bir nitelikte değildir[40]. İşte bilgisayarların bu işlevi yerine getirmesini sağlayan unsur yazılımdır.

Sözlükte yazılım, *"bir bilgisayarda donanıma hayat veren ve bilgi işlemede kullanılan programlar, yordamlar, programlama dilleri ve belgelemelerin tümü"* olarak tanımlanmıştır[41].

Bilgisayarda iki tür yazılım bulunmaktadır. Bunlar; işletim yazılımı ve uygulama yazılımıdır.

a. İşletim Yazılımı

İngilizce Operating System teriminden dilimize çevrilen işletim yazılımları, bilgisayarın çalışmasını ve en temel fonksiyonlarını yerine getirmesini sağlayan yazılımlardır[42]. Sistem yazılımı olarak da ifade edilen bu yazılımlar, bilgisayarda hangi işin nasıl bir düzen içinde ve bilgisayarın hangi özellikleri kullanılarak yapılacağını tayin eden, bilgisayarın çalışma süresi boyunca donanım özelliklerini denetleyen, yazılım özellikleriyle donanım özellikleri arasında bağlantı kuran ana kontrol programlarıdır[43].

b. Uygulama Yazılımı

Belirli bir fonksiyonu yerine getirmek veya bir problemi çözmek için yazılan ve bilgisayarda mevcut işletim sistemine uyumlu olarak çalışan ve yazı yazma, hesap işleri gibi işlemleri yapmayı sağlayan bir yazılım türüdür[44]. İşletim yazılımları, genel olarak bilgisayarın işlemesini sağlamak için çalışırken; uygulama yazılımı, kullanıcının belli bir işi yapabilmesi ve kendisi için faydalı sonuçlar elde edebilmesi için kullanılan yazılım türüdür[45]. Bu yazılımlar, bilişim verilerini oluşturmak veya işlemek gibi amaçlarla kullanılabilir[46].

---

40 **Kadayıfcılar,** s.26**; Kurt,** s.36.
41 http://www.tdk.gov.tr (E.T: 26.10.2018).
42 **Dülger,** s.64; **Değirmenci,** Bilişim Suçları, s.14.
43 **Kadayıfçılar**, s.26; **Yenidünya/Değirmenci;** s.23; **Esra Yaycı**, Bilişim Suçları, Yayımlanmamış Yüksek Lisans Tezi, Gazi Üniversitesi SBE, Ankara, s.9. https://tez.yok.gov.tr/UlusalTezMerkezi/ (E.T: 25.11.2018); **M. Tunç Demircan**, Yeni ve Eski TCK Bağlamında Bilişim Alanında Suçlar, Legal Yayınevi, İstanbul, 2016, s.15.
44 **Kurt**, s.36.
45 **Dülger,** s.65.
46 **Kurt**, s.36.

İnternetteki bilgiye ulaşmamızı, dokümanların transfer edilip görüntülenmesini sağlayan "Web Tarayıcı" uygulamalarının yazılımları verilebilecek en iyi örnektir. Eskiden uzmanlık alanlarıyla, askeri ya da ticari alanlarla ilgili yazılımlar bilişim suçlarına konu olmaktayken, günümüzde hemen her yazılım türü bilişim suçlarına konu olabilmektedir[47].

C. BİLGİSAYARLA İLGİLİ TEMEL KAVRAMLAR

1. Veri

Bilişim sistemlerinin amacı, yapıtaşı olan veriyi saklamak, işlemek ve sonuç çıkarmaktır[48]. Veri, İngilizce bir terim olan "data" kelimesinin dilimizdeki karşılığıdır. Sözlükte veri*; "olgu, kavram ya da komutların, iletişim, yorum ve işlem için elverişli biçimsel ve uzlaşımsal bir gösterimi"* şeklinde tanımlanmıştır[49]. Bir başka tanıma göre ise veri, bilgisayar tarafından iletişim, açıklama ve işlem amacıyla herhangi bir amaç, konu, durum, koşul, fikir ya da diğer unsurları açıklamak için kullanılan sayılar, harfler, simgeler belirtmek üzere kullanılan genel terimdir[50].

Sanal Ortamda İşlenen Suçlar Sözleşmesi'nin[51] "tanımlar" başlıklı birinci maddesinde "bilgisayar verisi" terimi, *"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.

---

47 **Dülger,** s.65.

48 **Yenidünya/Değirmenci, s**.47.

49 http://tdk.gov.tr/ (E.T: 25.10.2018).

50 **Özlem Meltem Kurtaran/Faruk Çubukçu,** Ansiklopedik Bilgi İşlem Terimleri Sözlüğü, İstanbul, Türkmen Kitabevi, 1991, s.177; Benzer bir tanım için bkz. **M. Zekeriya Gündüz,** Bilişim Suçlarına Yönelik IP Tabanlı Delil Tespiti, Yayımlanmamış Yüksek Lisans Tezi, Fırat Üniversitesi FBE, Elazığ, 2013**,** s.29. https://tez.yok.gov.tr/UlusalTezMerkezi/ (E.T: 25.11.2018).

51 Avrupa Konseyi tarafından 2001 yılında oluşturulan Sanal Ortamda İşlenen Suçlar Sözleşmesi, 10 Kasım 2010 tarihinde Türkiye tarafından imzalanmış ve TBMM Dışişleri Komisyonu'nun sözleşme ile ilgili raporunu 20 Aralık 2012 tarihinde sunmasının ardından 2 Mayıs 2014 tarihli 28988 sayılı Resmi Gazete'de yayınlanarak yürürlüğe girmiştir. (**Halid Özkan,** Sorularla, Açıklamalı İçtihatlı, Bilişim Hukuku Mevzuatı, Adalet Yayınları, Ankara, 2014, s.42.)

TCK'nın 243'üncü maddesinin gerekçesinde, sistem içindeki bütün soyut unsurların, fıkrada geçen veri teriminin kapsamında olacağı ifade edilmiştir.

5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanunun[52] 2/1-k maddesinde, İnternet Ortamında Yapılan Yayınların Düzenlenmesine Dair Usul ve Esaslar Hakkında Yönetmelik'in 3/1-p maddesinde ve İnternet Toplu Kullanım Sağlayıcılar Hakkındaki Yönetmelik'in 3/1-m maddesinde veri; "*bilgisayar tarafından üzerinde işlem yapılabilen her işlem yapılabilen her türlü değer"* şeklinde tanımlanmıştır.

Doktrinde veri çeşitli şekillerde tanımlanmıştır. Örneğin;

Değirmenci; "*bilgisayarda yer alan formatlanmış bilgi"*[53],

Dülger; *"bilişim sistemlerinin, üzerinde işlem yapabildiği, bu işleme dayalı sonuçlar üretebildiği, saklayabildiği, sakladıklarını sonradan tekrar okuyup işleyebildiği ve diğer bilişim sistemlerine iletebildiği her türlü bilgi*"[54],

Eralp; "*bilgisayar tarafından üzerinde işlem yapılabilen her türlü değer"*[55],

Yazıcıoğlu; *"Veri, bilgilerin belirli bir formata dönüştürülmüş hali"*[56],

Yenidünya/Değirmenci; *"bir bilişim sisteminde saklanan her şey veridir"*[57] şeklinde tanımlamıştır.

---

52 5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun, 04/05/2007 tarihinde kabul edilmiş, 23/05/2007 tarih ve 26530 sayılı Resmi Gazete'de yayımlanarak yürürlüğe girmiştir. http://www.resmigazete.gov.tr/eskiler/2007/05/20070523-1.htm (E.T: 11.06.2018).

53 **Olgun Değirmenci,** 2004 Türk Ceza Kanunu'nun Bilişim Suçları Bakımından Değerlendirilmesi, TBB Dergisi, Y:18 S:58, Mayıs-Haziran, 2005, s.200.

54 **Dülger,** s.79.

55 **Eralp**, s.139.

56 **Yılmaz Yazıcıoğlu**, Bilgisayar Suçları, Kriminolojik, Sosyolojik ve Hukuki Boyutları İle, İstanbul, Alfa Yayınları, 1997, s.29.

57 **Yenidünya/Değirmenci,** s.47-48.

Bilgisayarın var olma amacı üzerine yüklü bulunan verilerdir; bu nedenle veriler ceza hukuku açısından da suçun konusunu oluşturması yönünden önemlidir[58].

2. Program

Bilgisayarların belirli bir amaca ulaşabilmeleri için hazırlanan komutlar dizisine program denir[59]. Bir başka tanıma göre ise program, bir bilgisayarın istenilen şekilde çalışmasına yardımcı olmak, kullanıcı ile bilgisayar arasında köprü vazifesi görmek, bilgisayarın fiziksel çalışmasının kullanıcı tarafından denetlenmesine ve istenilen şekilde çalışmasına olanak vermek ve bilgisayarın çalışmasının sonuçlarından kullanıcının faydalanmasını sağlamak üzere sistematik olarak bir araya getirilmiş olan veri dizileridir[60].

D. BİLİŞİM VE BİLİŞİM SİSTEMİ

Bilgisayar kavramı gibi, Prof. Dr. Aydın Köksal tarafından "informatic" kelimesinin karşılığı olarak dilimize kazandırılan bir diğer kavram olan bilişim[61], bilginin elektronik olarak işlenip, yüksek hızlı veri, ses ve görüntü taşıyan iletişim hatları aracılığıyla aktarılmasını ifade eder[62] .

Sözlükte bilişim; *"Bilgi olgusunu, bilgi saklama, erişim dizgeleri, bilginin işlenmesi, aktarılması ve kullanılması yöntemlerini, toplum ve insanlık yararı gözeterek inceleyen uygulamalı bilim"* olarak tanımlanmakla birlikte *"bilgisayar da içeride olmak üzere, bilişim ve bilgi erişim dizgelerinde kullanılan türlü araçların tasarlanması, geliştirilmesi ve üretilmesiyle ilgili konuları da kapsadığı"* ifade edilmiştir[63].

Doktrinde bilişim çeşitli şekillerde tanımlanmıştır. Bunlardan bazıları şu şekildedir;

---

58 **Dülger,** s.79; **İsmail Ergün,** Siber Suçların Cezalandırılması ve Türkiye'de Durum, Ankara, Adalet Yayınevi, 2008, s.6.
59 **Gültekin,** s.12.
60 **Yazıcıoğlu, s.**.30,31.
61 **Aydın Köksal**, Bilişim Terimleri Sözlüğü, Ankara, Türk Dil Kurumu Yayınları, 1981, s.28; **Köksal**, Adı Bilgisayar Olsun, s. 408.
62 **Kurtaran/Çubukçu**, s.35.
63 http://www.tdk.gov.tr (E.T: 26.10.2018).

Artuk/Gökcen/Yenidünya; *"insanların teknik, ekonomik, sosyal, kültürel, hukuksal veya benzeri alanlarda sahip oldukları verinin saklanması, saklanan bu verinin elektronik olarak işlenmesi, organize edilmesi, değerlendirilmesi ve yüksek hızlı ses veya görüntü taşıyan iletişim araçları ile aktarılmasıdır"*[64].

Aydın; "*bilginin iletişim yapısı ve özellikleri; bilginin aktarılması, organize edilmesi, saklanması, tekrar elde edilmesi, değerlendirilmesi ve dağıtımı için gerekli kuram ve yöntemlerdir*[65]*",*

Akbulut; "*insanların teknik, ekonomik ve toplumsal alanlardaki iletişimde kullandığı ve bilimin temeli olan bilginin elektronik araçlarla özellikle bilgisayarlar aracılığıyla işlenip, ses, görüntü ve veri taşıyan iletişim hatları aracılığıyla aktarılması bilimidir*[66]*",*

Dülger; *"insanların teknik ekonomik siyasal ve toplumsal alanlardaki iletişiminde kullandığı bilginin, özellikle bilgisayar aracılığıyla düzenli ve akılcı biçimde işlenmesi, her türden düşünsel sürecin yapay olarak yeniden üretilmesi, bilginin bilgisayarda depolanması ve kullanıcıların erişime açık bulundurulması bilimidir."*[67]**,**

Ergün; *"insanoğlunun teknik, ekonomik ve toplumsal alanlardaki iletişiminde kullandığı ve bilimin dayanağı olan bilginin, özellikler elektronik makineler aracılığıyla düzenli ve rasyonel biçimde işlenmesi bilimidir*"[68]**,**

Yazıcıoğlu; *"bilginin elektronik olarak işlenip, yüksek hızla veri, ses ve görüntü kaydı taşıyan iletişim hatları aracılığıyla aktarma faaliyetlerinin gerçekleştiği alandır"*[69]

---

64 **Artuk/Gökcen/Yenidünya,** Türk Ceza Kanunu Şerhi, s.4643.
65 **Emin Doğan Aydın**, Bilişim Suçları ve Hukukuna Giriş, Ankara, Doruk Yayınları, 1992, s.3.
66 **Berrin Bozdoğan Akbulut**, Bilişim Suçları, Kemal Oğuzman'a Armağan, İstanbul, Galatasaray Üniversitesi Yayınları, 2004, s.46-47.
67 **Dülge**r, s.70.
68 **Ergün,** s. 10.
69 **Yazıcıoğlu,** s.131.

Yargıtay Ceza Genel Kurulunun (YCGK) 19 Haziran 2007 tarihli vermiş olduğu E. 2007/6-36 K. 2007/150 sayılı kararda bilişim kavramının "*bilginin otomasyona tabi tutulması sonucunda işlenmesini, başka deyişle, verinin saklanması, organize edilmesi, değerlendirilmesi, nakledilmesi, çoğaltılmasını*" ifade ettiği belirtmiştir[70].

Bilişim sistemlerinin en yaygın unsuru verilerin saklanması, işlenmesi ve aktarılmasını sağlaması bakımından bilgisayarlardır[71]. Ancak bilgisayarlar dışında da, bilişim sistemi olarak nitelendirilebilecek aygıtlar mevcuttur[72].

Bilişim kavramı, mevzuatımızda ilk kez 1989 tarihli Türk Ceza Kanunu Ön tasarısının 342'inci maddesinin gerekçesinde "*bilişim alanı*" olarak yer almış ve bu kavram da "*bilgileri toplayıp depo ettikten sonra bunları otomatik işleme tabi tutan sistemlerden oluşan alan*" olarak tanımlanmış ancak 765 Sayılı TCK'da yer almamıştır. Bu tanım 14.06.1991 tarihli Türk Ceza Kanununda Değişiklik Yapılmasına Dair Kanun'un gerekçesinde de yer almaktadır. Yine Adalet Bakanlığı tarafından hazırlanan 1997 tarihli Türk Ceza Kanunu Ön Tasarısı'nda bilişim alanı, "*verileri toplayıp, yerleştirdikten sonra bunları otomatik işlemlere tabi tutma imkânı veren manyetik sistemler*" olarak tanımlanmıştır[73].

2000 tarihli Türk Ceza Kanunu Ön Tasarısının 345'inci maddesinin gerekçesinde yine bilişim alanı kavramına yer verilmiş olup bu kavram, "*verileri toplayıp yerleştirdikten sonra bunları otomatik olarak işleme tabi tutma olanağı veren manyetik sistemlerden oluşan*

---

70 **Yargıtay Ceza Genel Kurulu,** 19.06.2007 tarihli ve 2007/6-136 E., 2007/150 K. sayılı kararı www.kazanci.com (E.T:20.09.2018) Yine aynı kararın devamında, *"Bilgisayar, (kompütür, elektronik beyin) aritmetik ve mantık işlemi dizileriyle oluşturulmuş programlara göre verileri (bilgileri) otomatik işleme tabi tutan sistemlere verilen ortak isim iken, bilişim (enformatik) ise, bilgisayardan da faydalanılmak suretiyle bilginin saklanması, iletilmesi ve işlenerek kullanılır hale gelmesine konu olan akademik ve mesleki disipline verilen addır; yani başka bir deyişle, bilgisayar kullanma ilmidir."* denilerek bilişim kavramının bilgisayarı da kapsayan bir üst kavram olduğu ortaya konulmuştur.

71 **Erdoğan,** Bilişim Suçları, s.16.

72 **Yenidünya**, s.1030; **Seher Ergüç,** Türk Bankacılık Sisteminde İnternet Bankacılığı İle Yapılan Dolandırıcılıklar ve Bilişim Suçları Hukuku, Yayımlanmamış Yüksek Lisans Tezi, Kadir Has Üniversitesi SBE, İstanbul, 2008, s.59 https://tez.yok.gov.tr/UlusalTezMerkezi/ (E.T: 25.11.2018).

73 **Yenidünya /Değirmenci**, s.28; **Bahaddin Alaca,** Ülkemizde Bilişim Suçları ve İnternetin Suça Etkisi (Antropolojik ve Hukuki Boyutları ile), Ankara Üniversitesi SBE, Yayımlanmamış Yüksek Lisans Tezi, Ankara, 2008, s.3. https://tez.yok.gov.tr/UlusalTezMerkezi/ (E.T: 25.11.2018).

alan" olarak tanımlanmıştır[74]. 2003 tarihli Türk Ceza Kanunu Öntasarı metninde ise bilişim alanı kavramı kaldırılmış, onun yerine "bilişim sistemleri" kavramı getirilmiştir. Bu kavram da tasarı metninde, *"verileri toplayıp yerleştirdikten sonra bunları otomatik olarak işleme tabi tutma olanağı veren manyetik sistemler"* olarak tanımlanmıştır[75]. Bu tanımlama kabul edilmiş ve 5237 Sayılı TCK'nın 243'üncü maddesinin gerekçesinde de aynı şekilde yer almıştır. Bilişim sistemi tabirindeki "sistem" ile verilerin depolanmasını, işlenmesini, kullanılmasını ve nakledilmesini sağlayan çeşitli cihazlar ve olguların bütünü ifade edilmektedir[76].

Akarslan'ın ifadesine göre bilişim sistemi, "*bilgi veya veriyi alan, bunları işleme tabi tutan, sonuçları çıktı şeklinde verebilen elektronik makinelerdir*"[77].

Artuk/Gökcen/Yenidünya bilişim sistemini "*veri-işlem ve veri iletişim unsurlarını taşıyan araçların bütünü*" şeklinde tanımlamış olup madde gerekçesinde yer alan tanımlamanın bilgisayara yönelik olduğunu ancak bilgisayarların da manyetik olma özelliğinin bulunmadığını ifade etmiştir[78].

Eralp; "*bilgisayar, çevre birimleri, iletişim altyapısı ve yazılımlardan oluşan veri işleme, saklama, iletmeye yönelik sistemdir*." şeklinde tanımlamıştır.[79]

Özbek/Doğan/Bacaksız/Tepe'ye göre ise bilişim sistemi; "*verilerin saklanması, organize edilmesi, değerlendirilmesi, nakledilmesi, çoğaltılması gibi fonksiyonları otomatik olarak gerçekleştiren sistemlerdir.*"[80].

---

74 2000 tarihli Türk Ceza Kanunu Ön Tasarısı, **Adalet Bakanlığı Tarafından Basılan Yayınlanmamış Metin**, s. 335 Aktaran; Kurt, s.25.

75 2003 tarihli Türk Ceza Kanunu Ön Tasarısı, TBMM Tarafından Basılan Yayınlanmamış Metin, s.179 Aktaran; **Kurt,** s.25.

76 **Yazıcıoğlu**, s.224.

77 **Hüseyin Akarslan**, Bilişim Suçları, 2. Baskı, Ankara, Seçkin Yayıncılık, 2015, s.29.

78 **Artuk/ Gökcen /Yenidünya**, Türk Ceza Kanunu Şerhi, s. 4643.

79 **Eralp,**. 33.

80 **Veli Özer Özbek/Koray Doğan/Pınar Bacaksız/İlker Tepe,** Türk Ceza Hukuku Özel Hükümler, Ankara, Seçkin Yayıncılık, 2017, s. 947.

Yenidünya ise; "*veri-işlem ve veri-iletişim unsurlarını taşıyan araçların bütününe, bilişim sistemi denilmektedir*" şeklinde ifade etmiştir[81].

Tanımlamalardan yola çıkıldığında alan ve sistem kavramları arasında bir anlam farkı bulunmamaktadır. Nitekim Malkoç[82] da bilişim sistemini tanımlarken, "*…bir başka ifade ile bilişim alanı…*" diyerek kavramların birbiri yerine kullanıldığını ifade etmektedir.

Sanal Ortamda İşlenen Suçlar Sözleşmesi'nde "*Terimlerin Kullanımı*" başlıklı birinci bölümde, bilişim sistemi kavramı yer almamaklar birlikte bilgisayar sistemi kavramı tanımlanmıştır. Buna göre; "*bilgisayar sistemi terimi bir veya birden fazlası, bir program uyarınca otomatik olarak veri işleyen herhangi bir cihaz veya birbiriyle bağlantılı veya ilgili bir grup cihazı ifade eder*". Ulusal mevzuatta ise bilişim sistemi, Ceza Muhakemesinde Ses ve Görüntü Bilişim Sisteminin Kullanılması Hakkında Yönetmelik'in 3/1-b maddesinde "*bilgisayar, çevre birimleri, iletişim altyapısı ve programlardan oluşan veri işleme, saklama ve iletmeye yönelik sistemi*" şeklinde tanımlanmıştır[83].

Bilişim kavramına ilişkin açıklamalarımızda da ifade ettiğimiz üzere, bilişim suçları yalnızca bilgisayarlarla işlenmediğinden TCK'da yer alan "*bilişim sistemi*" terimi daha yerindedir[84]. Kaldı ki şu an akıllı telefon, akıllı bileklik, akıllı saat gibi giyilebilir teknoloji ürünleri dahi veri işleme, saklama ve iletme fonksiyonlarına sahip olup bir bilişim sistemidir.

E. BİLİŞİM SİSTEM AĞLARI VE İNTERNET

Modern bilgisayarların ilk dönemlerinde bilgisayarlar arası veri aktarımları disketlere kopyalanmak suretiyle gerçekleştirilmekteydi[85]. Ancak zamanla hem depolanan

---

81 **Yenidünya,** s.1029.

82 **İsmail Malkoç,** Açıklamalı-İçtihatlı Yeni Türk Ceza Kanunu, Ankara, Yetkin Yayıncılık, 2013, s.3802.

83 Bu Yönetmelik, 4/12/2004 tarihli ve 5271 sayılı Ceza Muhakemesi Kanunu, 3/7/2005 tarihli ve 5395 sayılı Çocuk Koruma Kanunu ve 27/12/2007 tarihli ve 5726 sayılı Tanık Koruma Kanununa dayanılarak hazırlanmış ve 20.09.2011 tarihinde yayımlanarak yürürlüğe girmiştir.

84 Benzer görüşler için bkz. **Erdoğan,** Bilişim Suçları, **s.**12; **Berrin Akbulut,** Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme, Selçuk Üniversitesi Hukuk Fakültesi Dergisi, C:24, S:2, 2016, s.26.

85 **Özkul,** s.16.

veriler ve bilgisayar kullanımı hem de veri aktarım ihtiyacı artmıştır[86]. Bu sebeple bilgisayarlar arasında iletişim kurulmaya çalışılmıştır. İşte bu ihtiyaç doğrultusunda oluşturulan, bilgisayarların birbirleri ile iletişim kurmasını sağlayan fiziki ortam ve bu aktarım için gerekli donanım "*ağ*" (network) kavramı ile ifade edilmiştir[87].

Sözlükte ağ, *"En az bir bilgisayar ile çoğullayıcı, anahtar veya yönlendirici cihazların kullanımı ile oluşturulan veri iletim yapısı"* olarak tanımlanmıştır[88]. Bilişim sistem ağları, kullanım şekillerine göre başlıca *"iç ağ (intranet)"*[89], *"gelişmiş intranet (ekstranet)"*[90], *"sanal özel ağlar (VPN)"*[91] ve *"internet" olarak ayrılmaktadır.* Ancak günümüzde en yaygın kullanılan ağ, internettir.

Bilgisayarlar arası iletişim önce kısa mesafedeki bilgisayarlar arasında kablolar aracılığıyla kurulan ağ sayesinde gerçekleştirilmiş ve daha sonra modemler aracılığıyla daha uzak mesafelerdeki bilgisayarların birbirlerine bağlanması sağlanmıştır[92]. İnternet ise dünya

---

86 **Yenidünya/Değirmenci,** s.35; **Necmi Murat Güngör,** Yeni Türk Ceza Kanunu Kapsamında Bilişim Suçları ve Emniyet Genel Müdürlüğü Uygulamaları, Yayımlanmamış Yüksek Lisans Tezi, İstanbul Üniversitesi SBE, İstanbul, 2007, s.32. https://tez.yok.gov.tr/UlusalTezMerkezi/ (E.T: 25.11.2018).

87 **Yenidünya/Değirmenci**, s.35; **A. Caner Yenidünya,** Bilişim Sistemine Hukuka Aykırı Erişim Suçu, Legal Fikri ve Sınai Haklar Dergisi, C:1 S:4 Y:2005, s.1030.

88 http://tdk.gov.tr/ (E.T: 01.11.2018).

89 İntranet, işyerlerinde çalışanlar arası iletişimi sağlamak ve bilgi paylaşmak amacıyla kullanılan özel bir iş ağıdır. Esas olarak, işyerinin kendi özel Web sitesidir; İnternet ile aynı network protokollerini ve aynı altyapıyı kullanır. Yetkisiz kullanıcılardan bir firewall (güvenlik duvarı) ile korunur. Bu güvenlik tedbiri sayesinde çift yönde iletişim trafiği kontrol edilir ve iç ağın korunması sağlanır.
http://bidb.itu.edu.tr/seyir-defteri/blog/2013/09/07/intranet-(i%C3%A7-a%C4%9F)-ve-extranet-(d%C4%B1%C5%9F-a%C4%9F) (E.T: 10.12.2018).
İntranet kullanarak aynı kurum içinde e-mail gönderilebileceği gibi, internet web sayfalarına da ulaşılabilir ve kurum içi çalışanlar satış bilgileri, işveren talimatları, insan kaynakları bilgilerini ve diğer veri tabanlarını birbirleriyle paylaşabilirler. bkz. **Topaloğlu**, s.93.

90 Ekstranet, internet tabanlı ancak sadece izin verilen kişilerin girebildiği ve kullanıcılar açısından güvenli erişim sağlayan bir sistemdir. Erişim genellikle kullanıcı adı ve şifre ile gerçekleşir. Bu sistemde müşteriler, bayiler, alıcı ve satıcılar aynı ortamdadır. Yani eksranet, şirket dışı unsurlarla da etkileşimi olan bir şirket intraneti olarak da tanımlanabilir."
http://www.idc-online.com/technical_references/pdfs/data_communications/Internet_Intranet_and_Extranet.pdf (E.T: 10.12.2018).

91 Sanal özel ağlar, firmaların şubeleri ve iş ortakları ile aralarında veri iletişimini güvenilir, kolay ve ekonomik biçimde sağlamasına olanak veren bir tünelleme teknolojisidir. Kurumların yerel ağlarını internet ortamı üzerine taşınmasını sağlar. VPN teknolojisinde, noktalar arası ekonomik ve güvenilir bağlantılar kurulurken iletişim maliyetini minimum seviyede tutabilmek için internet ortamını "iletişim omurgası" olarak kullanılır. VPN'lerde kullanılan ağ kamuya açık bir ağdır, ancak ileti bir noktadan diğer noktaya kadar özel bir tünel aracılığı ile şifrelenerek ulaşır. **Arif Yıldız/ M. Ali Akdeniz**, **"**Vpn (Sanal Özel Ağlar)**"**
http://www.hasanbalik.com/projeler/bitirme/32.pdf (E.T: 10.12.2018).

92 **Güngör,** s.33.

üzerindeki tüm bilişim ağlarını ve bilgisayarları birbirleri ile bağlantılandırarak belli esaslar dahilinde, kendine özgü bir dille iletişimini sağlamıştır[93]. Yani internet, bilgisayarlar arası haberleşme ağıdır[94].

Soğuk savaş döneminde Sovyetler Birliği'nin Sputnik uydusunu uzaya göndermesinden sonra Amerikan Hükümeti, olası bir nükleer atak halinde dahi bilgisayarlar arasında iletişimin ve bilgi aktarımının sağlanacağı bir ağ üzerinde çalışmalara başlamış,[95] bu çalışmalar sonucunda 1969 yılında internet olarak bilinen ARPANET (Advanced Research Projects Agency Network) adlı bir askeri bilgisayar ağı oluşturulmuştur[96]. Zamanla birbirine bağlanan bilgisayarların aynı özellikle olmaması nedeniyle bilgisayarlar arasındaki iletişimin daha kolay sağlanması için çeşitli protokoller geliştirilmiş olup bunlardan en yaygını TCP/IP protokolleridir. İnsanın, bilgiyi saklama, paylaşma ve ona kolayca ulaşma arzusu ve gereksiniminden ortaya çıkan internet, birçok bilgisayar sistemini TCP/IP protokolüyle birbirine bağlayan ve hızla büyüyen küresel bir iletişim ağıdır[97].

Yenidünya/Değirmenci TCP/IP protokolünü *"dört katmanlı (uygulama katmanı, ulaşım katmanı, yönlendirme katmanı ve fiziksel katman) bir yapıya sahip olan internet ağ mimarisinin protokol kümelerine verilen ad"* olarak tanımlamaktadır[98]. Bu protokoller, internet ağındaki veri iletişiminin kurallarını belirler ve bilgi aktarımı bu kurallar dahilinde yapılır. "TCP" iletim kontrol protokolü, "IP" internet protokolü anlamına gelir[99].

1986 yılında Amerikan Ulusal Araştırma Kurumu tarafından NFSNET kurulmuş, 1989 yılında World Wide Web teknolojisi, 1990 yılında da dosya transfer protokolü HTTP

---

93 **Yenidünya/ Değirmenci,** s.36; **Dülger,** s.82; **Ahmet Ünal,** Bilişim Suç Türlerinden Biri Olan Dağıtık Servis Dışı Bırakma Saldırılarının Önlenmesindeki Hukuki ve Teknik Zorluklar, Yayımlanmamış Yüksek Lisans Tezi, İstanbul Bilgi Üniversitesi SBE, İstanbul, 2014, s.3. https://tez.yok.gov.tr/UlusalTezMerkezi/ (E.T: 25.11.2018).

94 **Bülent Sözer**, Elektronik Sözleşmeler, İstanbul, Beta Basım Yayın, 2002, s.7; **Servet Yetim,** Bilişim Suçları ve Etkin Mücadele Yöntemleri, Terazi Hukuk Dergisi, C:9, S:95, 2014, s.80..

95 http://www.usg.edu/galileo/skills/unit07/internet07_02.phtml (A Brief History Of the Internet) (E.T: 03.11.2018).

96 http://www.internetsociety.org/internet/what-internet/history-internet/brief-history-internet (A Brief History Of The Internet) (E.T: 03.11.2018).

97 **Hüseyin Koçak / Ali Nazmi Dandin**, Toplumsal ve Yönetsel Alanda Bilişim Teknolojilerinin Kriminal Etkileri, Afyon Kocatepe Üniversitesi Sosyal Bilimler Dergisi, 2017, C:19, S:1, s.139; **Artun Avcı,** Türkiye'de İnternet ve İfade Özgürlüğü, Legal Yayıncılık, İstanbul, 2013, s.29.

98 **Yenidünya/ Değirmenci**, s. 39. **Hasan Sınar,** İnternet ve Ceza Hukuku, Beta Yayınları, 2001, s.24.

99 **Yenidünya/Değirmenci,** s. 40,41**; Dülger**, s.80; **Akbulut,** Bilişim Alanında Suçlar, s.13.

geliştirilmiş ve internetin bireysel kullanımı yaygınlaştırılmıştır. Türkiye internete 1993 yılının nisan ayından beri bağlı olup ilk bağlantı Türkiye Bilimsel Araştırma Kurumu (TÜBİTAK) destekli bir proje ile Orta Doğu Teknik Üniversitesi (ODTÜ)'den gerçekleştirilmiştir. Daha sonra 1994 yılında Ege Üniversitesi'nde, 1995 yılında Bilkent Üniversitesi'nde ve Boğaziçi Üniversitesi'nde, 1996 yılında ise İstanbul Teknik Üniversitesi (İTÜ)'de bağlantılar gerçekleştirilmiştir.[100]

İnternet, yüzyılımızın en önemli iletişim aracıdır. Ülkemiz de bu aracı en yoğun şekilde kullanan ülkelerden biridir. 30 Kasım 2018 itibariyle Avrupa ülkeleri arasında internet kullanım oranı bakımından beşinci sıradadır[101]. Türkiye İstatistik Kurumu tarafından, bireylerin 2018 yılında bilgisayar ve internet kullanım oranına ilişkin olarak yapmış olduğu çalışmada bilgisayar kullanım oranının 2004 yılında %23 iken 2018 yılında %59.6 ya internet kullanım oranının ise %18.8 iken %72.9'a yükseldiği ifade edilmiştir[102]. Yani internet ve bilgisayar kullanım oranları geçen bu süreçte iki katından daha fazla bir artış göstermiştir ve göstermeye devam etmektedir. 2017 yılında toplam nüfusun %80,7'sinin internete erişme imkanı bulunmaktadır. E-dönüşüm Türkiye projesinin başlaması ile birlikte kamu ile bireyler arasındaki iletişimde de internet kullanım oranı özellikle son yıllarda önemli oranda artış göstermektedir[103]. Bu durum hem daha fazla kişinin daha çok bilgiye kısa sürede ulaşmasını sağlamış hem de bilişim suçlarının da internetin kullanım oranıyla paralel artış göstermesini sağlamıştır. Çünkü internet yalnızca bilgisayarlar arası bağlantı kurmamış aynı zamanda fail ile mağdur arasında da bir bağlantı kurulmasını sağlayarak suçun kolay işlenebileceği bir alan oluşturmuştur[104].

---

100 **Burak Tunç Bilek**, Bilişim Suçları ve Üniversite Lisans Öğrencilerinin Bilişim Suçlarına Yönelik Görüşleri Yüksek Lisans Tez**i,** Ankara: Gazi Üniversitesi, 2012 https://tez.yok.gov.tr/UlusalTezMerkezi/ , s.10 (03.11.2018).

101 Internet Top 10 Countries in Europe, http://www.internetworldstats.com/ (E.T. 04.11.2018).

102 Türkiye İstatistik Kurumu, Hanehalkı Bilişim Teknolojileri Kullanım Araştırması, 2016. http://www.tuik.gov.tr/PreHaberBultenleri.do?id=21779 (E.T: 04.11.2018).

103 Bu artışın en önemli sebeplerinden biri olan "e-Dönüşüm Türkiye" projesine ilişkin detaylı bilgiye, çalışmanın ikinci bölümünde yer alan "Bilişim Sistemini Engelleme veya Bozma" suçuna ilişkin değerlendirmede yer verilmiştir.

104 **Sınar,** s.78; **Çetin Gümüş,** Bilişim Suçlarıyla Mücadelede Polisin Eğitimi, Yayımlanmamış Doktora Tezi, Fırat Üniversitesi SBE, Elazığ, 2008, s.38 https://tez.yok.gov.tr/UlusalTezMerkezi/ (E.T: 25.11.2018).

F. BULUT BİLİŞİM

Özellikle mobil iletişim platform ve ortamlarındaki gelişmeler, iş dünyasının çok dinamik bir yapıda olması ve sürat gerektirmesi, devletlerin ve ticari girişimcilerin bilişim teknolojilerine yaptıkları yatırımların artması gibi nedenler bulut bilişim kavramını ve teknolojilerini doğurmuştur[105]. Bulut bilişim, kullanılan bilişim aygıtları arasında bir platform üzerinden bilgi paylaşımını yüksek hızla sağlayan hizmetlerdir[106]. Sunucular üzerinde depolanan ve istemciler tarafından talep edilen işleme tabi tutulan veriler, ihtiyaç duyulduğu anda, internet üzerinden aktarılır[107]. Hemen hemen her gün sıklıkla kullandığımız iCloud, Dropbox, Google Drive, Gmail, Hotmail gibi ağlar bulut bilişim teknolojisinden faydalanmaktadır. Bulut bilişim sayesinde, istenilen bilgiye her yerden ve her türlü bilgi iletişim cihazı kullanarak ulaşmak mümkün olabilmektedir[108].

İngilizce *"cloud computing"* teriminin Türkçe'deki karşılığı olan bulut bilişim hakkında çeşitli tanımlar bulunmaktadır. Türk Standartları Enstitüsü'nce hazırlanan Bulut Bilişim Güvenlik ve Kullanım Standardı taslağına göre bulut bilişim;

> *"İşlemci gücü ve depolama alanı gibi bilişim kaynaklarının ihtiyaç duyulan anda, ihtiyaç duyulduğu kadar kullanılması esasına dayanan, uygulamalar ile altyapının birbirinden bağımsız olduğu ve veriye izin verilen her yerden kontrollü erişimin mümkün olduğu, gerektiğinde kapasitenin hızlı bir şekilde arttırılıp azaltılabildiği, kaynakların kullanımının kolaylıkla kontrol altında tutulabildiği ve raporlanabildiği bir bilişim türüdür"*[109].

---

105 **Adem Emekçi/Emin Kuğu/Murtaza Temiztürk**, Adli Bilişim Ezberlerini Bozan Bir Düzlem: Bulut Bilişim, Uluslararası Bilgi Güvenliği Mühendisliği Dergisi, C:2, S:1, 2016, s.9; **Arzu Öz**, Bulut Bilişim Veri Güvenliği, Yayımlanmamış Yüksek Lisans Tezi, Gazi Üniversitesi Bilişim Enstitüsü, Ankara, 2013, s.1 https://tez.yok.gov.tr/UlusalTezMerkezi/ (E.T:10.07.2019).

106 **Kutay Batı,** Bulut Bilişim ve Etkileri, Yayımlanmamış Yüksek Lisans Tezi, Dokuz Eylül Üniversitesi SBE, İzmir, 2015, s.3 https://tez.yok.gov.tr/UlusalTezMerkezi/ (E.T: 25.11.2018); **Murat Topaloğlu/Harun Özkişi/Egemen Tekkanat,** Bulut Bilişim, Seçkin Yayınları, Ankara, 2017, s.19.

107 **Hakan Kılıç,** Kamuda Bulut Bilişim Kullanımına Yönelik Risk Analiz ve Yönetimi, Yayımlanmamış Uzmanlık Tezi, T.C. Çevre ve Şehircilik Bakanlığı, Ankara, 2017, s.1.< (E.T: 27.06.2019).

108 **Türkay Henkoğlu/Özgür Külcü,** Bilgi Erişim Platformu Olarak Bulut Bilişim: Riskler ve Hukuksal Koşullar Üzerine Bir İnceleme, Bilgi Dünyası Dergisi, Y:14, S:1, 2013, s.64.

109 Türk Standartları Enstitüsü'nce hazırlanan Bulut Bilişim Güvenlik ve Kullanım Standardı Taslağı, https://statik.tse.org.tr/upload//tr/dosya/icerikyonetimi/1202/17032015093613-3.pdf (E.T: 26.06.2019).

Amerikan Ticaret Bakanlığı'na bağlı Ulusal Standartlar ve Teknoloji Enstitüsü tarafından ise "*minimum yönetim çabası ve hizmet sağlayıcısı desteği ile yayımlanabilecek ortak havuzlara ve konfigüre edilebilir kaynaklara (örneğin ağlar, sunucular, veri depoları, uygulamalar ve hizmetler) anında erişim sağlayan model"* olarak tanımlanmaktadır[110].

Bulut bilişim sisteminin üç temel bileşeni bulunmaktadır. Bunlar; kullanıcı, servis sağlayıcı ve servis geliştiricidir. Kullanıcı, servis sağlayıcılar tarafından sağlanan platform, yazılım veya altyapı sistemlerini kullanan tüzel veya gerçek kişidir[111]. Servis sağlayıcı, sunulacak hizmetleri tüketiciye ulaştırmakla yükümlü olan ve kaynakları birden fazla kullanıcıya farklı kiralama yöntemleri kullanarak sağlayan taraftır[112]. Servis geliştirici ise sağlayıcının sunduğu temel servisleri geliştiren ya da yeni uygulama veya servisler oluşturan taraftır[113].

Bulut bilişim hizmetleri genel olarak ücret karşılığında verilmektedir. Ancak belirli birtakım sınırlamalarla (kota, süre gibi) ücretsiz olarak da kullanılması mümkün olabilmektedir. Ücretsiz olarak sunulan bulut bilişim hizmetlerinden yararlanmak için dijital ortamda hizmet sözleşmesinin onaylanması dışında yazı bir sözleşme yapılması gerekmez[114]. Ancak, kurumsal olarak ve ücret karşılığı yararlanılan bulut bilişim hizmetlerinde sözleşme büyük önem taşımaktadır[115]. Bu hizmetler ile ilgili olarak çeşitli ihlaller ya da başka sorunlarda, kullanıcı ile hizmet sağlayıcının sorumluluğu yapılan sözleşme ile belirlenmektedir. Bu sözleşmelerde hizmet sağlayıcısının ne tür hizmet sunacağı, hizmeti nasıl sağlayacağı ve hizmetin yürütülmesinden, tamamlanmasından, olası hatalardan ve gizlilik ihlallerinden kimin nasıl sorumlu olacağı belirlenmelidir. Verilerin kişisel veri olması

---

110 https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf (E.T: 26.06.2019)
111 **Öz,** s.12; **Batı,** s.9; **Albayrak**, s.53.
112 **Öz,** s.13; **Batı,** s.10; **Albayrak**, s.53.
113 **Albayrak**, s.53; Öz, s.13.
114 **Turan**, s.107.
115 **Kutan Koruyan/F. Itır Bingöl**, Bulut Bilişim Hizmet Sağlayıcılarının Veriyi Koruyamama Durumuyla İlgili Türk, Avrupa Birliği ve Amerikan Hukukundaki Düzenlemeler, Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, C:17, S:3 Y:2015 s.381. (367-388)

durumunda bu sözleşmelerin Kişisel Verilerin Korunması Kanununa aykırılık teşkil etmeyecek şekilde düzenlenmesi gerekmektedir[116].

1. Bulut Bilişimin Avantajları

Bulut bilişim, bilişim teknolojisini kullanan kişi, kurum ve kuruluşlar için birçok avantaja sahiptir. Bu avantajlardan bazıları şu şekildedir;

a. Düşük Donanım Maliyeti

Bulut bilişimde tüm sistem internet bağlantısı üzerinden gerçekleştirilir ve yine internet bağlantısı üzerinden ücretlendirilir. Dolayısıyla verilerin saklanması için yüksek maliyetli sunucu odalarına ve yüksek performanslı bilgisayarlara ihtiyaç duyulmamakta bu da maliyetin düşmesini sağlamaktadır[117]..

b. Düşük Yazılım Maliyeti

Bulut bilişim, ortak bir sistem üzerinden çalışmakta olduğundan her bilgisayar için ayrı yazılım ihtiyacı bulunmamaktadır. Yine kullanılan yazılımların bakım ve güncellemeleri hizmet sağlayıcı tarafından yapıldığı için ek maliyet çıkmamaktadır[118].

c. Güncel Olma

Kullanılan uygulama veya yazılımın yeni sürümünün çıkması durumunda servis sağlayıcı tarafından bulut uygulaması otomatik olarak güncellenmektedir[119]. Bu sistemin en büyük avantajlarından biridir.

d. Uzaktan Erişim

Bulut bilişim, kullanıcıya ait verilerin internet üzerindeki bir sunucuya aktarılması, depolanması ve gerektiğinde uzaktan erişim yoluyla bu verilere erişme ve üzerinde değişiklik

---

116 **Turan,** s.117.

117 **Henkoğlu/Külcü,** s.66; **İbrahim Halil Seyrek**, Bulut Bilişim, İşletmeler için Fırsatlar ve Zorluklar, Gaziantep Üniversitesi Sosyal Bilimler Dergisi, Y:10 S:2 s.708. (701-713); **Kılıç,** s.50.

118 **Seyrek,** s.705.

119 **Batı,** s.16; **Kılıç,** s.52.

yapabilme temeline dayanmaktadır[120]. Bu da bulut bilişimin en önemli avantajlarından biridir.

e. Sınırsız Depolama

Bulut bilişimde depolama imkanı sınırsız denebilecek kadar geniştir ve teknoloji ile beraber gelişmeye devam etmektedir[121]. Bulut bilişim sisteminin geneline hakim olan kullandığın kadar öde mantığı burada da geçerlidir. Yani ne kadar geniş depolama alanı istenirse ödenen miktar artacaktır.

f. Veri Güvenliği

Bulut bilişim sisteminde yer alan veriler bulut sunucularda saklanmakta bu da yerel disklerde oluşabilecek bir arıza durumunda meydana gelebilecek bir veri kaybının önlenmesini sağlar[122].

3. Bulut Bilişimin Dezavantajları

Bulut bilişim teknolojisinin, sağladığı pek çok avantajın yanında bireylerin ve kurumların bu sistemleri kullanma konusunda çekimser olmasına sebep olan birtakım dezavantajları da bulunmaktadır.

a. Sabit İnternet İhtiyacı

Bulut bilişim sistemi, internet bazlı olup internete erişim imkanının bulunmadığı durumlarda erişim sağlanamadığı için kullanılabilir değildir. Bulut üzerindeki veri ancak internet bağlantısı gerçekleştiğinde erişilebilir ve üzerinde değişiklik yapılabilir duruma gelecektir.

---

120 **Gökhan Şengül/Atila Bostan,** Bulut Bilişimde Bilgi Güvenliği Standardizasyon Çalışmaları, 6. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı, s.264. https://www.iscturkey.org/assets/files/2016/03/2013-paper45.pdf (E.T:27.06.2019); **Kılıç,** s.51.

121 **Batı,** s.17.

122 **Batı,** s.17.

b. İnternet Hızı

Bulut bilişim internet bazlı olduğundan, bağlanılan internetin kalitesi bulut bilişim sisteminin hizmet kalitesini etkilemektedir.

c. Veri Güvenliği

Bulut bilişim teknolojisinin ve bu teknolojinin kullanım alanlarının hızla gelişmesi ve yaygınlaşması kullanılan ortamları failler için de cazip hale getirmektedir. İnternet kullanımının artması ve her an her noktadan erişilebilir hale gelmesi ve bu sayede her türlü veriye de her an erişilebilmesi, bulut bilişim ortamlarını da bu alanda işlenen suçlar için yeni bir saha haline getirmiştir[123]. Bilişim teknolojilerinin bulunduğu ortamlarda her zaman risk faktörü vardır ve hiçbir zaman tam anlamıyla bir güvenlik söz konusu değildir[124]. Bulut bilişimde de veri güvenliği ile ilgili risklerin bulunması, kamusal ve özel sektörlerde tamamen bu sistemlere geçişin önündeki en önemli engeldir[125]. Gizlilik düzeyi yüksek verilerin herkesin ulaşabileceği platforma taşınması sorun yaratabilir.

Ayrıca bulut bilişim sistemine taşınan verilerin silinmemesi durumunda, depolama kaynağının bir başka kullanıcıya tahsis edilmesi halinde bu verilerin başka kullanıcıların eline geçme ihtimali de bulunmaktadır.

Bulut bilişim sistemlerinde yer alan verilerin güvenliği ile ilgili teknik risklerden bazıları şunlardır;

(1) Dış Kaynaklı Saldırılar

Bulut servis sağlayıcıları, çok sayıda iş alanına destek sağlamaları ve hizmetlerinin internet üzerinden kullanılabilir olması sebepleriyle, kendi web site portalları aracılığıyla saldırıya uğrama riski altındadır[126]. Bu kapsamda en yaygın saldırılar DDoS saldırılarıdır[127].

---

123 **Emekçi, Kuğu, Temiztürk,** s.11.
124 **Öz**, s.21.
125 **Ahmet Efe/Isamettin Omak,** Security Considerations Regarding Terms And Conditions of Cloud Service Providers, İleri Teknoloji Bilimleri Dergisi, C:8, S:1, 2019, s.31. https://dergipark.org.tr/download/article-file/719662 (E.T: 02.07.2019).
126 **Kılıç,** s.185.
127 DDoS saldırılara ilişkin açıklamalar için bkz. s.40.

(2) Verilerin Güvensiz veya Etkisiz Silinmesi

Bir kullanıcı, hizmet sağlayıcısını değiştirdiğinde sağlayıcının kullanıcı için ayırdığı kaynak geri alınarak başka bir kullanıcıya tahsis edilmektedir. Bu durumda önceki kullanıcının verilerinin tamamen silinememesi halinde başka kullanıcılar tarafından ele geçirilmesi mümkün olabilmektedir[128].

(3) Nakil Halindeki Veriyi Yakalama

Bulut bilişim sisteminin yapısı itibariyle çok fazla veri aynı anda dolaşımda olabilmektedir. Bu sebeple veri transferleri sırasında dinleme, sızdırma, iki bağlantı noktası arasındaki bağlantıyı izinsiz izleme gibi saldırılar olasıdır[129]. Sağlayıcı ile kullanıcı arasındaki hizmet sözleşmesinde sağlayıcının gizlilik taahhüdünde bulunması ve bu taahhüdün dolaşımdaki verileri de kapsaması, saldırı riskini azalmaktadır.

Veri güvenliği ile ilgili birtakım hukuksal riskler de bulunmaktadır. Örneğin, bulut bilişimde, servis sağlayıcı ve hizmet sağlayıcısı birbirinden farklı bir ülkede, verilerin depolandığı sunucular yine dünyanın farklı yerlerinde bulunabilmektedir[130]. Bu durum delillerin elde edilmesindeki zorluklar yanında, ilgili verilerin bulunduğu yere bağlı olarak söz konusu takip edilen faaliyetin ilgili yerde suç olup olmadığı, herhangi bir hukuki sorun oluşması durumunda uygulanacak hukukun ve yargılama yetkisinin belirlenmesi, elektronik delillerin toplanması gibi konularda güçlükler oluşturmaktadır[131].

Yine veri merkezleri hukukun üstünlüğünün eksik olduğu, öngörülemeyen yasal çerçeve ve uygulamalara sahip, uluslararası anlaşmalara saygı göstermeyen yüksek riskli ülkelerde yer alıyorsa, veri merkezleri yerel yetkililer tarafından basılabilir ve servis sağlayıcıları veri ve sistemleri açıklamak ya da el konulmasına izin vermek durumunda kalabilirler[132].

---

128 **Batı,** s.22**; Kılıç,** s.185.
129 **Kılıç,** s.186.
130 **Seyrek,** s.705.
131 **Öz**, s.25; **Emekçi, Kuğu, Temiztürk**, s.12.
132 **Kılıç,** s.191.

II. BİLİŞİM SUÇU KAVRAMI, GENEL ÖZELLİKLERİ VE TÜRK CEZA HUKUKUNDA DÜZENLENEN BİLİŞİM SUÇLARI

A. KAVRAM

Teknolojinin gelişmesi ile beraber bilişim, günlük yaşamın hemen hemen her alanında vazgeçilemez olmuştur. Öyle ki, bir sistemin çökmesi halinde insanlar iş yapmaz hatta iletişim kuramaz hale gelmiştir. Bu sistemlerin hızla gelişmesi ile birlikte insan hayatında kapladığı yerin artması, bu sistemler üzerinde ve sistemler aracılığıyla suçun işlenmesindeki kolaylık, failin tespitinin zorluğu gibi sebepler bu alandaki suçların da artmasına ve çeşitlenmesine sebep olmuştur[133].

Bilinen ilk bilişim suçu 18 Ekim 1966 tarihli Minneapolis Tribune'da yayınlanan "Bilgisayar uzmanı banka hesabında tahrifat yapmakla suçlanıyor" başlıklı makale ile kamuoyuna yansımıştır[134]. O tarihten bu yana bilişim araçlarının çoğalması ve yaygınlaşması sebebiyle mevzuatta bilişim suçu kategorisine giren suçların sayısı ve bu suçların işlenme oranı katlanarak artmaktadır[135].

Bilişim suçları, mevzuatta tanımlanmış bir suç şekli değildir. Sürekli değişime ve gelişime açık bir alan olduğundan net bir tanımlama yapmak yerine suçları oluşturan fiillerin sayılması yoluna gidilmiştir[136]. Doktrinde de bu nedenle üzerinde anlaşılmış ortak bir tanım bulunmamaktadır[137].

---

133 **Çığır İlbaş,** Bilişim Suçlarının Sosyo-Kültürel Seviyelere Göre Algı Analizi, Yayımlanmamış Yüksek Lisans Tezi, Başkent Üniversitesi FBE, Ankara, 2009, s.2 https://tez.yok.gov.tr/UlusalTezMerkezi/ (E.T: 25.11.2018); **İsmail Melih Taş,** Bilgisayar Tabanlı Bilişim Suçlarının Adli Bilişim Çerçevesinde İncelenmesi ve Analizi, Yayımlanmamış Yüksek Lisans Tezi, Marmara Üniversitesi FBE, İstanbul, 2013, s.1 https://tez.yok.gov.tr/UlusalTezMerkezi/ (E.T: 25.11.2018); **Ersoy**, s.168.
Yener Ünver, Türk Ceza Kanunu'nun ve Ceza Kanunu Tasarısının İnternet Açısından Değerlendirilmesi**,** İstanbul Üniversitesi Hukuk Fakültesi Mecmuası İnternet özel Bölümü, 2001, C.:59, Sayı:1-2, s.51.

134 **Emin Doğan Aydın**, Bilişim Sistemlerinde, Güvenlik, Güvenirlik, Mahremiyet ve Bilişim Suçları Marmara İletişim Dergisi, 1992, Sayı:1, http://dergipark.gov.tr/maruid/issue/434/3229 (E.T: 04.06.2018) s.113.

135 **Halil İbrahim Dilek,** Bilişim Suçları ve Türk Hukuk Sistemindeki Yeri, Dicle Üniversitesi SBE, Yayımlanmamış Yüksek Lisans Tezi, Diyarbakır, 2006, s.6 https://tez.yok.gov.tr/UlusalTezMerkezi/ (E.T: 25.11.2018).

136 **Hakan Karakehya**, Türk Ceza Kanununda Bilişim Sistemine Girme Suçu TBB Dergisi 2009, S:8, s.2. http://portal.ubap.org.tr/App_Themes/Dergi/2009-81-498.pdf (E.T:05.06.2018).

137 **Berrin Bozdoğan Akbulut**, Bilişim Suçları, Selçuk Üniversitesi Hukuk Fakültesi Dergisi 2000, C:8, s.549. https://www.selcuk.edu.tr/hukuk/birim/web/sayfa/ayrinti/2102/tr (E.T 04.06.2018).

Akbulut bilişim suçlarını, *"verilerle veya veri işlemle konu bağlantısı olan ve bilişim sistemleriyle veya bilişim sistemine karşı işlenen suçlar"* olarak tanımlamaktadır[138]. Yazıcıoğlu, "*ceza kuralları uyarınca, bilgisayarın konusunu, vasıtasını veya simgesini oluşturduğu, suç olgusu içeren fiiller*" olarak tanımlamıştır[139].

Karagülmez ise bilişim suçunu "*bilişim sistemine yönelik veya bilişim sisteminin kullanıldığı suç*" şeklinde tanımlamaktadır[140].

Diğer bir tanıma göre ise, bilgisayarın suç konusu veya aracı olduğu her türlü kanun dışı eylem, bilgisayar suçlarını oluşturur[141].

Daha genel bir tanımlamayla bilişim suçları temelde bilişim sistemi aracılığıyla veya bilişim sistemine karşı işlenen suçlardır[142].

Yazıcıoğlu'nun tanımında da olduğu gibi bilişim araçlarının en yaygın olanının bilgisayarlar olması ya da bilgisayar esasına dayanması sebebiyle doktrinde *"bilgisayar suçu"* kavramı da kullanılmaktadır[143]. Ancak, günümüzde akıllı cep telefonları veya televizyonlar ile de bilişim suçlarının işlenebildiği ve bilişim kavramın bütün bilişim araçlarını kapsadığı düşünüldüğünde bilişim suçları kavramının kullanılması yerinde olacaktır.

---

138 **Akbulut**, s.551.

139 **Yazıcıoğlu**, s. 142.

140 **Karagülmez**, s.54.

141 **Klaus Tiedemann**, Bilgisayarla İşlenen Suçların Ceza Hukuku Yönünden İncelenmesi, (Çev:FeridunYenisey), İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, 1975, C:41, s.321, http://www.journals.istanbul.edu.tr/iuhfm/article/view/1023010611/1023009846 (E.T: 05.11.2018).

142 **Emin Doğan Aydın**, Bilişim Suçları ve Hukukuna Giriş, Ankara: Doruk Yayınevi, 1992, s.3; **Veli Özer Özbek,** "İnternet Kullanımında Ortaya Çıkabilecek Bazı Ceza Hukuku Sorunları" s.107. http://hukuk.deu.edu.tr/dosyalar/dergiler/DergiMiz4-1/PDF/ozbek5.pdf (E.T: 06.10.2018).

143 **Yazıcıoğlu,** s.224,225; **Ersoy,** s.159 **Faruk Erem,** Bilgisayar Suçları ve Türk Ceza Kanunu, http://tbbdergisi.barobirlik.org.tr/m1993-19932-968 (E.T: 03.02.2019).

B. BİLİŞİM SUÇLARININ ÖZELLİKLERİ

Bilişim suçları yapısı itibariyle kolay işlenebilir niteliktedir ancak, hem suçun hem de failin tespiti oldukça zor olup teknik ve hukuki açıdan uzmanlık gerektirir[144]. Bunun sebebi, çoğunlukla suç oluşturan fiillerin dijital ortamda gerçekleştirilmesi nedeniyle suçun işlendiği yerin tespitinin zor olması ve faillerinin çoğunlukla anonim profillere sahip olmasıdır[145]. İzini saklamak isteyen fail kendi internet bağlantısını, bir başka yer ve ülkede bulunan vekil sunuculara bağlanarak gerçekleştirmekte ve devamında internetteki eylemlerde bu vekil sunucunun IP numarasını bırakmakta ve kendini gizlemektedir[146].

Suçun dijital ortamda işlenebilmesinin bir sonucu da faillerin her an her yerde bu fiilleri gerçekleştirebilmesidir[147]. Bu aşamada suç uluslararası bir boyut kazanabilmekte ve uluslararası iş birliği gerektirebilmektedir[148]. Ayrıca, fiilin milisaniyelerle ölçülen zaman dilimlerinde işlenebilmesi, bu suçlarda maddi hareketin tespitini de güçleştirmektedir[149].

Bir suçun bilişim suçu olması için mutlaka bilişim sistemlerinin kullanılması gerekmektedir ve bu suçlar bilişim sistemlerinin kullanıldığı her alanda işlenebilmektedir. Bu sistemlerin kullanılması için failin belli bir düzeyde teknik bilgiye sahip olması

---

144 **Alper Güneş,** Bilişim Suçları ve İdarenin Hukuki Sorumluluğu, Yayımlanmamış Yüksek Lisans Tezi, Selçuk Üniversitesi SBE, Konya, 2015, s.15 https://tez.yok.gov.tr/UlusalTezMerkezi/ (E.T: 25.11.2018).

145 **Feridun Nizam**, Avrupa Birliği Bilişim Politikası ve Türkiye'nin Uyumu**,** Akademik Bilişim 2005 Konferansı Konuşma Metni, s.4, https://ab.org.tr/ab05/tammetin/89.doc (E.T: 03.02.2019) ; **Eşref Adalı, "**İnternet Suçları" Bilişim ve İnternet Teknolojilerinin Ceza Hukuku Açısından Doğurduğu Yeni Sorunlar Konferansı Konuşma Metni, Bursa, İçişleri Bakanlığı Yayını, 2001, s.39; **İsmail Fert,** İnternet Kafeler Üzerinden Gerçekleştirilen Bilişim Suçları, Adli Psikiyatri Dergisi, C:2, S:1, 2005, s.18, https://jurix.com.tr/article/7288 (E.T: 18.12.2018).

146 TBMM, Bilişim ve İnternet Araştırma Komisyonu Raporu, 2012, s.841. http://www.biakraporu.org/docs/rapor.kisim3.bolum01.pdf (E.T: 03.02.2019); **Karagülmez**, s.80.

147 **Hayati Pallı,** Türk Hukukunda ve Mukayeseli Hukukta Bilişim Suçları, Yayımlanmamış Yüksek Lisans Tezi, Erciyes Üniversitesi SBE, Kayseri, 2008, s.48 https://tez.yok.gov.tr/UlusalTezMerkezi/ (E.T: 25.11.2018); **Ufuk Taşçı / Ali Can,** Türkiye'de Polisin Siber Suçlarla Mücadele Politikası, Fırat Üniversitesi Sosyal Bilimler Dergisi, C:25, S:2, Elazığ, 2015,s.231.

148 **Cahit Aliusta/Recep Benzer**, Avrupa Siber Suçlar Sözleşmesi ve Türkiye'nin Dahil Olma Süreci, Uluslararası Bilgi Güvenliği Mühendisliği Dergisi, 2018, C:4 S:2, s.35-36; **Fatih Selami Mahmutoğlu**, Karşılaştırmalı Hukuk Bakımından İnternet Sujelerinin Ceza Sorumluluğu, İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, İnternet Özel Bölümü, İstanbul, 2001 C:59, Sayı:1-2, s.39.

149 **Hikmet Dijle,** Türkiye'de Eğitimli İnsanların Bilişim Suçlarına Yaklaşımı, Gazi Üniversitesi FBE, Yayımlanmamış Yüksek Lisans Tezi, Ankara, 2006, s.6 https://tez.yok.gov.tr/UlusalTezMerkezi/ (E.T: 25.11.2018); **Barış Emre Alp**, 5237 Sayılı Türk Ceza Kanunu'nda Bilişim Sistemini Engelleme, Bozma, Verileri Yok Etme veya Değiştirme Suçu, Yayımlanmamış Yüksek Lisans Tezi, Çankaya Üniversitesi SBE, Ankara, 2018, s.25. https://tez.yok.gov.tr/UlusalTezMerkezi/ (E.T: 25.11.2018).

gerekmektedir[150]. Bu da suçu, klasik suçlar gibi herkes tarafından işlenebilir olmaktan çıkarmaktadır. Ancak; günümüzde hemen her alanda bilişim sistemlerinin kullanılıyor olması suçun işlenme oranını artırdığı gibi bilişim sistemleri ile ilgili temel bir bilgiye sahip kişilerin de suçun faili olabilmesine yol açmaktadır[151].

Bilişim suçlarında fail, daha az emekle büyük zararlar meydana getirilebilmektedir[152]. Örneğin, bir hastanenin arşiv sistemine girilerek mevcut verilerin değiştirilmesi sonucunda müdahale edilen hastaların ölümüne sebep olunabilir. Bu da bireysel zarardan çok kitlesel zararlar meydana getirmeyi amaçlayan faillerin bilişim suçlarını tercih etmesine sebep olabilmektedir.

Bilişim suçlarını işleyenlerin teknik bilgiye sahip olmaları, bu suça ilişkin yasal düzenlemeleri ve suçun tespitini yapacak kişilerin de teknik bilgiye sahip olmasını ya da teknik açıdan destek almalarını gerektirmektedir[153]. Bu da uzun vadede, üniversitelerde bilişim ve bilişim hukuku derslerinin verilmesi, bu alanda işlenen suçlara ilişkin uzmanlaşmış birimlerin oluşturulması, delil tespiti ve delil toplamanın suç açısından oldukça önemli olması sebebiyle kolluk personellerinin bu alanda uzmanlaşmasının sağlanması ve meslek içi eğitimlerle bilgilerin sürekli güncel tutulması, ihtisas mahkemeleri kurularak[154] bu alanda hem hukuki hem de teknik bilgiye sahip hakim ve savcılar tarafından yargılamanın gerçekleştirilmesi ve yine meslek içi eğitimlerle hakim ve savcıların da bu alandaki bilgilerinin güncel kalmasının sağlanması, uzmanlaşmış kişilerin başka birimlere atanmaması gibi çözümlerle sağlanabilir. Kısa vadede ise bu alanda uzmanlaşmış teknik bilirkişilerden faydalanılması gerekmektedir.

---

150 **Pallı,** s.48.

151 **İnci Biçkin,** "Siber Suç Sözleşmesi ve 5237 S. Türk Ceza Kanununda Bilişim Suçları", Yargıtay Dergisi, C:32, Ocak-Nisan 2006, Sayı:1-2, s.165.

152 **Erdoğan**, Bilişim Suçları, s.88.

153 **Erdoğan**, Bilişim Suçları, s.89-90; **İsmail Tulum,** Bilişim Suçları ile Mücadele, Süleyman Demirel Üniversitesi SBE, Yayımlanmamış Yüksek Lisans Tezi, Ankara, 2006, s.23 https://tez.yok.gov.tr/UlusalTezMerkezi/ (E.T: 25.11.2018).

154 **Serkan Gönen/Halil İbrahim Ulus/Ercan Nurcan Yılmaz,** Bilişim Alanında İşlenen Suçlar Üzerine Bir İnceleme, Bilişim Teknolojileri Dergisi, C:9, S:3, 2016, s.236.

C. BİLİŞİM SUÇLARININ İŞLENME ŞEKİLLERİ

1. Virüsler

Virüsler, kendisinin değiştirilmiş bir kopyasını eklemek için işletim sistemlerini ve programları değiştiren veya çalışamaz hale getiren ya da onlara zarar veren programlardır[155]. En büyük özellikleri kendi kendilerini çoğaltabilmeleri ve yayılmalarıdır[156]. Virüsler, çoğunlukla yerleştikleri programın işletilmesiyle bilgisayarın hafızasına geçerler ve bilgisayar kapatılıncaya kadar orada kalıcı hale gelirler[157]. Virüslerin diğer zararlı yazılımlardan farkı, bulaştıkları bilişim sisteminde bulunan yazılımları çökerterek, bilişim sistemine olası en fazla zararı verecek şekilde tasarlanmalarıdır[158].

2. İstem Dışı Alınan Elektronik Postalar (SPAM)

İstem dışı alınan elektronik postalar Uluslararası Ticaret Örgütü tarafından, bir bülten ya da haber grubu üzerinden ticari amaç taşımayan, forum konuları ile ilgili olmayan ve gönderilmesine açık bir şekilde izin verilmeyen reklam olarak tanımlanmıştır[159]. SPAM veya istenmeyen e-posta kavramı genellikle, reklam, ürün ve web ilanları, kolay para kazanma vb. içerikli e-postalar için kullanılır[160]. Spamlar, kişilerin e-posta kutularını da gereksiz yere doldurur ve bu sebeple kişinin e-posta kutusuna, bilgi sağlayıcı, yararlı herhangi bir e-posta geldiğinde otomatik olarak e-postanın reddedilmesi ihtimali söz konusu olduğundan mağduriyete sebep olabilir[161]. 6563 sayılı Elektronik Ticaretin Düzenlenmesi Hakkında Kanunun 5.11.2014 tarihinde Resmi Gazete'de yayımlanması ve 01.05.2015 tarihinde yürürlüğe girmesiyle ticari elektronik iletilerin gönderilmesi açıkça önceden onay alınması şartına bağlanmıştır. Spam iletilerin sistemin işleyişini engelleyecek boyuta

---

155 **Akbulut,** Bilişim Alanında Suçlar, s.76; **Gül,** s.40; **Değirmenci,** Bilişim Suçları, s.88.
156 **Albayrak**, s.29.
157 **Akbulut,** Bilişim Alanında Suçlar, s.77.
158 **Dülger,** s.112.
159 **Tekin Memiş**, Hukuki Açıdan Kitlelere E-Posta Gönderilmesi, Atatürk Üniversitesi Erzincan Hukuk Fakültesi Dergisi, C:5, S:1-4, 2001, s.432,433.
160 **Cahide Ünal/İsmail Şahin**, İstanmeyen Elektronik Postaların (SPAM) Filtrelenmesi için Bir Uzman Sistem Tasarımı ve Gerçekleştirilmesi, Politeknik Dergisi, C:20, S:2, 2017, s.267. https://dergipark.org.tr/download/article-file/385860 (E.T:02.07.2019).
161 **Alp,** s.36; **Dülger,** s.114.

ulaşması halinde TCK'nın 244'üncü maddesi kapsamında değerlendirilmesi gerekmektedir[162].

3. Truva Atı (Casus Yazılımlar – Trojan Horse)

Truva atı yönteminde fail, bilgisayarda kullanılan programın istediği çalışmayı gerçekleştirmesi için içine gizli bir bilgisayar programını ilave etmektedir. Böylece cihaz kendi işlemlerini yaptıktan sonra, fail tarafından düzenlenmiş olduğu üzere, bir veya birkaç işlem daha gerçekleştirmektedir. Yani önce program sistem sahibinin amaçladığı şekilde çalışmakta ve fakat bu işlemden sonra ya fail tarafından çağrıldığında yahut önceden verilen direktifler doğrultusunda, failin istediği doğrultuda çalışmaktadır[163]. Truva atlarının en yaygın kullanım alanlarından birisi, çok kullanıcılı bilişim sistemlerinin güvenlik mekanizmalarını kırmaktır[164].

4. Sistem Güvenliğini Kırma (Hacking)

Sistem güvenliğini kırma, bilgi veya program elde etmek, zarar vermek için bir bilişim sistemine yetkisiz erişim olarak tanımlanabilir[165]. Bilişim korsanları, internet üzerinden sistemlerin güvenliğinin kırarak, tespit edilene kadar sistem içerisinde istediği bilgiye ulaşabilmekte, istedikleri verileri ele geçirebilmektedir[166]. Bu yöntemlerle hackerler, haberleşme özgürlüğü, özel hayatın gizliliğini ihlal gibi birçok hakkı ihlal edebildikleri gibi sistemin işleyişini de bozabilirler[167].

Bilişim sisteminin güvenliğinin kırılıp içeri girilmesi eyleminin diğer suç işleme şekillerinden farkı, genellikle sisteme giriş sırasında yardımcı yazılımlar kullanılmasından ziyade eylemin bizzat bilişim korsanlarının becerisine dayanmasıdır[168].

---

162 **Kurt,** s.73.
163 **Yazıcıoğlu**, s.153-154, **Dülger**, s.104, **Ergün,** s.17
164 **Değirmenci,** s.80.
165 **Karagülmez,** s.87.
166 **Alp,** s.39.
167 **Yaycı,** s.31.
168 **Dülger,** s.107.

5. Veri Aldatmacası (Data Diddling)

Veri aldatmacası ile verinin bilgisayara veya hafızasına kaydı sırasında değiştirilmesi, bilgisayara yanlış veri girilmesi veya bazı verilerin kasten bırakılması ifade edilmektedir[169]. Bu işlem belgelerin tahrif edilmesi, veri ortamlarının özel olarak hazırlanmış materyal ile değiştirilmesi, kartlara ek karakter kaydı gibi yöntemlerle gerçekleştirilebilir[170]. Fail, sisteme girdiği ya da sistemde bıraktığı verilerle, sistemde mevcut veriler üzerinde istediği gibi değişiklik yapma imkanına sahiptir[171]. Bilişim suçları içerisinde işlenmesi en kolay ve işlendikten sonra tespiti en zor yöntem olduğundan sıklıkla tercih edilmektedir.

6. Sosyal Mühendislik

Sosyal mühendislik; etkileme, zorlama, aldatıcı ilişkiler geliştirme, sorumluluğu, etik değerleri, dürüstlüğü ya da bağlılığı azaltma amacını güden yöntemler kullanarak kişileri gizli bilgi vermeleri veya erişim sağlamaları için aldatma sürecidir[172]. Bilişim sistemlerinin kullanımının yaygınlaşması sebebiyle bu yöntemle son zamanlarda sıklıkla karşılaşılmaktadır.

Bu yöntemde failler isteklerini akıllıca ortaya koyarak karşı tarafın güveninden yararlanmaktadırlar. Bu sebeple sosyal mühendislik uzmanları daha çok karşı tarafın dış yüzü olarak adlandırılan yani servis elemanları, çağrı merkezi elemanları, müşteri hizmetleri personeli gibi hareket ederek kişilere ulaşıp onlarla iletişime geçerler[173].

Sosyal mühendisliğin amacı bilgi toplamak olup, bilgi toplamanın ilk adımı internet, teknoloji dergileri, şirket broşürleri gibi açık kaynaklardan yapılacak araştırmadır. İkinci adımda ise hedef sistem hakkında bilgi toplanmakta ve özelikle sistemin güvenlik açıkları araştırılmaktadır[174].

---

169 **Kurt,** s.62; **Yaycı,** s.333.
170 **Aydın,** s.48.
171 **Yazıcıoğlu**, s.153.
172 **Hasan Bağcı**, Sosyal Mühendislik ve Denetim, Denetişim Dergisi, S:1, 2009, s.43, https://dergipark.org.tr/download/article-file/209001 (E.T: 02.07.2019).
173 **Alp**, s.31.
174 **Orta,** s.76.

7. Gizlice Dinleme

Bilişim sistemlerinin veri naklinde kullandığı ağlara girilerek veya bilişim sistemlerinin az da olsa yaydığı elektromanyetik dalgaların yakalanarak verilerin tekrar elde edilmesi tekniğidir[175]. Bu yöntem en çok bilgisayar ekranlarının yaydığı elektromanyetik dalgaların araya konulacak yükselteçler vasıtasıyla yakalanarak, kendi ekranlarına yansıtılması ile yapılmaktadır[176].

8. Solucanlar (Network Worms)

Ağ solucanı, kullanıcının etkisi olmadan kendi kendine çalışabilen ve aynen kendisi gibi bir kopyasını, veri iletim ağına bağlantısı olan diğer bilişim sistemlerine kopyalayabilen yazılım türleridir[177]. Ağ üzerinden bir bilişim sistemine gelen bir ağ solucanı ya bir virüs gibi davranarak yazılıma zarar verir ya da sisteme bir Truva atı bırakır ve çoğu zaman bıraktıkları tüm izleri silerler[178]. Solucanların en büyük tehlikesi kendilerini büyük sayılarda çoğaltma becerileridir. Talimatları yerine getirir, sistemi yavaşlatır, sistemdeki bilgileri kullanıcısına ulaştırır[179].

9. Tavşanlar (Rabbits)

Tavşan olarak adlandırılan yazılımlar, içine girdikleri bilişim sisteminin içinde işlemciye sürekli anlamsız komutlar vererek işlemcinin bilişim sisteminin normal işleyişini sağlayan komutları vermesini engeller ve giderek sistemin yavaş çalışmasına, en sonunda da çalışamaz hale gelmesine sebep olur[180]. Bu yazılımlar çok hızlı üreyebilirler ve sistem en sonunda durma noktasına gelir[181]. Tavşanların faaliyete geçebilmesi için dışarıdan müdahaleye (tavşanın bulaştığı dosyanın açılması ya da çalıştırılması gibi) ihtiyacı yoktur[182].

---

175 **Kurt,** s.62.
176 **Alp,** s.29.
177 **Dülger,** s.109.
178 **Değirmenci,** s.87.
179 **Gül,** s.40.
180 **Kurt,** s.75; **Dülger,** s.110.
181 **Gül,** s.40; **Değirmenci,** Bilişim Suçları, s.107.
182 **Değirmenci,** s.103.

10. Bukalemunlar (Chameleon)

Bukalemunlar, sistem içerisinde normal bir şekilde zararsız bir yazılım gibi davranıp o niteliklere sahipmiş gibi görünerek sistem içerisine dahil olurlar[183]. Bunlar uygun olarak programlandırıldıklarında kanunun aradığı şartlara uygun olarak oluşturulmuş yazılımların her hareketlerini taklit etme özelliklerine sahiptirler[184].

11. Web Sayfası Hırsızlığı ve Yönlendirmesi

Bir web sayfasına ulaşmak isteyen kullanıcının ulaşmak istediği web sayfasına benzer şekilde hazırlanmış başka bir sayfaya yönlendirilmesi ve bu sayfada işlem yapmak isteyen kişinin kendiliğinden verdiği kullanıcı adı ve şifresine ulaşmak veya çok bilinen web sayfalarına ulaşmak için adresi küçük farklılıklarla yanlış yazanların adresin neresinde yanlış yapacağını tahmin ederek bunu yazabileceklerin ulaşabileceği bir sayfa oluşturulması yöntemidir[185]. Bu yöntem genellikle TCK'nın 142'nci maddesinin ikinci fıkrasının "e" bendinde yer alan bilişim sistemi kullanmak suretiyle hırsızlık suçunun işlenmesinde sıklıkla kullanılır[186].

12. Oltalama (Phishing)

İngilizce *"Password"* (şifre) ve *"Fishing"* (Balık Avlamak) kelimelerinin birleşmesiyle oluşturulan Phishing, Türkçe'ye oltalama, sazan avı, yemleme olarak çevrilmiş olup bilgi ve iletişim teknikleri kullanılmak suretiyle hedef alınan kişilerin aldatılarak veya ikna edilerek kişisel bilgilerin ele geçirilmesi ve kötü niyetle kullanılması olarak tanımlanmakta ve bu yönüyle bir tür sosyal mühendislik saldırısı olarak da nitelendirilmektedir[187]. En sık kullanılan sosyal mühendislik saldırılarından ve siber tehditlerden biri olan yemleme, diğer siber tehditler gibi, siber saldırganlar tarafından, siber suç olarak nitelendirilen eylemleri gerçekleştirmek üzere kullanılmaktadır[188]. Yemleme, iki

---

183 **Gül,** s.40.
184 **Akbulut,** Bilişim Alanında Suçlar, s.82.
185 **Kurt,** s.73.
186 **Dülger**, s.120.
187 **Orta,** s.86; **Alp,** s.30; **Dülger,** s.117; **Akbulut**, Bilişim Alanında Suçlar, s.86.
188 **Mustafa Ünver/Ayşe Gül Mirzaoğlu,** Yemleme (Phishing) Raporu, Bilgi Teknolojileri ve İletişim Kurumu Yayınları, 2011, s.2. https://www.academia.edu/24841831/Yemleme_-_Phishing (E.T:02.07.2019)

şekilde gerçekleşmektedir. Bunlardan birincisi, hedef alınan kişi aldatılarak sahte internet sitesi veya eposta adresi ya da telefon numarasına yönlendirilmektedir. Bu amaçla, istek dışı haberleşme, açılır pencerelerin kullanılması ya da arama motorları gibi araçlar devreye sokulmaktadır. İkinci yöntem ise kötücül yazılım kullanma gibi teknik hile yöntemleri kullanılarak hedef alınan kişinin bilgisayarında ya da eriştiği sitelerde bir takım ayar değişiklikleri yaparak kişisel verilerin ele geçirilmesidir[189].

13. Gizli Kapılar (Trap Doors)

Gizli kapı veya hile kapısı; işletim sistemleri veya çok işlevli ve kullanıcılı sistemleri hazırlayan bilgisayar programcılarının bunları meydana getirirken ileride ortaya çıkabilecek durumlara göre, sistem şifrelerinde değişiklik yapabilmeyi veya yeni şifreler girebilmeyi sağlamak üzere sisteme bıraktıkları çeşitli giriş olanaklarına denmektedir. Ancak genelde, ortaya çıkabilecek meşru bir amaca hizmet etmek için bırakılan kapılar yine kötü niyetli bir programcının tasarrufları için iyi bir imkân kapısı da olabilmektedir[190].

14. DDoS Saldırıları

DDoS saldırısı çevrimiçi bir uygulama veya hizmetin çalışmasını engellemek amacıyla yapılan ve bant genişliğinin tamamını kullanarak sistemin cevap vermesini engellemeyi hedefleyen siber saldırı türü olarak tanımlanabilmektedir[191]. Bu saldırılar, sistemin erişilebilirliğine yönelik saldırılardır. Bu yöntemde, sistem kapasitesini aşacak şekilde anlık olarak sisteme istek gönderme yaparak aşırı yükleme yapılması amaçlanmakta ve bu sayede sistem bu istekleri karşılayamamakta ve cevap veremez duruma gelmektedir[192]. Diğer bir yöntem ise hedef olarak belirlenen sistemlerin açıklarından yararlanarak saldırı yapmaktır.

---

189 **Dülger,** s.117; **Ünver**, s.3 vd.

190 **Yazıcıoğlu,** s.157, **Ergün,** s. 19; **Ebru Altunok/ Fatih Vural,** Bilişim Suçları, Denetişim Dergisi, S:8, 2011, s.79, https://dergipark.org.tr/download/article-file/208853 (E.T:18.12.2018).

191 Ulusal Siber Olaylara Müdahale Merkezi (USOM -TRCERT) Bilgi Teknolojileri ve İletişim Kurumu DDoS El Kitabı, s.3 http://some.sdu.edu.tr/assets/uploads/sites/408/files/ddos-el-kitabi-22092017.pdf (E.T:02.07.2019).

192 **Topaloğlu/Özkişi/Tekkanat,** s.85.

D. TÜRK CEZA KANUNU'NDA DÜZENLENEN BİLİŞİM SUÇLARI

Bilişim sistemlerinin zamanla yaygınlaşması ve buna paralel olarak bu sistemlerin sağladığı faydaların kötüye kullanımı mevzuatta bu fiillere yönelik yaptırımların öngörülmesine neden olmuştur[193].

Türk Ceza Kanunu, iki kitaptan oluşmaktadır. Birinci kitap ceza hukuku ile ilgili genel ilkeleri içeren üç kısımdan oluşmaktadır. İkinci kitap ise ceza hukuku ile ilgili özel hükümlerin, suç tiplerinin yer aldığı, "*insanlığa karşı suçlar*", "*kişilere karşı suçlar", "topluma karşı suçlar"* ve *"millete ve devlete karşı suçlar ve son hükümler"* başlıklı dört kısımdan, bu kısımlar da çeşitli bölümlerden oluşmaktadır.

Kanunun *"kişilere karşı suçlar"* başlıklı ikinci kısmının *"özel hayata ve hayatın gizli alanına karşı suçlar"* başlıklı dokuzuncu bölümünde ve *"topluma karşı suçlar"* başlıklı üçüncü kısmının *"bilişim alanında suçlar"* başlıklı onuncu bölümünde *"bilişim sistemine girme", "sistemi engelleme, bozma, verileri yok etme veya değiştirme", "banka veya kredi kartlarının kötüye kullanılması"* ve *"yasak cihaz ve programlar"* suçları düzenlenmiştir. Bunun yanında bilişim suçu niteliğinde olmayan ancak bilişim sistemleri aracılığıyla işlenmesi mümkün olan *"kişisel verilerin kaydedilmesi", "kişisel verileri hukuka aykırı olarak verme veya ele geçirme", "haberleşmenin gizliliğini ihlal", "hakaret", "nitelikli hırsızlık"* ve *"nitelikli dolandırıcılık" suçları* ile *"müstehcenlik"* suçları da düzenlenmiştir. Teknolojinin hızla gelişmesi ile hemen hemen bütün suçlar bilişim sistemleri aracılığı ile işlenebilir hale gelmiştir[194].

Tez konumuz TCK'nın 244'üncü maddesinde düzenlenen *"Sistemi engelleme, bozma, verileri yok etme veya değiştirme"* suçları olup, konunun bilişim alanında işlenen

---

193 **Kızıltan,** s.20.

194 **Yasin Beceni**, Türk Hukuk'undaki Bilişim Suçlarının Tasnif Şekilleri, Ankara Barosu Hukuk Kurultayı 2006, Bilişim ve Hukuk Yargılama Hukuku, C.:4, Ankara, Ustaoğlu, Baskı Yayın Ltd. Ştd, 2006. s.68; **Eser Dursun,** Sosyal Medya Aracılığıyla İşlenen Suçlar (Geniş Anlamda Bilişim Suçları), Ceza Hukuku Dergisi, C:9, S:24, 2014, s.371 https://jurix.com.tr/article/3087 (E.T: 11.06.2018); **Cahit Aliusta/Recep Benzer,** Avrupa Siber Suçlar Sözleşmesi v Türkiye'nin Dahil Olma Süreci, Uluslararası Bilgi Güvenliği Mühendisliği Dergisi, C:4, S:2, 2018, s.36 https://dergipark.org.tr/download/article-file/645923 (E.T:11.06.2018).

diğer suçlarla yakın ilişkili olması sebebiyle bilişim alanında işlenen diğer suçlar da kısaca açıklanmıştır.

1. Bilişim Sistemine Girme veya Kalma Suçu (TCK m. 243)

Bilişim suçları TCK'nın ikinci kitabında *"Topluma Karşı Suçlar"* başlıklı üçüncü kısımda *"Bilişim Alanında Suçlar"* başlıklı onuncu bölümde yer almakla birlikte, mülga olan 765 sayılı TCK'da yer alan bilişim suçlarından farklı olarak *"bilişim sistemine hukuka aykırı olarak girme veya sistemde kalma"* ve "*bilişim sistemlerini hukuka aykırı olarak izleme"* eylemleri de suç olarak düzenlenmiştir.

Bilişim sistemine girme suçu, TCK'nın 243'üncü maddesinde düzenlenmektedir. Düzenleme ile ilgili olarak taraf olduğumuz Sanal Ortamda İşlenen Suçlar Sözleşmesi'ne uyumun artırılması için 24.03.2016 tarihli 6698 sayılı Kişisel Verilerin Korunması Kanunu ile birtakım değişiklikler yapılmıştır[195].

6698 sayılı Kanunun 30'uncu maddesi ile yapılan değişiklikle maddenin birinci fıkrasına getirilen *"veya"* ibaresi ile kanun metni ve gerekçe arasındaki çelişki giderilmiş ve bu sayede hukuka aykırı erişim ve sisteme hukuka uygun girdikten sonra hukuka aykırı olarak kalma eylemleri seçenekli hale getirilmiştir[196].

---

195 6698 sayılı Kişisel Verilerin Korunması Kanunu 24/03/2016 tarihinde kabul edilmiş, 07/04/2016 tarih ve 29677 sayılı resmi gazete'de yayımlanarak yürürlüğe girmiştir. Değişiklikle birlikte maddenin son hali şu şekildedir;
"(1) bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak giren veya orada kalmaya devam eden kimseye bir yıla kadar hapis veya adli para cezası verilir.
(2) yukarıdaki fıkrada tanımlanan fiillerin bedeli karşılığı yararlanılabilen sistemler hakkında işlenmesi halinde, verilecek ceza yarı oranına kadar indirilir.
(3) bu fiil nedeniyle sistemin içerdiği veriler yok olur veya değişirse, altı aydan iki yıla kadar hapis cezasına hükmolunur.
(4) (ek: 24.3.2016-6698/30 md.) Bir bilişim sisteminin kendi içinde veya bilişim sistemleri arasında gerçekleşen veri nakillerini, sisteme girmeksizin teknik araçlarla hukuka aykırı olarak izleyen kişi, bir yıldan üç yıla kadar hapis cezasıyla cezalandırılır."
https://www.mevzuat.gov.tr/MevzuatMetin/1.5.6698.pdf (E.T:06.11.2018)

196 **Mücahid Özbek,** Avrupa Siber Suçlar Sözleşmesinin Türk Ceza Hukukuna Etkileri, s.80, https://www.goksusafiisik.av.tr/Articletter/2015_Summer/GSI_Articletter_2015_Summer_Article6.pdf (E.T:18.12.2018); **Koca/Üzülmez** s.849.

Maddenin ikinci fıkrasında suça ilişkin indirim sebebi, üçüncü fıkrasında ise netice sebebi ile ağırlaşmış hali düzenlenmiştir.

Yine son değişiklikle eklenen dördüncü madde ile "*sisteme girmeksizin*" bilişim sisteminde veya sistemler arası veri nakillerinin teknik araçlarla ve hukuka aykırı olarak izlenmesi eylemi suç olarak düzenlenmiştir. Her ne kadar bu eylemin suç olarak düzenlenmiş olması, düzenlendiği maddeden bağımsız olarak yerinde ve Sanal Ortamda İşlenen Suçlar Sözleşmesi'ne uygun bir düzenleme olsa da "*Bilişim Alanında Suçlar*" başlıklı bölümün "*Bilişim Sistemine Girme*" başlıklı maddesinde gerçekleştirilen eylemin düzenlenmesi kanaatimizce yerinde olmamıştır ve ayrı bir maddede düzenlenmesi gerekmektedir[197].

Bu suçun düzenlenmesi ile korunan hukuki değer karma bir nitelik taşımaktadır[198]. Öncelikle, suçun düzenlenmiş olduğu başlığın "*toplum düzenine karşı suçlar*" olması düşünüldüğünde, suçla korunan hukuki değerlerin ilki, toplum düzenini korumaktır[199]. Bu suçla, kişilerin özel hayatının gizliliği, haberleşmenin gizliliği ve kullanıcı ile sistem sahibinin yani sistem içerisindeki verilerin sahiplerinin menfaatleri korunmaktadır[200]. Yine bu suçla korunan diğer bir hukuki yarar ise bilişim sisteminin güvenliğidir[201]. 6698 sayılı Kanun'la birlikte 243'üncü maddenin 4'üncü fıkrasına getirilen ve yeni düzenlenen *"bilişim sisteminin kendi içinde veya bilişim sistemleri arasında gerçekleşen veri nakillerini, sisteme girmeksizin teknik araçlarla hukuka aykırı olarak izlemek"* suçu ile de veri iletişimin gizliliğinin korunması amaçlanmıştır.

---

197 Benzer görüş için bkz. **Ahmet Gül**, Doğrudan- Dolaylı Bilişim Suçları, Ankara, Seçkin Yayıncılık, 2016, s. 57.

198 Suçla korunan hukuki yararın karma nitelikte olduğuna ilişkin benzer görüşler için bkz. **Artuk/Gökcen/Yenidünya**, Özel Hükümler, s.743, **Ali Parlar**, "Türk Ceza Hukuku'nda Bilişim Suçları", 3. Baskı, Ankara, Bilge Yayınevi, 2015, s.17, **Kurt**, s.148**; Karagülmez,** s.201**, Koray Doğan**, Bilişim Suçları ve Yeni Türk Ceza Kanunu, Hukuk ve Adalet Eleştirel Hukuk Dergisi, Y:2 S:6-7, 2005, s.335, **Özbek/Doğan/Bacaksız/Tepe**, Özel Hükümler, s.948; **A. Caner Yenidünya,** Bilişim Sistemine Hukuka Aykırı Erişim Suçu (TCK m.243), Legal Fikri ve Sınai Haklar Dergisi S:4 Y:2005, s.1024.

199 **Erdoğan**, Bilişim Suçları, s.121; **Yavuz Erdoğan,** Bilişim Sistemine Girme ve Kalma Suçu, Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi, C:12 Özel S., 2010, s.1370; **Güler,** s.16.

200 **Artuk/Gökcen/Yenidünya**, Özel Hükümler, s.743, **Dülger,** s.347 vd.; **Yazıcıoğlu**, Hukukumuzda TCK'nın 243'üncü madde kapsamında Bilişim Sistemine Girme Eylemi, s.81; **Erdoğan,** Bilişim Sistemine Girme ve Kalma Suçu, s.1370.

201 **Erdoğan,** Bilişim Sistemine Girme ve Kalma Suçu,s.1371.

TCK'nın 243'üncü maddesinde yaptırıma bağlanan fiiller 24.03.2016 tarihinde kabul edilen ve 06.04.2016 tarihinde yayımlanan ve bu tarih itibariyle yürürlüğe giren 6698 sayılı Kanun'la bir kısım değişikliğe uğradığından, yürürlük tarihi itibariyle lehe kanun uygulaması söz konusu olacaktır.

Kanun metninin değişiklik öncesi ilk halinde "*bilişim sistemine girme*" suçunun hareket unsuru, bilişim sisteminin bütününe veya bir kısmına hukuka aykırı olarak girmek ve orada kalmaya devam etmektir. Buna göre suçun oluşması için sisteme girmek yeterli olmamakta belirli bir süre sistemde kalmaya devam etmek gerekmektedir[202].

Değişiklik öncesi düzenlemeye göre, failin, sisteme hukuka uygun bir şekilde girdikten sonra hukuka aykırı olarak kalmaya devam etmesi halinde kanun, hukuka aykırı giriş ve kalmaya devam etmeyi bir bütün olarak ele aldığından suç oluşmayacaktır[203].

Madde metninde yapılan değişlik ile doktrinde eleştirilen gerekçe-madde metni çelişkisi ortadan kalkmış ve Sanal Ortamda İşlenen Suçlar Sözleşmesi'nin 2'nci maddesinde yer aldığı gibi sistemin tamamına veya bir kısmına haksız erişim suç olarak kabul edilmiştir. Dolayısıyla bu tarihten sonra işlenecek suçlar bakımından yalnızca erişimin hukuka aykırı olması yeterli sayılacak, kalmaya devam etme unsurunun varlığı aranmayacak, hukuka aykırı olması koşuluyla ani giriş çıkışlar da suç oluşturacaktır. Girmenin dışında herhangi bir suç işlenmese de sistemin güvenliğinin korunması zorunluluğu ülkeleri bu yönde düzenleme yapmaya yöneltmiştir[204].

Yine söz konusu değişiklik ile birlikte maddenin önceki halinde suç sayılmayan hukuka uygun girdikten sonra hukuka aykırı kalmak eylemi de hukuka aykırı olarak sistemde

---

202 Maddenin bu haliyle madde gerekçesi arasında çelişki bulunmakta ve haklı olarak doktrin tarafından eleştirilmekte ve aynı zamanda Sanal Ortamda İşlenen Suçlar Sözleşmesi'ne de aykırılık teşkil etmekteydi. Konuyla ilgili detaylı tartışmalar için bkz. **Karagülmez,** s.203 vd.; **Artuk/Gökcen/Yenidünya**, Özel Hükümler, s.744; **Kurt**, s.149 vd.; **Tezcan/Erdem/Önok**, s.842; **Dülger**, s.364, **Yaşar/Gökcan/Artuç**, s.6742-6743, **Yazıcıoğlu,** Hukukumuzda TCK'nın 243'üncü Madde Kapsamında Bililim Sistemine Girme Eylemi, S.82.

203 **Erdoğan,** Bilişim Sistemine Girme ve Kalma Suçu, s. 1375.

204 **Akbulut,** Bilişim Alanında Suçlar, s.116.

kalmak eylemi girme eyleminden bağımsız olarak düzenlendiğinden suç olarak kabul edilecektir.

"Sisteme hukuka aykırı olarak girmek" veya "*hukuka aykırı olarak kalmaya devam etmek*" suçları birbirinden bağımsız olarak düzenlendiğinden bu suç artık seçimlik hareketli suç niteliği taşımaktadır[205]. Sisteme hukuka aykırı olarak girmek eylemi icrai bir eylem olup ani yani neticesi harekete bitişik suçtur[206]. Sisteme hukuka aykırı olarak girildiği anda suç tamamlanmaktadır[207]. Hukuka aykırı olarak kalmaya devam etmek suçu ise mütemadi bir suçtur[208]. Temadinin kesildiği anda suç bitmiş olur.

Sistemin bütününe veya bir kısmına hukuka aykırı olarak girmek suç sayılmışsa da kanunda "sistemin bir kısmı" ifadesi tanımlanmamıştır. Ancak, Sanal Ortamda İşlenen Suçlar Sözleşmesi Açıklayıcı Memorandumu'nda yer alan erişim tanımından[209]yola çıkılarak bu eylem ***"****bilgisayar siteminin tamamına ya da bir parçasına (donanım, bileşenler, yüklenen sistemin saklanan verileri, dizinler, trafik ve içerikle ilişkili veriler) girilmesi"*[210] olarak anlaşılabilir[211]. Dolayısıyla bir bilişim sisteminin unsuru niteliğindeki herhangi bir veri

---

205 **Erdoğan,** Bilişim Suçları, s.125; **Koca/Üzülmez,** s.854.

206 **Koca/Üzülmez,** s.854.

207 **Özbek/Doğan/Bacaksız/Tepe,** Özel Hükümler, s.950,951. "Bilişim sistemine girmek", bir bilişim sisteminde bulunan verilerin bir kısmına veya tamamına, fiziken ya da uzaktan başka bir cihaz yoluyla erişilmesidir. Erişimi gerçekleştirmek için gevşek güvenlik önlemlerinden faydalanılabileceği gibi, var olan güvenlik önlemlerindeki boşluklar da kullanılabilir. Ağ üzerinden virüsler (komik resimler, kutlama kartları veya ses ve görüntü dosyaları gibi ekler halinde), truva atı (trojan horse), macro virüsü, solucanlar gibi kullanılarak veya sistemin açık kapıları zorlanarak giriş yapılabilir. Bilgisayar veri ve sistemlerine yapılan izinsiz giriş, aynı zamanda, "bilgisayara tecavüz", "kod kırma" ya da "bilgisayar korsanlığı" olarak da tanımlanmaktadır. Suçun, başkasına ait bilgisayarın açılarak içindeki verilerin görülmesi biçiminde olabileceği gibi, bir ağ aracılığıyla bilişim sisteminde oturum açılması yoluyla da işlenebilir. Girmede, iletişimin kablolu veya kablosuz olması ile mesafenin yakın ve uzak olması arasında da fark yoktur. Bir bilişim sistemine e-posta veya dosya gönderilmesi durumunda, bilişim sistemine girme söz konusu olmayıp yalnızca veri gönderildiğinden, bu durum girme kapsamında düşünülemez. Mağdurun kişisel bilgisayarına ait işletim sistemine bir başka internet kullanıcısının, mağdurun rızası olmaksızın girmesi de suç oluşturacaktır. Yargıtay 8. Ceza Dairesi, 11.03.2015 tarihli ve 2014/29566 E., 2015/13421 K. sayılı kararı www.lexpera.com (E.T:03.07.2019)

208 **Erdoğan,** Bilişim Sistemine Girme ve Kalma Suçu, s.1418.

209 Karagülmez, bizim de katıldığımız şekilde, fiziki bir yeri, alanı anlatan girmek eylemi yerine elektronik yapıdaki bilişim sistemine erişim eyleminin kullanılması gerektiğini düşünmektedir. bkz. **Karagülmez**, s.204.

210 Sanal Ortamda İşlenen Suçlar Sözleşmesi Açıklayıcı Memorandumu, 2. Madde Şerhi http://ozgureralp.av.tr/mevzuat/avrupa-konseyi-siber-suc-sozlesmesi-aciklayici-memorandum-internet-ve-hukuk-platformu-i-v-h-p-cevirisi/ (E.T: 07.11.2018).

211 **Ö. Umut Eker**, Türk Ceza Hukuku'nda Bilişim Suçları Eski TCK Bağlamında Hukukumuzda Yer Alan İlk Düzenlemeler ve 5237 Sayılı Yeni Türk Ceza Kanunu'nun İlgili Hükümlerinin Yorumu, Türkiye Barolar Birliği Dergisi, S: 62, Ocak-Şubat 2006, s.123, http://tbbdergisi.barobirlik.org.tr/m2006-62-196 (E.T: 07.11.2018).

kaynağına hukuka aykırı olarak girilmesi veya kalınması da bilişim sistemine girme suçunu oluşturacaktır[212]. Örneğin, CD-ROM, disket, USB (Universal Serial Bus) bellek aygıtı veya mobil telefonlara giriş de bilişim sistemine girme suçu niteliğinde olacaktır[213].

Sistemin bir kısmına veya tamamına girmek arasında bir fark görülmemektedir[214]. Suçun oluşması için diğer bir unsur olan "*kalmaya devam etme"* eylemi de failin erişim sağlandıktan sonra eylemin ciddiliğini ortaya koyacak ölçüde bulunmasıdır[215]. Bu süre bilişim alanında ileri düzey bilgi sahibi olan fail için kısa olabilirken daha az bilgi ve beceriye sahip olan fail için uzun olabileceğinden yeterli süre ölçüsünün araştırılması ve değerlendirilmesi somut olaya göre değerlendirilmelidir[216].

6698 sayılı Kanun ile yapılan bir diğer değişiklik ise 243'üncü maddeye eklenen 4'üncü fıkradır. Bu değişiklik ile önceki kanunda ve maddenin değişiklik öncesi halinde düzenlenmeyen yeni bir suç düzenlemesi yapılmış ve *"bilişim sisteminin kendi içinde veya bilişim sistemleri arasında gerçekleşen veri nakillerini, sisteme girmeksizin teknik araçlarla hukuka aykırı olarak izlemek"* eylemi yaptırıma bağlanmıştır. Bu düzenlemeye göre bu yeni suç tipinin oluşması için, bilişim sisteminin kendi içinde veya bilişim sistemleri arasında gerçekleşen veri nakillerine yönelik gerçekleştirilmesi, sisteme girilmeksizin gerçekleştirilmesi (teknik araçlarla izleme yöntemi ile) ve hukuka aykırılık bilinci ile gerçekleştirilmesi unsurlarının bir arada olması gerekmektedir.

Kişisel Verilerin Korunması Kanunu Tasarısı Alt Komisyon Raporu'na göre veri izlemesi eylemi "*bilişim sistemlerine herhangi bir müdahalede bulunmaksızın teknik araçlarla bilişim sistemleri arasındaki veri nakillerinin takip edilmesini"* ifade etmektedir[217].

---

212 **Özbek/Doğan/Bacaksız/Tepe,** Özel Hükümler, s.934.

213 **Akbulut,** Bilişim Alanında Suçlar, s.126; **Apiş,** s.61.

214 **Erdoğan,** Bilişim Suçları, s.127; **Yazıcıoğlu**, Hukukumuzda TCK'nın 243'üncü madde kapsamında Bililim Sistemine Girme Eylemi, s.82.

215 **Artuk/Gökcen/Yenidünya,** Türk Ceza Kanunu Şerhi, s.4632, **Erdoğan**, Bilişim Suçları, s.130; **Erdoğan,** Bilişim Sistemine Girme ve Kalma Suçu, s.1374.

216 **Karagülmez,** s.204-205; **Güler,** s.20.

217 117 sayılı Kişisel Verilerin Korunması Kanunu Tasarısı Alt Komisyon Raporu s.25. https://www.tbmm.gov.tr/sirasayi/donem26/yil01/ss117.pdf (E.T. 08.11.2018)

Yine rapora göre *"yasadışı araya girme eylemleri, temelde bilişim sistemlerine girilmeksizin işlenen*" fiillerdendir.

Hukuka aykırı izleme suçu, hareket bakımından icrai bir suçtur zira burada belirli bir amaca yönelen, kişinin isteğine ve iradesine bağlı, dış dünyada etki doğuran, bir şeyi yapmak şeklinde ortaya çıkan bir eylem bulunmaktadır[218]. Netice bakımından ise mütemadi bir suçtur[219]. Sistem içinde veya sistemler arası veri nakillerini teknik araçlarla hukuka aykırı olarak izleme eylemi gerçekleştiği anda suç tamamlanır ancak bitmez[220]. Temadi kesilince yani izleme eylemi bittiğinde suç da biter.

Bu düzenleme Kişisel Verilerin Korunması Kanunu Tasarısı Alt Komisyon Raporu'nda da belirtildiği üzere, Sanal Ortamda İşlenen Suçlarla Mücadele Sözleşmesi'nin 3'üncü Maddesine uyum sağlamak amacıyla getirilmiştir[221]. Sanal Ortamda İşlenen Suçlar Sözleşmesi Açıklayıcı Memorandumu'nda "*teknik yöntemler"* kullanarak müdahale, iletişimin içeriğinin dinlenmesi, denetlenmesi ya da izlenmesi ve verilerin içeriğinin bilgisayar sistemine erişim ve sistemin kullanımı yoluyla doğrudan ya da elektronik gizlice dinleme cihazlarının yardımıyla dolaylı olarak elde edilmesi olarak tanımlanmıştır[222]. Yasadışı izleme sonucu izlenen verilerin kaydedilmesi, ele geçirilmesi ya da özel hayatın gizliliğinin ihlal edilmesi gibi durumlarda TCK'nın 134'üncü maddesi (özel hayatın gizliliğini ihlal), 135'inci maddesi (kişisel verilerin kaydedilmesi), 136'ncı maddesi (verileri hukuka aykırı olarak ele geçirme) de gündeme gelebilecektir[223]. Teknik yöntemler, iletim hatlarına takılan teknik cihazlarla birlikte kablosuz iletişimi elde etmekte ve kaydetmekte kullanılan cihazları da kapsar[224]. Bu yöntemler yazılım, şifre ve kodların kullanımını da

---

218 **Koca/Üzülmez**, s.864.
219 **Dülger**, s.308.
220 **Koca/Üzülmez,** s.864; **Akbulut**, Bilişim Alanında Suçlar, s.168; **Dülger**, s.308.
221 117 sayılı Kişisel Verilerin Korunması Kanunu Tasarısı Alt Komisyon Raporu s.25. https://www.tbmm.gov.tr/sirasayi/donem26/yil01/ss117.pdf (E.T. 08.11.2018).
222 Sanal Ortamda İşlenen Suçlar Sözleşmesi Açıklayıcı Memorandumu Çevirisi https://www.ozgureralp.av.tr/avrupa-konseyi-siber-suc-sozlesmesi-aciklayici-memorandum-internet-ve-hukuk-platformu-i-v-h-p-cevirisi/.
223 **Gül, s**. 66.
224 **Dülger,** s.307.

kapsayabilir[225]. Teknik yöntemler kullanma şartı, gereğinden fazla fiili suç olarak tanımlamaktan kaçınmak için getirilmiş kısıtlayıcı bir şarttır[226].

TCK'nın 243/2'nci maddesinde, hukuka aykırı olarak girilen veya orada kalmaya devam edilen bilişim sisteminin, bedeli karşılığı yararlanılabilen sistemler olması halinde verilecek cezada indirime gidileceği düzenlenmiştir. Ancak, madde ya da madde gerekçesinde bedel karşılığı yararlanılabilen sistemlere ilişkin bir açıklama yapılmamıştır. Bu nitelikli halin uygulanması için eylemi konusunun bilişim sistemi olması ve bu sisteme girişin bir bedelinin olması, failin de bu sisteme bedeli ödemeden girmesi veya kalması gerekmektedir[227].

Maddenin üçüncü fıkrasında, *"bilişim sistemine girme suçunun gerçekleştirilmesi nedeniyle, sistemin içerdiği verilerin yok olması ya da değişmesi"* duruma cezai yaptırım öngörülmüştür.

Hukuka aykırı şekilde bilişim sistemine girme veya sistemde kalma sonucu, sistemdeki verilerin yok olması veya değişmesi halinde bu ağırlaştırıcı nedenin uygulanabilmesi için failin bu kasıtla hareket etmemiş olması ancak TCK'nın 23'üncü maddesi gereği bu netice açısından en azından taksirle hareket etmiş olması gerekir[228]. Failin kastının doğrudan sistemdeki verileri değiştirmek veya yok etmek olduğu hallerde 243'üncü madde değil 244'üncü madde uygulama alanı bulacaktır[229].

Suça ilişkin ağırlaştırıcı nedenin uygulanabilmesi için sistem içerisindeki verilerin yok olması veya değişmesi neticelerinden birinin gerçekleşmesi yeterlidir[230]. Her iki

---

225 **Özbek/Doğan/Bacaksız/Tepe,** s.952.

226 Sanal Ortamda İşlenen Suçlar Sözleşmesi Açıklayıcı Memorandumu, 2. Madde Şerhi http://ozgureralp.av.tr/mevzuat/avrupa-konseyi-siber-suc-sozlesmesi-aciklayici-memorandum-internet-ve-hukuk-platformu-i-v-h-p-cevirisi/ (E.T: 10.11.2018)

227 **Dülger,** s.272; **Erdoğan,** Bilişim Sistemine Girme ve Kalma Suçu, s.1396; **Yaşar/Gökcan/Artuç**, s.6379.

228 **Erdoğan**, Bilişim Suçları, s.153; Dülger, s.265.

229 **Artuk/Gökcen/Yenidünya,** Türk Ceza Kanunu Şerhi, s.4654**; Yazıcıoğlu,** Hukukumuzda TCK'nın 243. Madde Kapsamında Bilişim Sistemine Girme Eylemi, s.85; **Karagülmez**, s.212; **Esen**, 630.

230 **Karagülmez,** s.212; **Dülger**, s.272; **Erdoğan**, Bilişim Sistemine Girme ve Kalma Suçu, s.1402.

neticenin bir arada gerçekleşmesi sonucu değiştirmemekle birlikte cezanın bireyselleştirilmesi konusunda önem taşımaktadır.

06.04.2016 tarihinden önce gerçekleştirilen eylemler bakımından hukuka aykırı olarak bilişim sistemine anlık giriş çıkış sonucu meydana gelen verilerin yok olması ve değişmesi neticesi, başlangıç eylemini suç olarak nitelendirilmediğinden kişiyi sorumluluk altına sokmayacaktır[231]. Ancak 6698 Sayılı Kanun ile yapılan değişiklik sonucu sisteme hukuka aykırı giriş çıkışlar da cezai yaptırıma bağlandığından, ağırlaşmış netice bakımından sorumluluk doğmaktadır.

TCK'nın 243'üncü maddesinde düzenlenen suçun manevi unsuru kast olup taksirle işlenemez[232]. 6698 Sayılı Kanun ile yapılan değişiklik öncesi maddenin birinci fıkrasında öngörülen suçun gerçekleşmesi için failin hukuka aykırı olarak sisteme girmesi ve kalmaya devam etmesi gerektiğinden eylemlerin tamamı bakımından kast unsurunun bulunması gerekmektedir[233]. Failin tesadüfen sisteme girdikten sonra sistemin sınırlandığını fark etmesine rağmen bilerek ve isteyerek kalmaya devam etmesi halinde de tipiklik açısından suç oluşmayacaktır[234]. Yine aynı şekilde hukuka aykırı olduğunu bilerek ve isteyerek bilişim sistemine ani giriş çıkış yapması halinde de madde metninde öngörülen kalmaya devam etme unsuru gerçekleşmediğinden suç oluşmayacaktır[235].

6698 Sayılı Kanun ile yapılan değişiklik sonrası ise ani giriş çıkış şeklinde dahi olsa kasten ve hukuka aykırı olarak bilişim sistemine girme halinde suç oluşacaktır[236]. Yine tesadüfen giriş yapıldıktan sonra kasıtlı olarak kalmaya devam etme halinde de suç oluşmuş olacaktır[237].

---

231 **Erdoğan**, Bilişim Suçları, s.157.
232 **Kurt,** s150; **Karagülmez** s.212; **Yenidünya**, s.1037; **Koca/Üzülmez,** s.856; **Akbulut**, Bilişim Alanında Suçlar, s.36.
233 **Erdoğa**n, Bilişim Suçları, s.156; **Meran**, s.567.
234 **Erdoğan**, Bilişim Suçları s.157; **Erdoğan,** Bilişim Sistemine Girme ve Kalma Suçu, s.1406.
235 **Koca/Üzülmez**, s.856.
236 **Dülger;** s.259.
237 **Koca/Üzülmez**, s.856, 857; **Özbek/Doğan/Bacaksız/Tepe,** Özel Hükümler, s.951.

Maddenin üçüncü fıkrasında yer alan ağırlaştırıcı halin uygulanabilmesi için de ifade etmiş olduğumuz gibi failin gerçekleşen netice bakımından taksirinin bulunması gerekmektedir[238]. Taksir unsurunun bulunmaması halinde TCK'nın 23'üncü maddesi gereği gerçekleşen sonuçtan sorumlu tutulamayacak, kastının bulunması halinde ise 244'üncü madde uygulama alanı bulacaktır[239].

Bilişim sistemine girme suçu maddenin 6698 sayılı Kanun ile değiştirilmesinden önce de sonra da bilişim sistemlerine girerek işlenmesi zorunlu olan diğer bilişim suçları için geçit suçu niteliğindedir[240]. Bu nedenle TCK'nın 244'üncü maddesinde düzenlenen sistemi engelleme, bozma ve yok etme suçunda, bilişim sistemine girme eylemi geçit olma özelliği taşıdığından fail sadece final suçtan cezalandırılmalıdır[241].

15. Banka ve Kredi Kartlarının Kötüye Kullanılması Suçu (TCK m. 245)

Önceki bölümlerde de belirtmiş olduğumuz gibi, teknoloji geliştikçe hayatımız da bununla doğru orantılı olarak kolaylaşmaktadır. Ancak bu gelişmeler kötü amaçlarla kullanıldığında, sağlamış olduğu faydalar kadar hatta daha da fazla zararlara yol açabilmektedir[242].

Bilişim suçlarının en yaygın görülen türlerinden biri de yine hemen hemen herkesin sahip olduğu ve yaygın olarak kullandığı banka ve kredi kartlarının kötüye kullanılmasıdır. Banka veya kredi kartlarının kötüye kullanılması, işlenebilmesi için bilişim sistemine ihtiyaç duyulan bir suç olması nedeniyle, bilişim suçu türüdür[243]. Maddede, bir bilişim sistemine bağlı olarak çalışan ve bilişim temelli bir faaliyetin sonucu olarak fonksiyon gösteren banka

---

238 **Dülger,** s.278; Ağırlaşmış neticenin taksirle işlenemeyeceğine ilişkin görüş için bkz. **Özbek/Doğan/Bacaksız/Tepe,** Özel Hükümler, s.955.

239 **Yenidünya**, s. 1041.

240 **Artuk/Gökcen/Yenidünya,** Türk Ceza Kanunu Şerhi, s.4655; **Erdoğan**, Bilişim Suçları, s.170; **Yenidünya,** Bilişim Sistemine Hukuka Aykırı Erişim Suçu (TCK m.243) s. 1039.

241 **Yazıcıoğlu,** Hukukumuzda TCK'nın 243. Madde Kapsamında Bilişim Sistemine Girme Eylemi, s.86, **Erdoğan**, Bilişim Suçları, s.171; **Koca/Üzülmez,** s.861. 243 ve 244'üncü maddeler arasındaki içtima ilişkisi, 244'üncü maddeye ilişkin değerlendirmelerin yapıldığı ikinci bölümde detaylı olarak ele alınmıştır.

242 **Çiçek**, s.13; **Ekim, s**.1.

243 **Damla Ermeydan,** Türk Ceza Kanunu'nda Bilişim Suçları, Yayımlanmamış Yüksek Lisans Tezi, Çağ Üniversitesi SBE, Mersin, 2018, s.70 https://tez.yok.gov.tr/UlusalTezMerkezi/ (E.T: 25.11.2018).

ve kredi kartlarıyla işlenen suçlar kastedilmektedir[244]. 765 sayılı TCK'dan farklı olarak 5237 sayılı Kanunda ilk kez, doğrudan banka ve kredi kartlarının kullanımı suç olarak düzenlenmiştir.[245]

Maddenin birinci fıkrasında gerçek ve geçerli bir kartın, sahibinin veya verilmesi gereken kişinin rızası olmaksızın kullanılması söz konusudur. İkinci fıkrasında, gerçek bir kart veya kart numarasının sahtecilik yoluyla yeniden üretilmesi, satılması, devredilmesi, satın alınması veya kabul edilmesi eylemleri yaptırım altına alınmıştır. Üçüncü fıkrasında ise sahte olarak üretilen yani gerçek olmayan kart ile gerçek olduğu halde birtakım müdahaleler sonucu sahte hale getirilen kartın kullanılması sonucunda yarar sağlanması eylemi yaptırıma bağlanmıştır.

Maddenin dördüncü fıkrasında şahsi cezasızlık sebebi yer almakla, birinci fıkrada yer alan suçların yani gerçek ve geçerli kartın sahibinin veya verilmesi gereken kişinin rızası dışında kullanma eylemlerin fıkrada sayılan akrabalara karşı işlenmesi durumunda ilgili akrabaya ceza verilmeyeceği düzenlenmiştir.

---

244 **Şaban Cankat Taşkın,** Bilişim Hukuku Uluslararası Anlaşmazlıklar, Türkiye Barolar Birliği Dergisi, S: 85, 2009, s. 335. http://tbbdergisi.barobirlik.org.tr/m2009-85-571 (E.T: 25.11.2018).

245 Bu madde de ilk düzenlemeden sonra iki kere değişikliğe uğramış olup 5377 sayılı Kanun'un 27.maddesi ve 5560 sayılı Kanun'un 11'inci maddesi ile değiştirilmiş son hali şu şekildedir; *"(1) Başkasına ait bir banka veya kredi kartını, her ne suretle olursa olsun ele geçiren veya elinde bulunduran kimse, kart sahibinin veya kartın kendisine verilmesi gereken kişinin rızası olmaksızın bunu kullanarak veya kullandırtarak kendisine veya başkasına yarar sağlarsa, üç yıldan altı yıla kadar hapis ve beş bin güne kadar adlî para cezası ile cezalandırılır.*
(2) Başkalarına ait banka hesaplarıyla ilişkilendirilerek sahte banka veya kredi kartı üreten, satan, devreden, satın alan veya kabul eden kişi üç yıldan yedi yıla kadar hapis ve on bin güne kadar adlî para cezası ile cezalandırılır.
(3) Sahte oluşturulan veya üzerinde sahtecilik yapılan bir banka veya kredi kartını kullanmak suretiyle kendisine veya başkasına yarar sağlayan kişi, fiil daha ağır cezayı gerektiren başka bir suç oluşturmadığı takdirde, dört yıldan sekiz yıla kadar hapis ve beş bin güne kadar adlî para cezası ile cezalandırılır.
(4) Birinci fıkrada yer alan suçun;
a) Haklarında ayrılık kararı verilmemiş eşlerden birinin,
b) Üstsoy veya altsoyunun veya bu derecede kayın hısımlarından birinin veya evlat edinen veya evlâtlığın,
c) Aynı konutta beraber yaşayan kardeşlerden birinin,
Zararına olarak işlenmesi hâlinde, ilgili akraba hakkında cezaya hükmolunmaz.
(5) Birinci fıkra kapsamına giren fiillerle ilgili olarak bu Kanunun malvarlığına karşı suçlara ilişkin etkin pişmanlık hükümleri uygulanır." Beşinci fıkra 6/12/2006 tarihli 5560 sayılı Kanunun 11'inci maddesi ile eklenmiştir.

Maddeye sonradan eklenen beşinci fıkrada ise, yine birinci fıkrada yer alan suçlar bakımından Kanun'un 168'inci maddesinde yer alan, malvarlığına karşı suçlara ilişkin etkin pişmanlık hükümlerinin uygulanacağı düzenlenmiştir.

Maddenin birinci fıkrası ile başkasına ait banka veya kredi kartını ele geçiren veya elinde bulunduran kişinin, kart sahibinin veya kartın kendisine verilmesi gereken kişinin rızası olmaksızın bunu kullanarak veya başkasına kullandırtarak, kendisine veya başkasına yarar sağlaması yaptırıma bağlanmıştır. Burada kişilerin ya da kurumların malvarlıklarının yanı sıra bankacılık sistemi, ticari yaşam, kamu güveni ve bilişim alanı da korunmak istenmiştir[246].

Suçun oluşması için birden fazla hareketin gerçekleşmesi gerekmektedir[247]. Bunlardan biri başkalarına ait banka veya kredi kartının ele geçirilmesi ya da elde bulundurulması diğeri de bu suretle kendisine ya da bir başkasına yarar sağlanmasıdır. Bu nedenle suç, çok hareketli suçlardan birleşik hareketli suç niteliğindedir[248]. Suçun oluşumu için iki hareketin de gerçekleştirilmesi gerekir. Ayrıca, faydanın sağlanması neticesinin gerçekleşmesine yönelik her türlü eylem suçu oluşturacağından, kartın ne şekilde kullanılacağı bakımından suç serbest hareketli bir suçtur[249]. Yine madde metninde "*kullanmak*" ve "*kullandırtmak*" ibareleri yer aldığından icrai bir suçtur ve ihmali hareketle işlenememektedir[250].

Burada öncelikle başkasına ait banka kartının "her ne suretle olursa olsun ele geçirilmesi veya elde bulundurulması" üzerinde durulmalıdır. Ele geçirme, başkalarına ait

---

246 **Yavuz Erdoğan,** Türk Ceza Kanunu'nda Banka ve Kredi Kartlarının Kötüye Kullanılması Suçu, Legal Hukuk Dergisi, C:9, S:107, 2011, s.4279; **Ketizmen,** s.187.

247 **Koca/Üzülmez**, s.891; **Erdoğan,** Banka ve Kredi Kartlarının Kötüye Kullanılması, s.4281.

248 **Koca/Üzülmez,** s.891; **Koray Doğan,** Bilişim Suçları ve Yeni Türk Ceza Kanunu, Hukuk ve Adalet Eleştirel Hukuk Dergisi Y:2, S:6-7, 2005, s.310.

249 **Veli Özer Özbek,** Banka veya Kredi Kartlarının Kötüye Kullanılması Suçu (TCK m.245), Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi, C:9, Özel Sayı, 2007, s.1034; **Cengiz Apaydın,** Başkalarına Ait Banka Hesaplarıyla İlişkilendirerek Sahte Banka veya Kredi Kartını Üretmek, Satmak, Devretmek, Satın almak veya Kabul Etmek, Terazi Hukuk Dergisi, C:12, S:127, 2017, s.47.

250 **Eylem Baş,** Banka ve Kredi Kartlarının Kötüye Kullanılması Yüksek Lisans Tezi, Ankara: Ankara Üniversitesi SBE, 2011, s.158, https://tez.yok.gov.tr/UlusalTezMerkezi/ (E.T: 24.11.2018); **Erdoğan,** Banka ve Kredi Kartlarının Kötüye Kullanılması, s.4281.

banka veya kredi kartının, habersizce veya yetkisiz olarak ya da bularak veya başka bir şekilde ele geçirilmesi anlamına gelmektedir[251]. Burada kartın ele geçiriliş biçimi önem taşımamaktadır.

Elinde bulundurmak ise kartın, fail tarafından aktif bir harekette bulunulmaksızın, sözleşme veya görev gereği ya da kart hamilinin iradesi sonucu failin elinde bulunmasıdır.[252] 5464 sayılı Banka Kartları Ve Kredi Kartları Kanununa[253] göre kredi kartı; nakit kullanımı gerekmeksizin mal ve hizmet alımı veya nakit çekme olanağı sağlayan basılı kartı veya fizikî varlığı bulunmaya n kart numarasını ifade ettiğinden fiziki varlığı ele geçirilmemiş olmakla birlikte kart bilgilerinin elde edilmesi suretiyle haksız yarar elde edilmesi durumunda da kredi kartlarının kötüye kullanılması suçu oluşur[254].

Üzerinde durulması gereken diğer bir konu ise *"kart sahibinin veya kartın kendisine verilmesi gereken kişinin rızası olmaksızın"* ifadesidir. Kart sahibi ve kartın kendisine verilmesi gereken kişi; banka tarafından adına kart düzenlenen kişiyi ifade etmekle birlikte, kartın kendisine verilmesi gereken kişi ifadesinde kullanıma hazır olan kart üretildikten sonra sahibine teslim aşamasında olması ya da kaybedilen kartın başkası tarafından bulunması gibi durumlar söz konusudur[255].

Suçun meydana gelmesi için ele geçirilen veya elde bulunan kredi kartının kullanılması veya kullandırtılması gerekmektedir. Burada "*kullanarak*" kavramı, failin kartı bizzat haksız yere kullanmasını, "*kullandırtarak*" kavramı ise kartı ele geçirin ve elinde bulunduran kişinin başkasına bu kartı kullandırtma fiilini ifade etmektedir[256]. Kanunda hangi şekillerde kullanılacağı veya kullandırtılacağı öngörülmediğinden, haksız yarar sağlama

---

251 **Karagülmez**, s. 290.

252 **Mehmet Emre Yıldız**, Banka ve Kredi Kartlarının Kötüye Kullanılması Suçu, İzmir: Dokuz Eylül Üniversitesi SBE, 2011, s.60-61.

253 5464 sayılı Banka Kartları ve Kredi Kartları Kanunu, 30.05.2007 tarihli 26537 sayılı Resmi Gazete'de yayımlanmış ve yayımı tarihinde yürürlüğe girmiştir.

254 **Dülger**, s.478; **Koca/Üzülmez**, s.893.

255 **Karagülmez**, s.291; **Erdoğan,** Banka ve Kredi Kartlarının Kötüye Kullanılması, s.4283; **Koca/Üzülmez,** s.892; **İshak Tufanoğlu,** Banka veya Kredi Kartlarının Kötüye Kullanılması Suçu, Yayımlanmamış Yüksek Lisans Tezi, İstanbul Üniversitesi SBE, İstanbul, 2014, s.25 https://tez.yok.gov.tr/UlusalTezMerkezi/ (E.T: 25.11.2018).

256 **Karagülmez**, s.291; **Erdoğan,** Banka ve Kredi Kartlarının Kötüye Kullanılması, s.4281; **Pallı**, s.180.

neticesini ortaya çıkaracak her türlü eylem kullanma veya kullandırtma kapsamında değerlendirilebilir[257].

Suçun tamamlanması için gereken son hareket kişinin kendisine veya başkasına haksız yarar sağlamasıdır[258]. Yani suçun oluşumu bakımından, haksız yarar sağlama neticesinin gerçekleşmesi aranmakta ancak bu yararı kimin elde ettiği önem taşımamaktadır. Sağlanan bu yarar maddi niteliktedir[259].

245'inci maddenin ikinci fıkrasında sahte banka veya kredi kartı üretilmesi, satılması, devredilmesi, satın alınması veya kabul edilmesi ayrı bir suç olarak düzenlenmiştir. Banka veya kredi kartlar tamamen sahte olarak, haksız olarak ele geçirilen banka veya kredi kartı numara ve şifrelerini para çekme eylemlerinde kullanılan boş manyetik bantlı beyaz kartlara yüklenmesi işleminde kullanılan "*Reader&Encoder*" isimli cihaz vasıtasıyla boş beyaz kartlar üzerindeki manyetik şerit üzerine kopyalama gibi işlemlerle üretilebileceği gibi, "*Embosser*" adı verilen bir başka cihazla kart üzerindeki ismi değiştirme gibi gerçek kartlar üzerinde işlem yapılarak da sahteleştirilme gerçekleştirilebilir[260]. Bunların yanı sıra sahte olarak, internette kullanılmak üzere oluşturulan ve fiziksel varlığı olmayan sanal kartların üretimi de bu madde kapsamında değerlendirilmelidir[261].

Maddede yer alan seçimlik suçlardan biri olan başkalarına ait banka veya kredi kartıyla ilişkilendirilerek sahte banka veya kredi kartı üretilmesi hareketi, *"başkalarına ait banka veya kredi kartıyla ilişkilendirmek"* ve *"sahte olarak üretmek"* olarak iki farklı hareketten oluştuğu için birleşik hareketli bir suçtur. Suçun oluşması için bu iki hareketin birlikte yapılması gerekmektedir[262].

---

257 **Erdoğan,** Banka ve Kredi Kartlarının Kötüye Kullanılması, s.4280.
258 **Pallı**, 190; **Özbek**, Banka veya Kredi Kartlarının Kötüye Kullanılması Suçu, s.1034.
259 **Özbek/Doğan/Bacaksız/Tepe,** Özel Hükümler, s.986.
260 **Mesut Budak**, Banka ve Kredi Kartlarının Kötüye Kullanılması Suçu Yüksek Lisans Tezi**,** Polis Akademisi Başkanlığı Güvenlik Bilimleri Enstitüsü, 2009, s.69, https://tez.yok.gov.tr/UlusalTezMerkezi/ (E.T: 25.11.2018).
261 **Dülger**, s.488; **Koca/Üzülmez,** s.904; **Erdoğan,** Banka ve Kredi Kartlarının Kötüye Kullanılması, s.4309.
262 **Dülger**, s.487; **Erdoğan,** Banka ve Kredi Kartlarının Kötüye Kullanılması, s.4310.

TCK'nın 245/2'nci maddesinde yer alan suçun tamamlanabilmesi için haksız yarar elde edilmesi aranmamaktadır[263]. Maddede öngörülen hareketlerden birinin gerçekleştirilmesi halinde suç gerçekleşecektir. Bu eylemler sonucu haksız yararın elde edilmesi durumunda 245/3'üncü maddede yer alan suç oluşacaktır[264].

Üretmek eylemi sözlükte, "*oluşturmak, yaratmak, meydana getirmek"* şeklinde tanımlanmıştır[265]. Bu suç açısından değerlendirildiğinde ise, bir banka veya kredi kartının, herhangi bir şekilde başkasına ait bir hesapla ilişkili olarak gerçeğinden ayrı olarak ilk kez oluşturulması, çıkarılması veya çoğaltılması veya kimlik denetimini aşmak için gerçek bir kartın dış bilgilerini failin kendi kimlik bilgilerine göre değiştirilmesi anlamına gelmektedir[266].

Satmak eylemi, "*bir değer karşılığında bir malı alıcıya vermek"* şeklinde tanımlanmış olup[267], suç kapsamında, kartın bir bedel karşılığında alıcıya verilmesini ifade etmektedir[268]. Burada satma eylemini gerçekleştiren kişinin üretici olması gerekmez[269]. Devretmek eylemi ise, "*bir malın mülkiyetini, bir mal üzerindeki hakkı başkasına geçirmek"* anlamına gelmekte[270] ve kartın, karşılık aranmaksızın alıcıya verilmesini ifade etmektedir[271]. Devir işleminin belli bir süre için ya da süresiz yapılması önem taşımamaktadır. Satın almak eylemi, kartın bedel ödenmek suretiyle elde edilmesi anlamına gelmektedir[272]. Böyle bir durumda hem satın alan hem de satan kişi suçu işlemiş olur[273]. Kabul etmek ise belli bir süre

---

263 **Özbek,** Banka veya Kredi Kartlarının Kötüye Kullanılması Suçu, s.1031.
264 **Yaycı,** s.112; **Özbek,** Banka veya Kredi Kartlarının Kötüye Kullanılması Suçu, s. 1048.
265 http://www.tdk.gov.tr/ (E.T: 02.03.2019).
266 **Erdoğan,** Bilişim Suçları, s.335; **Erdoğan,** Banka ve Kredi Kartlarının Kötüye Kullanılması, s.4310; **Pallı,** s.197.
267 http://www.tdk.gov.tr/ (E.T: 02.03.2019).
268 **Erdoğan,** Bilişim Suçları, s.336.
269 **Pallı,** s.197,198.
270 http://www.tdk.gov.tr/ (E.T: 02.03.2019).
271 **Erdoğan,** Banka ve Kredi Kartlarının Kötüye Kullanılması, s.4311; **Özbek,** Banka veya Kredi Kartlarının Kötüye Kullanılması Suçu, s.1047.
272 **Erdoğan,** Bilişim Suçları, s.336.
273 **Karagülmez,** s.290.

için ya da süresiz olarak bedel ödenmeksizin alınmasını ifade eder[274]. Yine bu durumda da hem devreden hem de kabul eden suçu işlemiş olur[275].

5464 sayılı BKKKK'nın "*izinsiz kart çıkarma"* başlıklı 38'inci maddesinde de kanunda belirtilen izinleri almaksızın kartlı sistem kuran, kredi kartı çıkaran veya üye işyeri anlaşması yapan veya ticaret unvanları, her türlü belgeleri, ilân ve reklamları veya kamuoyuna yaptıkları açıklamalarda bu işlerle uğraştıkları izlenimini yaratacak söz ve deyimleri kullanan gerçek kişiler ile tüzel kişilerin görevlilerinin cezalandırılacağı öngörülmüştür. Dolayısıyla failin sahte banka veya kredi kartı üretimi, tek fiille iki farklı kanunda yer alan suçu oluşturduğundan fikri içtima kuralları dahilinde en ağır cezayı gerektiren suçtan dolayı sorumluluğuna gidilecektir[276].

245'inci maddenin üçüncü fıkrasında, sahte oluşturulan veya üzerinde sahtecilik yapılan bir banka veya kredi kartını kullanmak suretiyle kendisine veya başkasına yarar sağlayan kişinin cezalandırılacağı öngörülmüştür. Burada sahte oluşturulan kartın kullanılması ve bu kullanım sonucu haksız yarar sağlama hareketleri birleşik hareketli suç olarak düzenlenmiştir ve suçun oluşması için iki hareketin de bir arada bulunması gerekmektedir[277]. Ancak maddede ne şekilde kullanılması gerektiği yer almadığından serbest hareketli bir suçtur. Haksız yarar sağlayan her türlü kullanım suç oluşturacaktır[278].

Maddede yer alan "*sahte oluşturulan*" ifadesi, sadece sahte üretilen kartları değil aynı zamanda gerçekdışı belgelerle banka görevlilerine sahte kredi veya banka kartı oluşturulmasını da kapsamaktadır[279].

---

274 **Erdoğan,** Banka ve Kredi Kartlarının Kötüye Kullanılması Suçu, s.4311; **Özbek,** Banka veya Kredi Kartlarının Kötüye Kullanılması Suçu, s.1047.

275 **Pallı,** s.198.

276 **Artuk/Gökcen/Yenidünya,** Özel Hükümler, s.717

277 **Mesut Orta,** Bilişim Suçları ve Elektronik Delillerin Toplanması, Muhafazası, Değerlendirilmesi, Sunulması (Adli Bilişim), Yetkin Yayınları, Ankara, 2015, s.105.

278 **Erdoğan,** Banka ve Kredi Kartlarının Kötüye Kullanılması, s.4321; **Veli Özer Özbek,** Banka veya Kredi Kartlarının Kötüye Kullanılması Suçu (TCK m.245), Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi, C:9, Özel Sayı, 2007, s.1053.

279 **Dülger**, s.494.

Yine suçun oluşumu bakımından, haksız yarar sağlama neticesinin gerçekleşmesi gerekmekte ancak bu yararı kimin elde ettiği önem taşımamaktadır. Sağlanan bu yarar maddi niteliktedir[280]. Suçun tamamlanması için failin mutlaka elde ettiği yarar üzerinde fiili egemenlik kurması gerekmez yani fail sahte kart aracılığıyla hesabına para aktardığında yarar sağlanmış olduğundan ayrıca bu parayı çekmesi gerekmemektedir[281].

Günümüzde gerek internet bankacılığı sırasında gerekse doğrudan internet üzerinden alışveriş yaparken banka veya kredi kartı üzerinde yer alan bilgiler kullanılmaktadır. Bu durumda kart bilgilerinin sahibinin rızası olmaksızın kullanılarak haksız kazanç elde edilmesi halinde TCK'nın 244'üncü maddesinin mi yoksa 245'inci maddesinin mi uygulanması gerektiği sorunu ortaya çıkacaktır[282].

Dülger bu konudaki görüşünü

"ister kart fiziksel olarak ATM cihazına sokularak kullanılsın ister fiziksel olarak ele geçirilen kartın üzerindeki numaralar kullanılsın, isterse de fiziksel olarak kart ele geçirilmeden karta ait bilgi ve numaraların ele geçirilmesiyle kullanılsın, sonuçta bir haksız yarar elde ediliyorsa 245/1. maddenin uygulanması gerekir."

şeklinde ifade etmiştir[283].

Özbek'e göre ise;

"kart bizatihi kullanılmadan sadece üzerindeki bilgilerden yararlanılarak kartın kullanılması ya da kullandırılması olanaklı hale gelmektedir. Bu halde söz konusu bilgilerin sahibinin rızası olmaksızın kullanılması halinde kanımızca m.244/2 ve 3 düşünülmelidir. Gerçekten bu durumda artık bilişim sistemindeki bir verinin gönderilmesi söz konusudur. Bu fiil bir banka ya da kredi kurumuna ait bilişim sistemi üzerinde gerçekleştiğinden m.244/3 uygulanacaktır."

---

280 **Erdoğan,** Banka ve Kredi Kartlarının Kötüye Kullanılması, s.4321; **Özbek,** Banka veya Kredi Kartlarının Kötüye Kullanılması Suçu, s.1054.

281 **Erdoğan,** Bilişim Suçları, s.349.

282 **Erdoğan,** Bilişim Suçları, s.125.

283 **Dülger,** s.377. Benzer görüş için bkz. **Karagülmez**, s.300.

5664 sayılı BKKK'nın üçüncü maddesinde yer alan kredi kartı tanımına göre, bu kartın fiziki varlığının bulunması zorunlu değildir. Yani, nakit para kullanımını gerektirmeyen, mal ve hizmet alımı veya nakit çekme olanağı sağlayan kart numaraları da kredi kartı olarak kabul edilmektedir. Dolayısıyla bu kart numaralarının kullanılarak haksız bir yarar elde edilmesi durumunda kredi kartının kötüye kullanımı söz konusu olacaktır. Her ne kadar suç bilişim sistemleri aracılığıyla işlenmiş olsa da TCK'nın 245'inci maddesinde düzenlenen banka veya kredi kartıyla yarar sağlama suçu 244'üncü maddenin dördüncü fıkrasında yer alan bilişim sistemi aracılığıyla yarar sağlama suçuna göre özel bir düzenleme olduğundan ve 244'üncü maddenin dördüncü fıkrası tali norm olarak düzenlendiğinden 245'inci maddeden hüküm verilecektir[284].

---

[284] *"Katılana ait kredi kartı bilgilerini kullanarak www.j...net sitesinden kontör satın alma şeklinde gerçekleşen eylemin, TCKnun 245/1. madde ve fıkrasında düzenlenen suçu oluşturacağı gözetilmeden, yazılı biçimde aynı yasanın 244/4. madde ve fıkrası uyarınca hüküm kurulması bozmayı gerektirmiştir."* **Yargıtay 8. Ceza Dairesi, 04.06.2014 tarihli ve 2014/760 E., 2014/13819 K. sayılı kararı**. *"TCKnun 245/1. maddesindeki suçun oluşabilmesi için haksız olarak ele geçirilen banka veya kredi kartının ya da kart bilgilerinin kullanılması suretiyle haksız menfaat temin edilmesi ya da engel nedenlerle menfaatin temin edilemeyerek suçun teşebbüs aşamasında kalması gerektiği, kartın hukuka aykırı olarak ele geçirilmesi eyleminin ise ayrı bir suçu oluşturacağı cihetle; sanığın hukuka aykırı olarak ele geçirdiği kartla ATM'den birden çok kez para çekmesi şeklinde gerçekleşen eyleminin TCK.nun 245/1-5 ve 43. maddeleri kapsamında değerlendirilmesi gerektiği gözetilmeden, yazılı şekilde hüküm kurulması bozmayı gerektirmiştir"* **Yargıtay 8. Ceza Dairesi, 05.06.2014 tarihli ve 2013/12670 E., 2014/13932 K. sayılı kararı.** *"5464 sayılı Banka Kartları ve Kredi Kartları Kanunu'nun 3/e maddesi uyarınca, "kredi kartının, nakit kullanımı gerekmeksizin mal ve hizmet alımı veya nakit çekme olanağı sağlayan basılı kartı veya fiziki varlığı bulunmayankart numarasını" ifade etmesi ve sanıklar Ergin, Erkan ve Elveda'nın yakınına ait kredi kartını fiziki olarak ele geçirmeden sadece kredi kartı numarasını kullanarak bilişim sistemi üzerihden kontör satın alınması ve aynı sistem üzerinden başkalarına kontörlerin satılması eylemleri nedeniyle dava açıldığının anlaşılması karşısında; fiilin 5237 sayılı TCK'nın 245/1 ve 43. maddelerinde öngörülen zincirleme suretiyle banka ve kredi kartlarının kötüye kullanılması suçunu oluşturacağı…"* **Yargıtay 11. Ceza Dairesi, 17.09.2008 tarihli ve 2008/12914 E., 2008/8887 K. sayılı kararı.** *"Başkasına ait kredi kartının kötüye kullanılması suretiyle yarar sağlama suçunun oluşabilmesi için kartın fiziken kullanımı gerekmeyip kart bilgilerinin kullanılması yeterli olduğu cihetle; katılana ait kredi kartı bilgileri ile internet üzerinden değişik tarihlerde birden çok kez alışveriş yapan sanığın eylemine uyan TCK.nun 245/1, 43 madde ve fıkraları gereğince cezalandırılması gerektiği gözetilmeden, yazılı şekilde bilişim sisteminin kullanılması suretiyle hırsızlık suçundan hüküm kurulması…"* **Yargıtay 8. Ceza Dairesi, 05.05.2014 tarihli ve 2013/6328 E., 2014/11449 K. sayılı kararı**. *"Başkasına ait kredi kartının kötüye kullanılması suretiyle yarar sağlama suçunun oluşabilmesi için kartın fiziken kullanımı gerekmeyip kart bilgilerinin kullanılması yeterli olduğu ve mağdurlardan Mehmet'e ait kart bilgilerini kullandığına ilişkin bir iddia bulunmadığı gibi kullanmaya yönelik herhangi bir icrai haretinin gerçekleşmemiş olduğu cihetle; oluşturduğu internet sitesine kontur satın almak üzere giren mağdurların kredi kartı bilgilerini elde edip elektronik posta adresine kaydederek mağdurlardan K.. S..'nın kredi kartı bilgileri ile internet üzerinden değişik tarihlerde birden çok kez kontur alışverişi yapan sanığın eyleminin zincirleme olarak başkasına ait kredi kartının kötüye kullanılması suretiyle yarar sağlama ve yine zincirleme olarak kişisel verilerin kaydedilmesi suçlarına uyar nitelikte olduğu gözetilmeden mağdur Kezban'a yönelik TCK.nun 245/1, 43, ayrıca her iki mağdura yönelik olarak da 135, 43 madde ve fıkraları uyarınca cezalandırılması yerine yazılı şekilde TCK.nun 244/4 ve 43. ve 244/4, 35 madde ve fıkralarından hüküm kurulması bozmayı gerektirmiştir."* **Yargıtay 8. Ceza Dairesi, 07.05.2014 tarihli ve 2013/11684 E., 2014/11750 K. sayılı kararı.**

16. Yasak Cihaz ve Programlar (TCK m. 245/A)

Bilişim teknolojilerindeki gelişmeler neticesinde bilişim sistemlerinin insan hayatının vazgeçilmez bir parçası olması, hayatı kolaylaştırmanın yanı sıra, kötüye kullanılması sonucunda kişilerin haklarının ihlal edilmesi, maddi ve manevi zararlar verilmesi, bilgi sistemlerine yetkisiz girilerek verilerin çalınması gibi eylemlerle ceza hukukunda yeni suçların oluşmasına yol açmıştır[285]. Bilişim suçları da bilişimin kendisi gibi sürekli ve hızlı şekilde değişmekte, devamlı olarak değişen ve sayısı artan birçok değişik araçla işlenebilmektedir[286]. Bu suçlar herhangi bir araç kullanmadan işlenebiliyor olsa da, bilişim suçlarının işlenme sebeplerinden birisi de bu suçları işlemedeki kolaylık olduğundan, çoğu zaman yardımcı araçlar kullanılmaktadır[287]. Bu sebeple kanun koyucu, 6698 sayılı kanun ile yapılan değişiklik ile TCK'da ilk kez, bilişim suçlarının işlenmesini kolaylaştıran programların, cihazların, kodların imal edilmesini, sevk edilmesini, nakledilmesini, depolanmasını, kabul edilmesini, satılmasını, satın alınmasını, başkasına verilmesini veya bulundurmasını da cezalandırmak üzere 245/A maddesini eklemiştir[288].

Bilişim alanında işlenen suçlara ilişkin düzenlemelerin yer aldığı Sanal Ortamda İşlenen Suçlar Sözleşmesi'nin *"Cihazların Kötüye Kullanımı*" başlıklı altıncı maddesinde, taraf devletlerin, kasten ve haksız yere bilişim suçlarının işlenmesi için bilgisayar programı ya da suç işlemek amacıyla tasarlanmış bir cihazın üretimi, satışı, kullanım amacıyla tedarik edilmesi, ithal edilmesi, dağıtımı veya başka şekilde erişilebilir hale getirilmesi eylemlerinin suç olarak düzenleyeceği öngörülmüştür. Dolayısıyla 6698 sayılı Kanun ile yapılan bu

---

285 **İbrahim Korkmaz,** Cihaz, Program, Şifre ve Güvenlik Kodlarının Bilişim Suçlarının İşlenmesi Amacıyla İmal ve Ticareti Suçu, Terazi Hukuk Dergisi, C:13, S:142, 2018, s.46; **Özge Apiş,** Bilişim Sistemine Girme Suçu Bakımından Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama Kopyalama Elkoyma Koruma Tedbiri, Yasama Dergisi, C:12 S:37, 2018, s.50; **Murat Önok**, Avrupa Konseyi Siber Suçlar Sözleşmesi Işığında Siber Suçlarla Mücadelede Uluslararası İşbirliği, s.1230 https://dergipark.org.tr/download/issue-file/517 (E.T:11.06.2018).

286 **Orta,** s.75.

287 **Korkmaz,** s.46.

288 Madde 245/A "*Bir cihazın, bilgisayar programının, şifrenin veya sair güvenlik kodunun; münhasıran bu Bölümde yer alan suçlar ile bilişim sistemlerinin araç olarak kullanılması suretiyle işlenebilen diğer suçların işlenmesi için yapılması veya oluşturulması durumunda, bunları imal eden, ithal eden, sevk eden, nakleden, depolayan, kabul eden, satan, satışa arz eden, satın alan, başkalarına veren veya bulunduran kişi, bir yıldan üç yıla kadar hapis ve beşbin güne kadar adli para cezası ile cezalandırılır."* **Özbek/Doğan/Bacaksız /Tepe**, Özel Hükümler, s.1006.

düzenleme Sanal Ortamda İşlenen Suçlar Sözleşmesi'ne uyum sağlamak amacıyla sözleşmede yer alan maddeye paralel şekilde yapılmıştır. Bununla ilgili olarak Meclis Alt Komisyon Raporu'nda da, sözleşmenin altıncı maddesine uygun şekilde bilişim alanında suç işlenmesini kolaylaştıran cihazların kötüye kullanılmasının cezalandırılmasının istendiği yer almaktadır[289].

Madde metninde yer alan eylemlerin yaptırıma bağlanmasında bilişim suçları ile bilişim sistemleri araç kılınarak işlenen suçlarla etkin ve caydırıcı bir şekilde mücadele amaçlanmıştır[290]. Zira gelişen teknoloji ve yaygın kullanım sebebiyle, suç konusu yazılımların internette bir linkin açılması, bir verinin indirilmesi ya da kaydedilmesi ile bilişim sistemine yerleşebilmekte ve bu sayede, sistemin kendisine ya da sistemde yer alan verilere yönelik birtakım eylemler gerçekleştirerek büyük zararlara neden olabilmektedir. Ayrıca bu tür cihaz ve programların, bilişim sistemlerinin güvenliğini test etmek amacıyla yapılması veya oluşturulması halinde belirtilen suç oluşmayacaktır[291]. Yine failin cezalandırılması için söz konusu cihaz, program, şifre veya güvenlik kodunun suçun işlenmesi bakımından elverişli olması gerekmektedir[292].

Doğrudan veya dolaylı bilişim suçlarının işlenmesinde kullanılmak üzere cihaz, program, şifre ve sair güvenlik kodlarının üretimi ve bunlara erişimin sağlanmasının suç olarak düzenlenmesi önemli bir açığı kapatmış olsa da Özbek/Doğan/Bacaksız/Tepe'nin bizim de katıldığımız görüşüne göre kanun sistematiği açısından madde başlıklarının seçiminde suçun eylem unsurunun ön plana çıkarıldığı gerçeğinden hareketle; *"yasak cihaz ve programlar*" başlığı suçta düzenlenen eylemleri yansıtmadığından yerinde olmamıştır. Dolayısıyla madde başlığının "*suçta kullanılacak cihaz ve programların üretilmesi, yayılması veya bulundurulması"* şeklinde tercih edilmesi isabetli olabilecektir[293].

---

289 **Akbulut,** Bilişim Alanında Suçlar, s.347, **Korkmaz**, s.49.
290 **Koca/Üzülmez**, s.912,913; **Dülger**, s.454.
291 **Koca/Üzülmez**, s.913.
292 **Korkmaz,** s.51; Alt Komisyon Raporu, s.26 **tbmm.gov.tr**›sirasayi/donem26/yil01/ss117.pdf (02.12.2018).
293 **Özbek/Doğan/Bacaksız /Tepe**, Türk Ceza Hukuku Özel Hükümler, Ankara, Seçkin Yayınevi, 2017, s. 1012.

Maddede yer alan düzenlemeye göre; *"bir cihazın, bilgisayar programının, şifrenin veya sair güvenlik kodunun, bilişim alanında suçlar ile bilişim sistemlerinin araç olarak kullanılması suretiyle işlenen diğer suçların işlenmesi için yapılması veya oluşturulması durumunda, bunların imal edilmesi, ithal edilmesi, sevk edilmesi, nakledilmesi, depolanması, kabul edilmesi, satılması, satışa arz edilmesi, satın alınması, başkalarına verilmesi veya bulundurulması"* eylemleri cezai yaptırıma bağlanmıştır[294]. Madde metninde de anlaşılacağı üzere suç, seçimlik hareketli bir suçtur ve belirtilen hareketlerden birinin yapılması ile suç tamamlanır[295]. Bu açıdan suçun oluşması için bir zararın meydana gelmesi beklenmediğinden, soyut tehlike suçudur[296].

Kanaatimizce metinde yer alan yapma kavramı cihazların, oluşturma kavramı ise program, şifre ve sair güvenlik kodlarının meydana getirilmesi anlamında kullanılmıştır.

İmal kavramı, sözlük anlamına göre ham maddeyi işleyip mal üretme anlamına gelmektedir. İmal etmek ise; ham maddeyi işleyerek bir mal üretmek demektir[297]. 245/A kapsamında ise bu kavram; bir cihazın, bilgisayar programının şifrenin veya sair güvenlik kodunun bilişim alanındaki suçlar ile bilişim sistemlerinin araç olarak kullanılması suretiyle işlenen suçların işlenmesini sağlamak amacıyla kullanılmaya elverişli şekilde üretilmesini ifade etmektedir[298].

Cihazların imal edilmesi dışında programlar da imal edilebilir. İmal edilen programlar yeni bir yazılım olabileceği gibi mevcut yazılımın bir türevi de olabilir. Burada önemli husus türev yazılımların kaynak yazılımdan ayırt edilebilir özelliklere sahip olmasıdır[299]. İhmal suretiyle bu suçun işlenmesi mümkün olmadığı için imali oluşturan hareketlerin icra edilmesi gerekir.

---

294 **Akbulut,** Bilişim Alanında Suçlar, s.347.
295 **Korkmaz,** s.51.
296 **Özbek/Doğan/Bacaksız/Tepe**, s.1015.
297 http://tdk.gov.tr/ (E.T: 03.12.2018).
298 **Özbek/ Doğan/Bacaksız/Tepe**, s.1015.
299 **Özbek/ Doğan/Bacaksız/Tepe,** s.1015.

İthal kavramı ise, başka bir ülkeden mal getirme veya satın alma; dış alım anlamına gelmektedir[300]. Bilişim alanındaki suçlar ile bilişim sistemlerinin araç olarak kullanılması suretiyle işlenen suçların işlenmesini sağlamak amacıyla kullanılmaya elverişli cihaz ya da programların yasadışı olarak ülke sınırlar dışından ülke sınırları içerisine sokulması durumunda suç gerçekleşmiş olacaktır[301]. Şifre ve sair güvenlik kodlarının da taşınabilir bellek, cd, hafıza kartı gibi veri taşıyıcılarla ülke dışından ülke sınırları içerisine sokulması durumunda da suç oluşmaktadır[302].

İthal suçunun oluşması bakımından, suç konusunun ülkeye hangi yolla sokulduğu önem taşımamaktadır.[303] Yine suçun oluşumu bakımından failin kastının, bilişim suçlarının işlenmesini sağlamak amacıyla üretilmiş cihaz, bilgisayar programı, şifre ve sair güvenlik kodunun ülkeye getirmek olmalıdır[304]. Failin kastının suç konusunu ülkeye sokma kastının belirlenemediği transit geçişlerde, nakletme suçu söz konusu olabilecektir[305]. Yine bu hareket de ihmali olarak gerçekleştirilememektedir.

Sevk etme; göndermek anlamına gelmektedir[306]. Maddedeki anlamı itibariyle bir cihazın, bilgisayar programının, şifrenin veya sair güvenlik kodunun, bilişim alanında suçlar ile bilişim sistemlerinin araç olarak kullanılması suretiyle işlenen diğer suçların işlenmesi için oluşturulduğu yerden ya da bulunduğu yerden başka bir yere bir kişi aracılığıyla yollanmasını ifade etmektedir. Sevk edilen yerin yakın ya da uzak olması ya da sevk için bir bedelin ödenip ödenmediği suçun oluşumu bakımından önem taşımamaktadır[307].

Sevki gerçekleştiren kişinin, sevk ettiği nesnenin bilişim suçunun işlenmesini sağlayacak bir cihaz, bilgisayar programı, şifre ve sair güvenlik kodu olduğunu bilip,

---

300 http://tdk.gov.tr/ (E.T: 03.12.2018).
301 **Özbek/ Doğan/Bacaksız/Tepe**, s.1016.
302 **Korkmaz**, s.52.
303 **Özbek/ Doğan/Bacaksız/Tepe**, s.1016.
304 **Korkmaz,** s.52.
305 **Akbulut**, Bilişim Alanında Suçlar, s.356, 357.
306 http://tdk.gov.tr/ (E.T: 04.12.2018).
307 **Mesut Uzuntok**, Uyuşturucu Veya Uyarıcı Madde İmal Ve Ticareti Suçları, Yayımlanmamış Doktora Tezi,İstanbul, Marmara Üniversitesi SBE, 2008, s. 263, https://tez.yok.gov.tr/UlusalTezMerkezi/ (E.T: 04.12.2018).

bilmemesi, sevk edenin suçunun oluşması yönünden sonuca etkili değildir[308]. Yine suçun oluşumu bakımından sevk eyleminin ülke sınırları içerisinde gerçekleştirilmesi gerekmektedir. Eğer sevk işlemi yurtdışından yurt içine yapılmışsa ithal, yurt içinden yurt dışına yapılmışsa ihraç suçu oluşacaktır[309].

Nakletme; nakil işini yapmak, bir yerden başka bir yere geçirmek, iletmek anlamına gelmektedir[310]. Taşınan cihaz, bilgisayar programı, şifre ve sair güvenlik kodunun başkasına ait olması durumunda taşıyan açısından nakletme, maliki açısından ise sevk etme suçu oluşur[311]. Burada taşıyan kişinin taşıdığı cihaz, program, şifre ve sair güvenlik kodunun bilişim suçlarının işlenmesi amacıyla kullanılacağını bilmeden taşıması halinde yalnızca malik açısından sevk suçu oluşacaktır.[312]

Metinde yer alan bir diğer hareket de depolama hareketidir. Depolama sözlükte, saklamak veya korumak amacıyla ambara koymak, depo etmek, biriktirmek, ambarlamak şeklinde tanımlanmıştır[313]. Bu kavram 245/A maddesinde, doğrudan ya da dolaylı bilişim suçlarının işlenmesi amacıyla yapılan veya oluşturulan cihaz, bilgisayar programı, şifre ve sair güvenlik kodunun, fail tarafından kişisel kullanım amacı dışında herhangi bir nedenle, (satma, devretme, ihraç gibi amaçlarla) bir yerde korumak için tutmasıdır. Burada suçun maddî unsuru, cihaz, bilgisayar programı, şifre ve sair güvenlik kodunun herhangi bir yerde kullanım dışında bir amaçla saklanması veya tutulması için gereken icrai hareketlerin yapılmasıdır[314]. Saklanmaya başlandığı anda suç tamamlanır ancak bitmez; sürekliliğin kesildiği anda suç bitmiş olur. Dolayısıyla bu eylem bakımından suç kesintisiz suçtur[315]. Failin depoladığı cihaz, bilgisayar programı, şifre ve sair güvenlik kodunun maliki olmasının ya da bu depolama karşılığında ücret alıp almamasının suçun oluşması bakımından bir önemi

---

308 **Uzuntok,** s.263.
309 **Uzuntok,** s.263.
310 http://tdk.gov.tr/ (E.T: 04.12.2018).
311 **Özbek/ Doğan/Bacaksız/Tepe**, s.1016.
312 **Korkmaz,** s.52.
313 http://tdk.gov.tr/ (E.T: 04.12.2018).
314 **Özbek/ Doğan/Bacaksız/Tepe**, s.1017.
315 **Koca/Üzülmez,** s.914.

bulunmamaktadır[316]. Şifre ve sair güvenlik kodlarının elektronik ya da dijital ortamda depolanması mümkündür ancak her kaydetme depolama olarak nitelendirilmemelidir. Failin amacını belirlemek amacıyla kaydın niteliği, boyutu ve amacı gibi unsurların göz önünde bulundurulması gerekmektedir[317].

Kabul sözcüğü, bir şeye isteyerek veya istemeyerek razı olma, sunulan bir şeyi, armağanı alma, bir öneri uygun bulma, onaylama anlamlarına gelmektedir[318]. Yasak cihaz veya programlar açısından ise bunların mülkiyetinin veya zilyetliğinin bir bedel olmaksızın alınmasını ifade etmektedir. Mülkiyetin ya da zilyetliğin geçmesi ile suç tamamlanır.

Satmak, bir değer karşılığında bir malı alıcıya vermek anlamına gelmektedir[319]. 245/A maddesi kapsamında ise, yasak cihaz veya programların bir bedel karşılığında mülkiyetinin ya da zilyetliğinin devredilmesi anlamına gelmektedir. Burada taraf iradelerinin alım satım konusunda birleşmesi yeterli değildir. Aynı zamanda fiili hakimiyetin de devri gerekmektedir[320].

Arz kavramı sözlükte sunma, piyasaya mal sürülmesi, yüksek makama anlatma, bildirme anlamlarına gelmektedir[321]. Satışa arz etme ise bir malı satma iradesini açığa vuran herhangi bir hareketin yapılmasıdır[322]. Failin yasak cihaz veya programları satmak amacına yönelik pazarlık yapması, müşteri araması, kapora alması gibi hareketler bu suçu oluşturacaktır.

Satın almak, bir nesneyi belirlenen fiyatını ödeyerek kendine mal etmek anlamına gelir[323]. Satma hareketinin karşılığı olan bu hareket de bedel karşılığında yasak cihaz veya programların mülkiyetinin ya da zilyetliğinin devralınmasını ifade eder.

---

316 **Mehmet Zülfü Öner**, Türk Ceza Hukukunda Uyuşturucu veya Uyarıcı Madde İmal ve Ticareti Suçları, Doktora Tezi, Ankara Üniversitesi SBE, 2010, s.118 https://tez.yok.gov.tr/UlusalTezMerkezi/ (E.T: 25.11.2018).
317 **Özbek/ Doğan/Bacaksız/Tepe**, s.1017.
318 http://tdk.gov.tr/ (E.T: 04.12.2018).
319 http://tdk.gov.tr/ (E.T: 04.12.2018).
320 **Öner,** s.109.
321 http://tdk.gov.tr/ (E.T: 04.12.2018).
322 **Tezcan/Erdem /Önok**, s.642.
323 http://tdk.gov.tr/ (E.T: 04.12.2018).

Vermek, kelime olarak, üzerinde, elinde veya yakınında olan bir şeyi birisine eriştirmek, iletmek anlamındadır[324]. Maddede kabul etmek hareketinin karşılığı olarak düzenlenmiş olup söz konusu cihaz veya programların mülkiyetini veya zilyetliğinin herhangi bir bedel veya karşılık olmaksızın el değiştirmesini ifade etmektedir.

Maddede yer alan son hareket olan bulundurma ise kelime olarak, var olmasını, hazır bulunmasını sağlamak anlamına gelmektedir[325]. Maddedeki anlamı itibariyle yasak cihaz ve programlar üzerinde fiili ve hukuki egemenliğin kurulması ve bu maddeler üzerinde tasarruf imkânının sağlanmış olmasını ifade eder. Ayrıca, yasak cihaz veya programların bulundurulduğu yerin mülkiyetinin faile ait olması gerekmemektedir. Failin bu yere istediği an ulaşabilme imkanının bulunması yeterli bulunmaktadır[326]. Söz konusu program, şifre ve sair güvenlik kodlarının bilgisayarda bulundurulması da suçu oluşturmaktadır. Uygulamada en fazla gündeme gelecek olan hareketin, zararlı yazılım veya cihazın bulundurulması şeklinde olması beklenmektedir[327].

Maddede yer alan hareketlerin tamamı bakımından, söz konusu cihaz, bilgisayar programı, şifre ve sair güvenlik kodlarının suç işlemek amacıyla oluşturulduğu veya yapıldığı, bunların hazırlanış ve yakalanış şekline, fail ya da faillerin davranışlarına ve beyanlarına göre[328], somut olayın özellikleri dikkate alınarak belirlenebilecektir. Yine olayın özelliğine göre bilirkişi görüşü de alınmalıdır.

Bu suç, işlenmesi amaçlanan suçlar bakımından hazırlık hareketi niteliğindeki fiilleri cezalandıran bir suç tipidir. Bu nedenle bilişim alanında suçları işlemek amacıyla bu cihazları üreten kişiler, hem bu suçtan hem de amaçladıkları suçlardan dolayı ayrı ayrı cezalandırılmalıdır.

---

324 http://tdk.gov.tr/ (E.T: 04.12.2018).

325 http://tdk.gov.tr/ (E.T: 04.12.2018).

326 **Arzu Tuncer**, Uyuşturucu veya Uyarıcı Madde Ticareti ve Kullanılmasına İlişkin Suçlar, Doktora Tezi, İstanbul Kültür Üniversitesi SBE, 2011, s.94 https://tez.yok.gov.tr/UlusalTezMerkezi/ (E.T: 25.11.2018).; Dülger, s.458.

327 "Yeni Bir Bilişim Suçu: Zararlı Yazılım ve Yasak Cihaz", http://www.elithukuk.com/yeni-bir-bilisim-sucu-zararli-yazilim-ve-yasak-cihaz/ (E.T: 10.03.2019).

328 **Gül**, s.208.

İKİNCİ BÖLÜM
BİLİŞİM SİSTEMİNİN İŞLEYİŞİNİ ENGELLEME, BOZMA YOK ETME VEYA DEĞİŞTİRME SUÇLARI (m. 244)

Suç, insanlığın varoluşuyla birlikte ortaya çıkmış olup, dönemin koşullarına göre şekillenmiştir. Bilişim teknolojisinin gelişmesi ve bilginin eskiye göre daha hızla yayılması, önem kazanması, bilginin ekonomik, sosyal, siyasal değerinin artması, bu değerler üzerinde kolay yoldan hak sahibi olmak isteyen kişileri, bilişim teknolojisi marifetiyle suç işler hale getirmiştir[329]. Teknolojinin ve özellikle internetin ortaya çıkışı ile birlikte, bu şekilde hayatın her alanına girmesi bilişim sistemlerine yönelik suçların artmasına neden olmuş ve verilerin korunması konusunun önemini artırmıştır[330].

Verilerin korunması ile ilgili olarak Türk Ceza Hukuku'ndaki ilk düzenleme 765 sayılı TCK'nın ikinci kitabının mal aleyhine cürümler başlıklı onuncu babının on birinci faslında bilişim alanında suçlar başlığı ile (525/a), (525/b), (525/c) ve (525/d) maddelerinin eklenmesi ile yapılmıştır. Bu bölümde; *"bilgileri otomatik olarak işleme tabi tutmuş bir sistemden, programları, verileri veya diğer herhangi bir unsuru hukuka aykırı olarak ele geçirmek"* (525/a), "*bilgileri otomatik işleme tabi tutmuş bir sistemi veya verileri kısmen veya tamamen tahrip etmek"* (525/b), *"sahte bir belgeyi oluşturmak için bilgileri otomatik olarak işleme tabi tutan bir sistemi tahrif etmek"* (525/c), *"suç konusu eylemleri gerçekleştirenlere ayrıca uygulanacak cezalar"* (525/d) düzenlenmiştir.

5237 sayılı TCK'da ise bilişim sistemlerine yönelik suçlar, kanunun özel hükümleri düzenleyen ikinci kitabının, topluma karşı suçlara ilişkin üçüncü kısmının, bilişim alanında suçlar başlıklı onuncu bölümünde yer almaktadır. 5237 sayılı TCK'nın 244'üncü maddesi ile

---

329 **İbrahim Keskin**, Bilişim Suçları, Adalet Dergisi, Ankara, 2007, S:29, s.101. http://www.yayin.adalet.gov.tr/adaletdergisi/29.sayi/09_34_14.pdf (E.T: 03.01.2019).

330 **Ali Durdu**, Türk Silahlı Kuvvetleri Personelinin Bilişim Suçlarına Yönelik Yaklaşımı (Gaziantep İli Örneği), Yayımlanmamış Yüksek Lisans Tezi, Gaziantep Üniversitesi SBE, Gaziantep, 2015, s.6. https://tez.yok.gov.tr/UlusalTezMerkezi/ (E.T: 25.11.2018).

765 sayılı TCK'nın (525/b) maddesinden hareketle ve Sanal Ortamda İşlenen Suçlar Sözleşmesi'nin 4[331], 5[332] ve 8[333]'inci maddeleriyle paralel bir düzenleme yapılmıştır[334]. Sözleşmenin "*Verilere Müdahale*" başlıklı dördüncü maddesinde, taraf devletlere haksız bir şekilde ve kasten bilgisayar verisine zarar verilmesini, verinin silinmesini, verinin bozulmasını, verinin değiştirilmesin veya engellenmesini kendi ulusal mevzuatı kapsamında suç saymak için gerekli yasal düzenlemeleri yapma yükümlülüğü getirmiştir.

Zarar verme ve bozma ile veri ve programların bütünlüğünün ya da bilgi içeriğinin değiştirilmesi, silme ile fiziki bir varlığı bulunan eşyanın yok edilmesi, tanınmaz hale getirilmesi; engelleme ile verinin erişilmez kılınmasına neden olan herhangi eylemi, değiştirme ile var olan verinin kötücül yazılımlarla farklı hale getirilmesi dâhil olmak üzere başka biçime sokulması anlaşılmaktadır[335].

---

331 Madde 4- Verilere Müdahale; 1- Taraflardan her biri, bilgisayar verilerine haksız yere zarar verilmesi, verilerin silinmesi, tahrip edilmesi, değiştirilmesi veya engellenmesinin, kasten gerçekleştirildiği zaman, kendi iç hukuku kapsamında cezai suç olarak tanımlanması için gerekli olabilecek yasama tedbirlerini ve diğer tedbirleri kabul edecektir.
2- Taraflardan biri, 1. Paragrafta tanımlanan fiillerin ciddi zararla sonuçlanması gerektiğini şart koşma hakkını saklı tutabilir.

332 Madde 5- 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 cezai suç olarak tanımlanması için gerekli yasama tedbirlerini ve diğer tedbirleri kabul edecektir.

333 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 bir başkasına haksız yere maddi menfaat sağlamak için hile veya sahtekarlık niyetiyle;
a. Bilgisayar sistemlerine veri girişi yapma, verileri değiştirme, silme veya engelleme;
Bir bilgisayar sisteminin işleyişine herhangi bir müdahalede bulunma.

334 **Merve Erdem/Gürkan Özocak,** Avrupa Konseyi Siber Suç Sözleşmesi ve Türk Hukukuna Etkileri,s.15 http://www.ozocak.com/Dosyalar/27669f.pdf (E.T: 11.06.2018). TCK'nın 244'üncü maddesinin son hali şu şekildedir;
"Madde 244- Sistemi engelleme, bozma, verileri yok etme veya değiştirme
Bir bilişim sisteminin işleyişini engelleyen veya bozan kişi, bir yıldan beş yıla kadar hapis cezası ile cezalandırılır.
Bir bilişim sistemindeki verileri bozan, yok eden, değiştiren veya erişilmez kılan, sisteme veri yerleştiren, var olan verileri başka bir yere gönderen kişi, altı aydan üç yıla kadar hapis cezası ile cezalandırılır.
Bu fiillerin bir banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinde işlenmesi halinde, verilecek ceza yarı oranında artırılır.
Yukarıdaki fıkralarda tanımlanan fiillerin işlenmesi suretiyle kişinin kendisinin ya da başkasının yararına haksız bir çıkar sağlamasının başka bir suç oluşturmaması halinde, iki yıldan altı yıla kadar hapis ve beşbin güne kadar adli para cezasına hükmolunur."

335 Avrupa Konseyi Siber Suçlar Sözleşmesi Açıklayıcı Raporu, http://conventions.coe.int/Treaty/en/Reports/Html/185.htm. (E.T:03.07.2019).

Sözleşme ile TCK'nın 244'üncü maddesinde öngörülen seçimlik hareketler aynı şekilde ifade edilmemiş olsa da anlam itibariyle birbirleri ile örtüşmektedir. TCK, Sözleşme'den farklı olarak ayrıca veriye müdahalenin bir banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinden gerçekleştirilmesini nitelikli hal olarak görmüştür[336]. Sözleşme'de yer alan bu suç nedeniyle ciddi bir zararın doğması unsuruna TCK'nın 244'üncü maddesinde yer verilmemiştir.

Sözleşmenin *"Sisteme Müdahale"* başlıklı beşinci maddesi ile taraf devletlere, bilgisayar sistemine veri yükleyerek, verileri aktararak, verilere zarar vererek, verileri silerek, bozarak, değiştirerek veya engelleyerek bilgisayarın sisteminin çalışmasını kasten ve haksız bir şekilde ciddi ağırlıkta aksatma eylemini suç saymak için gerekli yasal düzenlemeleri yapma yükümlülüğü getirilmiştir

Hükmün amacı telekomünikasyon olanakları da dahil olmak üzere bilgisayar sistemlerinin yasalara uygun şekilde kullanımının bilgisayar verileri kullanılarak ya da bu veriler etkilenerek uluslararası düzeyde engellenmesi fiilinin suç olarak tanımlanmasıdır[337]. Korunan yasal hak, bilgisayar ya da telekomünikasyon sistemlerinin işletmeci ve kullanıcılarının bu sistemleri uygun biçimde işletme haklarıdır. Metin her tür işleyiş biçiminin koruma altına alınmasını sağlamak için tarafsız bir dille kaleme alınmıştır.

Bu suç için veri yüklemek, verileri aktarmak, verilere zarar vermek, verileri silmek, bozmak, değiştirmek veya engellemek hareketlerinden birinin gerçekleştirilmesi ve bu eylemin ciddi bir sistem aksaması ile sonuçlanması gerekmektedir. Sisteme müdahale sonucu sistemin işleyişinin ciddi ölçüde aksaması gerekmektedir[338]. Bu unsur dışında, madde kapsamında Sözleşme ile TCK'nın birbirleri ile uyumlu oldukları söylenebilir

---

336 **Nusret Onur Akpek,** Siber Suçlar Sözleşmesinin Getirdikleri ve İç Hukuk Açısından Konuya Yaklaşım, Yayımlanmamış Yüksek Lisans Tezi, İstanbul Bilgi Üniversitesi SBE, İstanbul, 2015, s.72 https://tez.yok.gov.tr/UlusalTezMerkezi/ (E.T: 25.11.2018).

337 Avrupa Konseyi Siber Suçlar Sözleşmesi Açıklayıcı Raporu Türkçe Çevirisi https://www.ozgureralp.av.tr/avrupa-konseyi-siber-suc-sozlesmesi-aciklayici-memorandum-internet-ve-hukuk-platformu-i-v-h-p-cevirisi/ (E.T:03.07.2019).

338 Avrupa Konseyi Siber Suçlar Sözleşmesi Açıklayıcı Raporu

Sözleşmenin *"Bilgisayarla Bağlantılı Dolandırıcılık"* başlıklı sekizinci maddesi ile de taraf devletlere kasten ve haksız bir şekilde, bilgisayar verilerini girme, silme veya engelleme, bilgisayar sistemlerinin işleyişine müdahale etme eylemleri ile bir başkasının mal kaybına neden olarak, kendisi veya bir başkası için haksız bir menfaat sağlamanın suç olarak düzenlemesi yükümlülüğü getirilmiştir.

Sözleşmenin bu maddesinin TCK'da farklı yansımaları bulunmaktadır. Bu suç, TCK'nın 142/2-e maddesinde yer alan bilişim sistemlerinin kullanılması suretiyle hırsızlık suçu, 158/1-f maddesinde yer alan bilişim sistemlerinin kullanılması suretiyle dolandırıcılık suçu, 244/4 maddesinde düzenlenen bilişim sistem ve verilerine yönelik eylemler sonucunda herhangi bir şekilde menfaat elde edilmesi halinde sistemi engelleme, bozma verileri yok etme veya değiştirme suçu ya da 245'inci maddede düzenlenen banka ve kredi kartlarının kullanılması suçu şeklinde işlenebilir.

Tez konumuz olan TCK'nın 244'üncü maddesinin birinci fıkrasında *"bilişim sistemini engelleme veya bozma"*, ikinci fıkrasında *"bilişim sistemindeki verileri bozma, yok etme, değiştirme veya erişilmez kılma, sisteme veri yerleştirme veya var olan verileri başka bir yere gönderme"*, üçüncü fıkrasında ise *"bilişim sistemi aracılığıyla kendisinin ya da başkasının yararına haksız bir çıkar sağlama"* eylemleri ayrı suçlar olarak düzenlendiğinden ayrı ayrı inceleme konusu olarak ele alınacaktır.

---

https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680081561 (E.T:03.07.2019).

I. BİLİŞİM SİSTEMİNİN İŞLEYİŞİNİ ENGELLEME VEYA BOZMA SUÇU

A. GENEL OLARAK

Bilgi teknolojileri ve iletişim sektörü, ekonomik ve sosyal gelişmenin temel altyapısını oluşturan önemli bir sektör haline gelmiş, bilgi ve iletişim teknolojileri ile hizmetlerine erişim, elektrik ve su gibi temel ihtiyaçlar arasına girmiştir[339].

Teknolojik gelişmelerle birlikte, internetin bütün dünyadaki toplumlara nüfuzu her geçen gün artarken, internet üzerinden verilen hizmetler ve internet trafiği de katlanarak artmaktadır. Veri trafiğindeki artış tahminleri, araştırmayı yapan kişi/kuruluşa göre farklılıklar gösterse de söz konusu artışın üssel (exponansiyel) olarak gerçekleştiği konusunda birleşmektedir[340]. CISCO Yazılım Şirketi tarafından 2016 yılında yapılan bir çalışmaya göre, önceki 5 yılda küresel anlamda toplam internet trafiğinin 2,3 kattan fazla arttığı görülmekte ve sonraki 5 yılda da 2,7 kata yakın artış olacağı tahmin edilmektedir[341].

Bilişim, bilgi teknolojileri ve internet, insanlığı yeni bir toplum biçimine taşıyan, tetikleyen ve temsil eden iç içe geçmiş araçlar bütünüdür[342]. Bilgiyi yaşamın odağına koyuş, ekonomik üretim ve bölüşüm sistemlerini bilgi odaklı yönlendiren toplumlar, yani "bilgi toplumları" yeni yüzyılın yönlendirici gücü olacaktır[343]. Ülkemizde de bu gelişmelere paralel

---

339 Ulusal Genişbant Stratejisi ve Eylem Planı, s.7. http://hgm.ubak.gov.tr/Content/UploadedFile/Ulusal%20Geni%C5%9Fbant%20Stratejisi%20ve%20Eylem%20Plan%C4%B1%202017-2020&&dfc2d335-235b-4293-a946-b371a6262244.pdf (E.T: 06.02.2019)

340 Ulusal Genişbant Stratejisi ve Eylem Planı, s.7. http://hgm.ubak.gov.tr/Content/UploadedFile/Ulusal%20Geni%C5%9Fbant%20Stratejisi%20ve%20Eylem%20Plan%C4%B1%202017-2020&&dfc2d335-235b-4293-a946-b371a6262244.pdf (E.T: 06.02.2019)

341 Ulusal Genişbant Stratejisi ve Eylem Planı, s.7. http://hgm.ubak.gov.tr/Content/UploadedFile/Ulusal%20Geni%C5%9Fbant%20Stratejisi%20ve%20Eylem%20Plan%C4%B1%202017-2020&&dfc2d335-235b-4293-a946-b371a6262244.pdf (E.T: 06.02.2019)

342 **Mustafa Akgül**, İnternet Yasakları ve Hukuk, Türkiye Barolar Birliği Dergisi, Yıl:21, Sayı:78, Eylül-Ekim 2008, s.354.

343 **Mesih Gözüşirin**, 5237 Sayılı Türk Ceza Kanununda Bilişim Suçları ve Bilişim Suçları ile Mücadeleye İlişkin Model Önerisi, Kara Harp Okulu Savunma Bilimleri Enstitüsü s.9; **Abdullah Taner Demiroğlu,** Stratejik İstihbaratın Önemi: Bilişim Suçları Uygulaması, Yayımlanmamış Yüksek Lisans Tezi, Polis Akademisi Güvenlik Bilimleri Enstitüsü, Ankara, 2015, s.63 https://tez.yok.gov.tr/UlusalTezMerkezi/ (E.T: 25.11.2018); **Olgun Değirmenci,** Bilişim Suçları Alanında Yapılan Çalışmalar ve Bu Suçların Mukayeseli Hukukta Düzenlenişi, Legal Hukuk Dergisi, S:11, Y:2003, s.2750.

olarak *"e-Dönüşüm Türkiye"* projesi oluşturulmuş[344] ve bu proje kapsamında kamu hizmetlerinin sunumunda, bilgi ve iletişim teknolojilerinden azami ölçüde yararlanılarak iyi yönetişim ilkelerinin hayata geçirilmesine katkıda bulunulması, bilgi ve iletişim teknolojilerinin kullanımının yaygınlaştırılması amaçlanmış ve E-DEVLET, UYAP, TAK-BİS gibi projeler üretilerek verilerin sistemde kayıtlı ve her an ulaşılabilir olması sağlanmıştır[345]. Bu projenin yürütülmesi amacıyla *"e-Dönüşüm Türkiye İcra Kurulu"* oluşturulmuş olup, bu kurulun sekreterya işlemleri T.C. Cumhurbaşkanlığı Strateji ve Bütçe Başkanlığı'na bağlı Bilgi ve İletişim Teknolojileri Dairesi tarafından yapılmaktadır[346].

Görünen odur ki, internetin sunduğu hizmetler ve sağladığı kolaylıklar hızla artmaya devam edecek ve her yeni gelişme, beraberinde çözümlenmesi gerekli yeni hukuki problemleri de getirecektir[347]. Bu projeler hizmetin sunulmasını ve hizmete erişimi hızlandırdığı gibi, sistemde meydana gelen bir arıza ya da sistemlere girilerek verilerin yok edilmesi veya sisteme girmenin engellenmesi gibi durumlarda o alandaki çalışmaların tamamen durmasına sebep olabilmektedir[348]. Bu gibi nedenlerle sistemlerin ve verilerin korunması büyük bir önem taşımaktadır.

Bu sebeple kanun koyucu TCK'nın 244/1'inci maddesi ile bilişim sisteminin işleyişinin engellenmesi veya bozulmasını bir yaptırıma bağlamıştır. Madde metninin gerekçesinde ise "*sistemlere yöneltilen ızrar fiilleri özel bir suç haline getirilmiştir. Aracın fizik varlığı ve işlemesini sağlayan bütün unsurları, söz konusu suçun konusunu*

---

344 **Özgür Uçkan**, Ankara Barosu Uluslararası Hukuk Kurultayı, 03-07 Ocak Ankara "Bilgi Ekonomisi, Bilgi Toplumu, Mahremiyet ve Güvenlik" konulu konuşma metni, Ankara, Ankara Barosu Yayınları, 2006, C:4 s.28.

345 **Fatma Turan,** Milli Eğitim Bakanlığı Bilişim Sisteminin Bir Alt Sistemi Olarak E-Okul Uygulamasına İlişkin İlköğretim Okullarındaki Yönetici, Öğretmen ve Veli Görüşleri, Yayımlanmamış Yüksek Lisans Tezi, Akdeniz Üniversitesi SBE, Antalya, 2010, s.62 https://tez.yok.gov.tr/UlusalTezMerkezi/ (E.T: 25.11.2018); **Uğur Batır**, E-Devlet Uygulamalarından Adalet Bakanlığı Ulusal Yargı Ağı Bilişim Sistemi Portalı (UYAP)'ın Etkinliğini Belirlemeye Yönelik Ankara Barosu Avukatları Üzerine Bir Alan Araştırması, Yayımlanmamış Yüksek Lisans Tezi, Gazi Üniversitesi Eğitim Bilimleri Enstitüsü, Ankara, 2013, s.59.

346 http://www.bilgitoplumu.gov.tr/ (E.T: 03.02.2019).

347 **Hasan Sınar**, "İnternetin Ortaya Çıkardığı Hukuki Sorunlara Bir Ceza Hukuku Yaklaşımı", Milletlerarası Hukuk ve Özel Hukuk Bülteni, Sayı: 1-2, 1997-1998, http://istanbul.dergipark.gov.tr/download/article-file/99545 (E.T: 03.02.2019).

348 **Bekir Peker,** Bilişim Suçları ve Bilişim Güvenliğinin Ulusal ve Uluslararası Boyutu, Yayımlanmamış Yüksek Lisans Tezi, Selçuk Üniversitesi SBE, Konya, 2010, s.5 https://tez.yok.gov.tr/UlusalTezMerkezi/ (E.T: 25.11.2018).

oluşturmaktadır" denilmiştir. Bilişim sistemine yapılacak müdahalenin kalıcı, geçici, kısmen ya da tümden olması önemli değildir[349].

B. KORUNAN HUKUKİ DEĞER

Suçla korunan hukuki değer, kanun tarafından emir hükmü ve yaptırımla koruma altına alınan haktır[350]. Bir hukuksal değerle ilişkilendirilemeyen herhangi bir suç tipinin, daha geniş bir ifadeyle haksızlığın bulunması mümkün değildir[351].

TCK'nın 244'üncü maddesinin birinci fıkrasında düzenlenen suçla korunan hukuki yarar konusunda doktrinde görüş birliği bulunmamaktadır. Bazı yazarların görüşleri ise şu şekildedir;

Akbulut, birinci fıkrada tüm bilişim sistemleri sahipleri, işletmecileri ile kullanıcılarının sistemin arızasız çalışmasındaki yararının korunduğunu ifade etmiştir[352].

Artuk/Gökcen/Yenidünya, bu suçla korunan hukuki değerin, *bilişim sistemlerinin işletmecilerinin ve kullanıcılarının sistemi uygun şekilde işletme haklarının, bilişim sistemlerinin doğru ve işlevlerine uygun şekilde faaliyetlerine devam etmesinin sağlanmasının ve bilişim sistemlerinin günümüzdeki rolleri dikkate alındığında haberleşme özgürlüğünün bu suçla korunması"* olduğunu ifade etmektedir[353].

Dülger, bu suçla korunan hukuksal değerin karma bir nitelik gösterdiğini ve yalnızca bilişim sistemlerinin veri ve yazılımlarından oluşan soyut unsurları değil, somut unsuru olan donanımları da koruduğunu ifade etmektedir. Buna göre korunan hukuki yarar, bilişim sistemi ve/veya sistemin içerdiği veriler üzerinde tasarruf yetkisi bulunan kişinin, verilerle

---

349 **Erdoğan,** Bilişim Suçları, s.189.

350 **M. Emin Artuk /Ahmet Gökcen /M. Emin Alşahin / Kerim Çakır**, Ceza Hukuku Genel Hükümler, 13. Baskı, Ankara 2019, s. 308.

351 **İzzet Özgenç**, Türk Ceza Hukuku Genel Hükümler, 14. Baskı, Ankara, Seçkin Yayıncılık, 2018, s.170.

352 **Akbulut,** Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme, s.17; **Akbulut,** Bilişim Alanında Suçlar, s.181.

353 **Artuk/ Gökcen /Yenidünya,** Türk Ceza Kanunu Şerhi,s.4659,4660.

oluşturulan değerlere herhangi bir engel olmadan ulaşılması ve kullanılmasındaki çıkarıdır[354].

Erdağ, bu suçun mala zarar vermenin elektronik bir türü olduğunu ve korunan hukuki değerin karma nitelik taşıdığını ifade etmiştir[355].

Karagülmez'e göre, 244'üncü maddenin bir ve iki numaralı fıkralarında korunan hukuki yarar, sistemlere yöneltilen ızrar fiillerini suç haline getirme düşüncesiyle bağlıdır. Bu suçların konusunu, bilişim sisteminin varlığını ve işlemesini sağlayan bütün diğer unsurlar oluşturmaktadır ve burada hem bilişim sisteminin hem de sistem içinde yer alan verilerin veya diğer unsurların zarar görmemesi amaçlanmaktadır[356].

Koca/Üzülmez ise; 244'üncü maddenin ilk ilki fıkrasıyla bilişim sistemlerinin doğru ve sağlıklı bir şekilde işleyişini korumak amacıyla, sistemin soyut unsurlarına zarar vermeye yönelik saldırıların yaptırım altına alındığı görüşündedir[357].

Bir başka görüşe göre ise, mala zarar verme suçunun bilişim alanındaki özel görünüş biçimini oluşturan bu suç aynı zamanda mülkiyet hakkını korumaktadır[358].

Kurt, bu suçun öncelikle mülkiyet hakkını, bilişim sisteminin dokunulmazlığı, iletişim kurma ve teknolojik gelişim özgürlüğünü korumakta olduğunu belirtmiştir[359].

Taşdemir ise bu suç ile veri güvenliğinin sağlanmasının amaçlandığını ifade etmiştir[360].

---

354 **Dülger,** s. 313.
355 **Erdağ,** s.280.
356 **Karagülmez,** s.235.
357 **Koca/Üzülmez,** Özel Hükümler, s.867.
358 **Durmuş Tezcan/M. Ruhan Erdem/R. Murat Önok**, Teorik ve Pratik Ceza Özel Hukuku, 16. Baskı, Seçkin Yayınları, Ankara, 2018, s.1047.
359 **Kurt,** s.162.
360 **Taşdemir**, Bilişim, Banka ve Kredi Kartlarının Kötüye Kullanılması ve Dolandırıcılık Suçu, s.255.

Özbek/Doğan/Bacaksız/Tepe, bilişim sisteminin ve verilerin güvenliği ile mülkiyet hakkının korunduğu görüşündedir[361].

Yazıcıoğlu; bu suçun düzenlenmesi ile temelde bilişim sisteminin işleyişi, özellikle sistemin kendisi yani donanımsal yanının koruma altına alındığını ifade etmiştir[362].

Yılmaz'a göre ise, bu suçla bilişim sistemi veya verileri üzerinde sahibi veya zilyedinin her türlü mülkiyet hakkı ve buna bağlı olarak toplum menfaati korunmak istenmiştir[363].

Bilişim sisteminin işleyişini engelleme ve bozma suçu, topluma karşı suçlar bölümünde yer almakta olup, bilişim sistemlerinin birbirleri ile etkileşim halinde olduğu ve çoğu zaman bir sistemin etkisiz hale getirilmesi sonucunda toplumun zarar gördüğü değerlendirildiğinde suçla korunmak istenen hukuki değerlerden birinin toplumun menfaatleri olduğu söylenebilir[364]. Ayrıca suç, bilişim sisteminin işleyişine yönelik eylemlere ilişkin olduğundan bilişim sistemleri sahiplerinin, işletmecilerinin ve kullanıcılarının sistemin işleyişinin herhangi bir arıza olmaksızın çalışmasındaki yararı korunmaktadır.

---

361 **Özbek/ Doğan/ Bacaksız/ Tepe**, s.959.

362 **Yılmaz Yazıcıoğlu**, "Yeni Türk Ceza Kanunundaki Bilişim Suçlarının Genel Değerlendirilmesi" Yeditepe Üniversitesi .Hukuk Fakültesi Dergisi, C. 2, S. 92, 2005, s.409 http://law.yeditepe.edu.tr/tr/yu-hukuk-fakultesi-dergisi (E.T: 05.02.2019).

363 **Sacit Yılmaz**, 5237 Sayılı TCK'nın 244. Maddesinde Düzenlenen Bilişim Alanındaki Suçlar, s.68. http://tbbdergisi.barobirlik.org.tr/m2011-92-669 (E.T: 27.01.2019).

364 **Erdoğan,** Bilişim Suçları, s.184; **Koca/Üzülmez,** Özel Hükümler, s.867.

C. SUÇUN UNSURLARI

1. Tipikliğin Maddi Unsurları

a. Fiil

TCK'nın 244'üncü maddesinin birinci fıkrasında, bilişim sisteminin işleyişini engelleme veya bozma suçu düzenlenmiştir.

Hareketin şekli bakımından suçlar, icrai ve ihmali olarak ortaya çıkabilir[365]. Hareket bir şeyi yapmak veya yapmamak şeklinde olabilir. İcrai hareket yasak şeklinde ortaya çıkan ve toplum düzenini bozucu davranışların yapılmamasını emreden normlara aykırılıktır[366]. Yapılması yasaklandığı halde bir hareket yapılmışsa buna, icrai hareket denir[367]. Suçlar genellikle icrai hareketle işlenir. Emredici hukuk kuralına aykırılık teşkil eden olumsuz davranış, ihmali suçu oluşturur[368]. Ancak, ihmali suçlarda failin sadece hareketsiz kalması yeterli değildir, önemli olan suç tipinde belirlenmiş olan hareketin yapılmamış bulunmasıdır[369]. Yani, kanun koyucunun suç tipinde yapılmasını emrettiği hareketi gerçekleştirmekle yükümlü olan kişinin hareketsiz kalması ya da beklenen davranışı gerçekleştirmemiş olması halinde suç oluşacaktır. Bilişim sisteminin işleyişini engelleme veya bozma suçu icrai olarak işlenir[370].

Kanunun tek bir fiilin icrasını suçun meydana gelmesi için yeterli görmesi halinde, tek hareketli suçlardan bahsedilir[371]. Ceza normunda birden fazla fiil gösterilir ve suçun oluşması için bu hareketlerin hepsinin yapılması beklenirse birleşmiş hareketli suçtan bahsedilir. Ancak; suç tipinde birden fazla hareket, birbirinden bağımsız olarak

---

365 **Veli Özer Özbek/ Koray Doğan/ Pınar Bacaksız/ İlker Tepe,** Türk Ceza Kanunu Genel Hükümler, 11. Baskı Ankara 2017, s.207

366 **Artuk/Gökcen/Alşahin/Çakır,** Genel Hükümler, s.321.

367 **Nur Centel /Hamide Zafer/ Özlem Çakmut,** Türk Ceza Hukukuna Giriş, 10. Baskı, Ankara 2017, s .170; **Ahmet Gökcen,** Belgede Sahtecilik Suçları (m.204-212), 4. Baskı, Ankara, Adalet Yayınevi, 2016, s.165

368 **Artuk/Gökcen/Alşahin/Çakır,** Genel Hükümler, s.321; **Özgenç**, Genel Hükümler, s.225.

369 **Artuk/Gökcen/Alşahin/Çakır,** Genel Hükümler, s.321.

370 **Erdoğan**, Bilişim Suçları, s.185.

371 **Özgenç**, Genel Hükümler, s.177.

düzenlenmişse bu suç, seçimlik hareketli suçtur[372]. Bu durumda hareketlerden bir tanesinin gerçekleştirilmesiyle suç oluştuğu gibi, birden fazla hareketin yapılması da birden fazla suç oluşturmayacaktır.

Doktrinde bilişim sistemini engelleme veya bozma suçunun serbest hareketli bir suç mu yoksa seçimlik hareketli bir suç mu olduğu yönünde görüş farklılıkları bulunmaktadır. Bu görüşlerden biri, engelleme ve bozma hareketlerinin seçimlik hareketler olduğu ve hareketlerden birinin gerçekleştirilmesi ile birlikte suçun oluştuğu yönündedir[373]. Ayrıca maddenin gerekçesinde de seçimlik hareketli bir suç meydana getirildiği belirtilmiştir. Doktrindeki diğer bir görüş ise, kanunda yer alan engelleme ve bozma kavramlarının, suçun hareketi değil neticesi olduğu ve bu sebeple suçun serbest hareketle işlenebilen bir suç olduğu yönündedir[374]. Kanaatimizce buradaki engelleme ve bozma suçun hareketi değil, hareketin neticesidir. Zira engelleme ya da bozma doğrudan uygulanabilen eylemler değildir. Bu eylemlerin gerçekleşebilmesi başka bir eylemin varlığına bağlıdır ve herhangi bir eylem bu neticenin gerçekleşmesini sağlayabilir. Dolayısıyla bu suç serbest hareketlidir.

Fiilin icrasının devam edip etmemesine göre suçlar; ani suç ve mütemadi (kesintisiz) suç olmak üzere ikiye ayrılmaktadır. Mütemadi suçlarda tipte yer alan hareketin gerçekleştirilmesiyle suç tamamlanır, ancak bitmez[375]. Bilişim sisteminin işleyişini engelleme veya bozma suçu da mütemadi bir suç olup, sistemin işleyişinin engellendiği veya bozulduğu anda suç tamamlanır ancak bitmez[376]. Suçun bitmesi için failin suç konusu eylemi üzerindeki iktidarı sona ermelidir. Suçun mütemadi olmasının birtakım sonuçları vardır. Örneğin, TCK'nın 66'ncı maddesine göre suç, temadinin sona erdiği anda işlenmiş sayılır ve

---

372 **Gökcen**, Belgede Sahtecilik, s.166-167; **Özgenç,** Genel Hükümler, s.179; **Olgun Değirmenci**, 2004 Türk Ceza Kanunu'nun Bilişim Suçları Bakımından Değerlendirilmesi, Türkiye Barolar Birliği Dergisi, S:58, 2005, s.205.

373 **Artuk/Gökcen/Yenidünya,** Türk Ceza Kanunu Şerhi, s. 4660; **Karagülmez,** s.187; **Yılmaz**, s.72; **Sinan Esen**, Malvarlığına Karşı Suçlar, Belgelerde Sahtecilik ve Bilişim Alanındaki Suçlar, Ankara, Adalet Yayınevi, 2007, s. 634.

374 **Kurt,** s.166; **Erdoğan,** Bilişim Sistemini Engelleme, Bozma, Verileri Yok Etme veya Değiştirme Suçu, s.147; **Erdoğan,** Bilişim Suçları, s.186; **Koca/Üzülmez,** Özel Hükümler, s.869.

375 **Artuk/Gökcen/Alşahin/Çakır,** s. 266; **Özgenç,** Genel Hükümler, s.183.

376 **Erdoğan,** Bilişim Suçları, s.185.

zamanaşımı temadinin kesildiği andan itibaren başlar. Yine suç temadinin bittiği yerde işlenmiş sayılır[377].

(1) Bilişim Sisteminin İşleyişini Engellemek

Sözlükte engelleme, *"istek, gereksinim veya bir davranışın belli bir sonuca ulaşmasının önlenmesi*" anlamına gelmektedir.[378]

Doktrinde bilişim sisteminin işleyişini engellemek hakkında üzerinde uzlaşılmış bir tanım bulunmamaktadır.

Artuk/Gökcen/Yenidünya; "*Bilişim sistemini engelleme, bilişim sisteminin işleyişini geçici olarak kesintiye uğratmaktır."* şeklinde tanımlamıştır[379].

Avşar/Öngören, "*sistemin gereği gibi çalışmasının önlenmesi, faaliyet ve kapasitesinin sınırlandırılması, sistemin işleyişinin yavaşlatılması veya tamamen kilitlenme noktasına getirilmesi"*[380] olarak ifade etmiştir.

Karagülmez, bilişim sisteminin işlemesini engelleme kavramını; "*sistemin geçici veya sürekli olarak çalışmasının herhangi bir şekilde kesintiye uğratılmasıdır. Burada hareket işleyişi engellemekte fakat bozmamaktadır.*" şeklinde açıklamıştır[381].

Ketizmen, "*sistem aracılığıyla veri işleme faaliyetinin gerçekleştirilmesinin engellenmesidir*." olarak ifade etmiştir[382].

---

377 **Artuk/Gökcen/Yenidünya,** Ceza Hukuku Özel Hükümler, s.678.
378 http://www.tdk.gov.tr/ (E.T: 31.01.2019).
379 **Artuk/Gökcen/Yenidünya,** Türk Ceza Kanunu Şerhi, s.4661.
380 **Avşar/Öngören,** s.136.
381 **Karagülmez**, s.237.
382 **Ketizmen**, s.129.

Kurt; *"sistemin engellenmesi teriminden; gerektiği gibi çalışmasının önlenmesi, faaliyet ve kapasitesinin sınırlandırılması, sistemin işleyişinin yavaşlatılması ya da tamamen kilitlenme noktasına gerilmesinin"* anlaşılması gerektiğini ifade etmektedir[383].

Malkoç'a göre ise bilişim sisteminin engellenmesi ile, "*sistemin teknik işleyişi, çalışması, çeşitli şekillerde engellenerek sistem çalışamaz, normal şekilde ve normal fonksiyonlarını yerine getiremez duruma sokulmaktadır."*[384].

Özbek/ Doğan/ Bacaksız/ Tepe; *"bir bilişim sisteminin işleyişine dışarıdan gerçekleştirilen bir müdahale ile kısmen veya tamamen önlenmesi durumu"* şeklinde ifade etmektedir[385].

Pallı; *"engelleme, sistemin işleyişinin dışarıdan gelmekte olan veya programlanmış olması nedeniyle süregelen bir dış müdahaleden dolayı veri işlem faaliyetinin sistem tarafından yerine getirilememesi*" olarak tanımlamıştır.

Yazıcıoğlu ise engellemenin *"sistemin işlemesine engel olmak, sistemin çeşitli usullerle daimi veya geçici olarak fonksiyon görmesinin engellenmesi"* anlamına geleceğini ifade etmiştir[386].

Yargıtay, sistemin işleyişinin engellenmesini, bilişim sisteminin verimli çalışmasının önlenmesi, icra ettiği faaliyet ve sahip olduğu kapasitesinin müdahale ile sınırlandırılması, yavaşlatılması ya da tamamen kilitlenme noktasına getirilmesi olarak tanımlamaktadır[387].

---

383 **Kurt,** s.161.
384 **Malkoç,** s.3830.
385 **Özbek/Doğan/Bacaksız/Tepe**, s.963.
386 **Yazıcıoğlu**, Bilgisayar Suçları, s.263.
387 Yargıtay 11. Ceza Dairesi, 24.03.2014 tarihli ve 2014/7245 E., 2014/5492 K. sayılı kararı. www.lexpera.com (E.T:03.07.2019)

Tanımlardan da anlaşılacağı üzere doktrinde engelleme suçunun geçici veya sürekli olmasının sonuca etki edip etmediği üzerinde görüş farklılıkları bulunmaktadır.

Kanaatimizce; engelleme geçici olmalıdır. Zira sistemin sürekli olarak engellenmesi durumunda kendinden beklenecek işi yapamayacak durumda olacağından bozulma olarak nitelendirilmesi gerekmektedir[388]. Bilişim sisteminin işleyişinin engellenmesi durumunda sistemin bozulması söz konusu olmayıp normalde yerine getirdiği fonksiyonları yerine getirmesi engellenmektedir. Engel olma, bilişim sisteminin tamamına yönelik olabileceği gibi, işleyişi etkileyen herhangi bir unsuruna yönelik de olabilir[389]. Sistemin yavaş çalışması sistemin engellenmesi kapsamına girmemektedir[390].

Engel olma, bilişim sisteminin genel olarak işleyişinin ya da bu işleyişe katkısı veya etkisi olan herhangi bir unsurun işleyişinin engellenmesi şeklinde de olabilir[391]. Burada önemli olan Özbek/Doğan/Bacaksız/Tepe'nin tanımında olduğu gibi kısmen veya tamamen engelleme neticesinin oluşmasıdır.

Engelleme suçu seçimlik hareketli olduğundan bilişim suçu işleme şekillerinden herhangi biri ile de örneğin sisteme virüs gönderilerek şifrelerin değişmesini sağlamak gibi yöntemlerle gerçekleştirilebilir. Sistemin işleyişine engel olma, sisteme fiziki etki şeklinde gerçekleştirilebileceği gibi, soyut unsurlara yapılan müdahalelerle de söz konusu olabilir. Verilerin bozulması, yok edilmesi, erişilmez kılınması, verilerin değiştirilmesi, sisteme veri yerleştirilmesi, sistemdeki verilerin iletilmesi suretiyle de sistemin işlemesine engel olunabilir[392].

Bilişim sistemi, hem soyut hem de fiziki unsulardan oluşmaktadır. Dolayısıyla sistemin işleyişini engelleme suçu yalnızca sistemin soyut yani yazılım unsuruna yapılan

---

388 **Özbek/Doğan/Bacaksız/Tepe**, s.963; **Demircan,** s.93; **Dülger**, s.321. Daimi veya geçici olmasının suçun oluşumu için önemli olmadığına ilişkin görüş için bkz. **Akbulut,** Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme, s.30.

389 **Dülger**, s.321.

390 **Mahmutoğlu**, s.866.

391 **Karagülmez**, s.237; **Güngör,** s.97.

392 **Akbulut,** Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme, s.28.

müdahale ile değil aynı zamanda donanım unsuruna yapılan müdahalelerle de gerçekleşmektedir. Yani bilişim sisteminin donanım unsuruna yapılan müdahaleler, sistemin işleyişini engelleme kastıyla yapılmış ve engelleme sonucu doğmuşsa, burada bir eylemle iki suç oluştuğundan bilişim sisteminin işleyişinin engellenmesi suçu ile TCK'nın 151'inci maddesinde yer alan mala zarar verme suçu arasında fikri içtima ilişkisi oluşacağı ve bu durumda daha ağır cezayı öngören 244'üncü maddenin uygulanması gerektiği düşüncesindeyiz.

(2) Bilişim Sisteminin İşleyişini Bozma

Sözlüğe göre bozma; *"Bir şeyi kendisinden beklenilen işi yapamayacak duruma getirmek; Bir yerin, bir şeyin düzenini karıştırmak; Dokunmak, zarar vermek, Geçersiz bir duruma getirmek"* anlamlarına gelmektedir[393].

Doktrinde bilişim sisteminin işleyişinin bozulması üzerine de uzlaşılmış bir tanım bulunmamaktadır.

Karagülmez; *"bilişim sisteminin işleyişini bozma, haksız müdahale ile sistemin haksız müdahale ile sistemin sağlıklı işleyişinin geçici veya sürekli şekilde ortadan kaldırılmasıdır. Bozmadan söz edebilmek için, sistemin işleyişinin kısmen veya tamamen sağlıksız hale gelmesi gerekmektedir."* şeklinde bir tanımlama yapmaktadır[394].

Ketizmen, bilişim sisteminin işleyişinin bozulmasını sistemin yazılımını oluşturan işletim sistemin ya da diğer programlar gibi sistem içerisinde veri işleme faaliyetinin ya da genel olarak işlem yapabilmesini sağlayan unsurlarına müdahale edilmesi sonucu, bunların

---

393 http://www.tdk.gov.tr/ (E.T: 31.01.2019)

394 Karagülmez, madde metninde yer alan bozma kavramının gereksiz olduğu kanaatindedir. Şöyle ki; her engelleme, bozma sonucunu doğurmaz fakat her bozma bir engelleme sonucunu doğurabilir. Bu görüş, Sanal Ortamda İşlenen Suçlar Sözleşmesi'nin 5. maddesinde verilerin bozulması yoluyla sistemin işleyişinden söz edilmesine dayandırılmıştır. (**Karagülmez**, s.238).

işlem yapabilme kabiliyetinin tamamen ya da kısmen ortadan kaldırılması olarak tanımlamıştır[395].

Kurt ise *"bilişim sisteminin işleyişini bozma ifadesinden bilişim sistemine bilişim suçunun işlenme şekillerinden birisiyle nüfuz ettikten sonra bilişim suçlarının işlenme şekillerinden birisiyle ya da fiziki saldırılar sonucu sistemin tamamıyla çökertilmesi, bozulması, işlemez hale getirilmesi anlaşılmalıdır."* şeklinde ifade etmektedir[396].

Yargıtay, bozma eylemini bilişim sistemine dahil olan mekanik parçanın veya bir yazılım programının esasen yapması gereken özgülendiği işlevi yapamayacak hale getirilmesi ile birlikte sistemin engellenmesi halinin en üst noktası olan durma noktasından daha ileri olarak sistemin çökertilmesi, zarara uğratılması, işlemez hale getirilmesi, hatta, fiziki olarak dahi zarar verilmesi olarak tanımlamaktadır[397].

Bozmak eyleminin nasıl gerçekleştirildiğinin suçun oluşumu açısından bir önemi yoktur[398]. Fail ister verilerin düzenini bozsun ister sistemi tahrip etsin isterse tahrip edilmek istenen bilişim sistemini parçalasın sonuç fark etmeyecek ve suç gerçekleşmiş olacaktır[399]. Burada dikkat edilmesi gereken şey, fiziki olarak verilen zararın sistemin işleyişine verilmesi gerektiğidir[400]. Aksi takdirde TCK'nın 151'inci maddesinde yer alan mala zarar verme suçu söz konusu olabilecektir. Bozulmanın kısmen veya tamamen sistemin işleyişini etkilemesi de suçun oluşması bakımından önem taşımamaktadır[401].

---

395 **Ketizmen**, s.135.

396 **Kurt**, s.165.

397 Yargıtay 11. Ceza Dairesi, 24.03.2014 tarihli ve 2014/7245 E., 2014/5492 K. sayılı kararı. www.lexpera.com (E.T:03.07.2019).

398 **Akbulut,** Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme, s.31; **Koca/Üzülmez,** Özel Hükümler, s.871.

399 **Dülger**, s. 322; **Koca/Üzülmez,** Özel Hükümler, s.871; **Güngör,** s.97.

400 **Kurt,** s.165, **Demircan**, s.94; **Dülger**, s.322; **Özbek/Doğan/Bacaksız/Tepe**, s.963.

401 **Mert Çakıcı**, Türk Ceza Kanunu m.243 ve m.244'te Düzenlenen Bilişim Suçları, Ceza Hukuku Dergisi, C: 9, S: 24, 2014, s:307; **Akbulut,** Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme, s.31.

b. Netice

İnsanın dış dünyaya yansıyan ihmali ya da icrai davranışından, dış dünyada meydana gelen değişiklik, ceza hukukunda "*netice*" olarak kabul edilir[402].

Çoğu suç, fiilin icra edilmesiyle tamamlanmaktadır. Bu suçlara "*sırf hareket suçları*" denmektedir[403]. Buna karşılık, bazı suçlarda, salt fiilin icra edilmesinden ayrı olarak kanuni tarifte belirtilen neticenin meydana gelmesi gerekir ki suç tamamlanmış olsun. Bu suçlara da neticeli suçlar denmektedir[404]. Bilişim sisteminin işleyişinin birtakım eylemler sonucunda engellenmesi veya bozulması durumunda engellenme veya bozulma suçun neticesini oluşturmaktadır. Dolayısıyla suç, neticeli bir suçtur.

Neticesine göre suçlar, zarar ve tehlike suçu olmak üzere iki grupta incelenmektedir. Genel olarak suçun oluşması için zarar meydana gelmesinin arandığı suçlara zarar suçu, buna karşılık sadece zarar tehlikesinin doğmasıyla yetinilen suçlara ise tehlike suçu denmektedir.[405]

Tehlike suçları, soyut ve somut tehlike suçları olarak ikiye ayrılmaktadır. Soyut tehlike suçlarında suçun kanuni tarifinde yer alan fiilin icra edilmesi yeterli olup, bunun dışında suçun konusu üzerinde gerçekten bir tehlikenin meydana gelip gelmediğinin araştırılmasına gerek yoktur[406]. Somut tehlike suçlarında ise, suçun kanuni tarifinde belirlenen fiilin icra edilmesinin yanı sıra, bu fiilin suçun konusu bakımından somut bir tehlike meydana getirip getirmediğinin, yani, gerçekten bir tehlikeye sebebiyet verip vermediğinin hakim tarafından araştırılıp tespit edilmesi gerekir[407].

---

402 **Gökcen,** Belgede Sahtecilik, s.200; **Özgenç**, Genel Hükümler s.185; **Artuk/Gökcen/Alşahin/Çakır,** s.332.

403 **Artuk/Gökcen/Alşahin/Çakır,** s.270; **Timur Demirbaş,** Ceza Hukuku Genel Hükümler, 12. Baskı, Ankara 2017, s.243.

404 **Özgenç,** Genel Hükümler s.185; **Demirbaş,** s.242,243; **Artuk/Gökcen/Alşahin/Çakır,** Genel Hükümler s.309.

405 **Artuk/Gökcen/Alşahin/Çakır**, Genel Hükümler, s.309, **Koca/Üzülmez**, Özel Hükümler, s.118, **Özgenç,** Genel Hükümler, s.214.

406 **Özgenç,** Genel Hükümler, s.215; **Centel/Zafer/Çakmut, s**.267.

407 **Özgenç,** Genel Hükümler, s.215; **Centel/Zafer/Çakmut, s**.267,268.

Doktrinde bu suçun zarar suçu mu yoksa tehlike suçu mu olduğu konusunda görüş birliği bulunmamaktadır. Bu görüşlerden birine göre bilişim sisteminin işleyişinin engellenmesi veya bozulması suçunun oluşumu için failin yaptığı hareketlerin neticesinde bir zararın meydana gelmesi gerekmektedir[408]. Dolayısıyla suç zarar suçudur. Diğer bir görüşe göre ise; sistemin işleyişinin engellenmesi veya bozulması sonucunda bir zararın doğmamasının mümkün olduğu, bu suçun oluşması için mutlaka bir zararın doğmasının aranamayacağı, Sanal Ortamda İşlenen Suçlar Sözleşmesi'nde de suçun oluşması bir zararın meydana gelmesi sonucuna bağlanmadığı ve bu sebeple suçun tehlike suçu olduğu yönündedir[409].

Fiil unsurunda da ifade edildiği gibi bilişim sisteminin işleyişini engelleme veya bozma suçunda engelleme veya bozma eylemleri, suçun hareketini değil neticesini oluşturmaktadır. Herhangi bir eylem neticesinde sisteminin işleyişinin engellenmesi veya bozulması suçu oluşturduğu gibi netice itibariyle bir zararı da oluşturmaktadır. Çünkü sistem engellendiği ya da bozulduğu takdirde bu geçici olsa bile kullanılamaz hale gelecektir. Dolayısıyla suç bir zarar suçudur.

c. Fail

Suç teşkil eden hareketi yapan kişiye fail denir. Ceza hukukuna göre, bir kimsenin fail olabilmesi için, insan olmak ve yaşayan kişi olmak üzere iki unsurun gerçekleşmesi gereklidir[410]. Bunun sebebi de iradi hareket yeteneğinin yalnızca yaşayan insana has olmasıdır[411]. TCK'nın 20'nci maddesinde de cezaların şahsiliği ilkesi benimsendiğinden ve madde gerekçesinde de sadece gerçek kişilerin suçun faili olabileceği ve sadece gerçek kişiler hakkında ceza yaptırımı uygulanabileceği belirtildiğinden, tüzel kişiler suçun faili olamaz,

---

408 **Artuk/Gökcen/Yenidünya,** Türk Ceza Kanunu Şerhi, s.4662; **Erdoğan,** Bilişim Suçları, s.186; **Burak Çekiç,** İnternet Aracılığı İle İşlenen Suçlar, Yayımlanmamış Yüksek Lisans Tezi, Marmara Üniversitesi SBE, İstanbul, 2006, s.110 https://tez.yok.gov.tr/UlusalTezMerkezi/ (E.T: 25.11.2018).

409 **Pallı,** s. 169; **Dülger,** s.332.

410 **Demirbaş,** s.489; **Zeki Hafızoğulları/Muharrem Özen**, Türk Ceza Hukuku Genel Hükümler, US-A Yayıncılık, Ankara, 2017, s.381.

411 **Gökcen**, Belgede Sahtecilik, s.201; **Akbulut,** Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme, s.19; **Artuk/Gökcen/Alşahin/Çakır**, Genel Hükümler, s.361.

yalnızca suçtan zarar gören olabilirler[412]. Çünkü, ceza hukukunda bir kimsenin suç işlediğinden bahsedilebilmesi, onun suç teşkil eden neticeyi meydana getiren hareketi iradesi ile gerçekleştirip gerçekleştirmemesine bağlıdır. Tüzel kişiler ancak faaliyet alanlarını gösteren tüzük kapsamında eylem ve işlemlerde bulunabilir ve tüzüklerinde kanun, genel ahlak ve adaba aykırı bir düzenleme yer alamaz[413]. Bu sebeple tüzel kişiler suçun faili olamayacak ancak tüzel kişiler hakkında da güvenlik tedbirleri uygulanabilecektir.

Kanuni tipteki fiilin herkes tarafından işlenebildiği suçlara "*genel suçlar*" veya "*herkes tarafından işlenebilen suçlar*" denir[414]. Ceza kanunlarındaki suçlar kural olarak, herkes tarafından işlenebilen suçlardır. Yasa hükmünde "*kişi", "kişinin*", veya "*kimse*" ifadelerinin kullanıldığı suçlar bu niteliktedir[415].

Kanun koyucu bazen de madde metninde suçun faili olabilecek kişileri sınırlandırabilmektedir. Bu tür suçlar "*özgü suç*" olup, metinde belirtilen niteliğe sahip olmayan kişiler suçun faili olamazlar[416]. Özgü suçlar da görünüşte özgü suç ve gerçek özgü suç olmak üzere iki gruba ayrılır. Görünüşte özgü suç, temel şekli herkes tarafından, nitelikli halinin ise sadece kanuni tanımda öngörülen koşulları gerçekleştiren kişi tarafından işlenebileceği suçlar olup, gerçek özgü suçlar ise, suçun basit halinin, sadece belli kişiler tarafından işlenebileceği suçlardır[417].

Bilişim suçlarının ilk ortaya çıktığı dönemde, bilişim sistemlerinin kullanımının yaygın olmaması sebebiyle belirli niteliklere ve teknik bilgiye sahip kişiler suçun faili olabiliyorlardı. Bu sebeple doktrindeki bir görüşe göre bilişim suçlarının işlenebilmesi için yeterli düzeyde bilgi birikiminin bulunması, bu sebeple bu suçların "beyaz yaka suçları"[418]

---

412 **Dülge**r, s.248, **Berrin Akbulut,** "**Ceza Hukuku Genel Hükümler",** 4. Baskı, Adalet Yayınevi, Ankara, 2017, s.338; Özgenç, Genel Hükümler, s.207.

413 **Artuk/Gökcen/Alşahin/Çakır**, s.370.

414 **Akbulut,** Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme, s.19.

415 **Kayıhan İçel**, **"Ceza Hukuku Genel Hükümler"** Beta Basım Yayın, 5. Baskı, 2017, s.303.

416 **Artuk/Gökcen/Alşahin/Çakır**, s.291**; Demirbaş**, s.489; **Gökcen,** Belgede Sahtecilik, s.201, **Özbek/Doğan/ Bacaksız/Tepe**, s.582.

417 **Akbulut,** Genel Hükümler, s.330, **Gökcen**, 201, **Özgenç,** Genel Hükümler, s.206.

418 Beyaz yaka suçu, bir kimsenin sahip bulunduğu mesleğinden kaynaklanan sosyal statüsünü ve kendisine duyulan güveni kötüye kullanarak işlediği suç teşkil eden eylemleri ifade etmektedir. Bkz. James W. Coleman, "Respectable

içerisinde değerlendirilmesi gerekmekteyken[419], diğer görüşe göre ise bu ayırt edici bir özellik olmadığından bugün için böyle bir gereklilik bulunmamaktadır[420]. Günümüzde ikinci görüşün baskın olduğu söylenebilir zira bilişim sistemleri ile etkileşim halinde bulunmayan çok az sayıda insan kalmıştır. Her ne kadar bilişim sistemlerinin güvenlik duvarlarının aşılarak suç oluşturan eylemlerin gerçekleştirilmesi temel bilgisayar kullanım bilgisinin üzerine bir bilgi gerektirse de şu an pek çok kişi, bilişim sistemlerine yönelik suç işlemeyi sağlayan ve kolaylaştıran programlara rahatça erişebilmekte ve herhangi bir eğitim almaya ihtiyaç dahi duymadan bu suçun faili olabilmektedir[421]. Nitekim kanun koyucu da yerinde bir yaklaşımla madde metninde suçun faili olabilecek kişiler bakımından herhangi bir sınırlama getirmemiştir[422].

Bilişim sisteminin işleyişini engelleme veya bozma suçunun failinin belirlenebilmesi için, suçun bilişim sisteminin hangi unsuruna yöneldiğinin tespit edilmesi gerekir. Fiil eğer bilişim sisteminin kendisine yöneltilmişse sistemin kendisinin, verilere yöneltilmişse verilerin hem bilişim sistemine hem verilere karşı gerçekleştirilmişse her ikisinin ayrı ayrı mülkiyet, kullanım ve tasarruf haklarının kime ait olduğu ve zararı kimin meydana getirdiği ortaya konulmalıdır[423]. Eğer bilişim sisteminin maliki, sistemin kullanım hakkını başkasına devrettikten sonra, başkasına devrettiği sistemin işleyişini engeller ya da bozarsa bu suçun faili olacaktır[424].

Crime, in: Criminology", Second Edition, 1995, s.249, tercüme eden ve aktaran **Artuk/Gökcen/Yenidünya**, Türk Ceza Kanunu Şerhi, s. 4637.

419 **Aydın**, s.30; **Yazıcıoğlu,** Bilgisayar Suçları, s.30.

420 **Yenidünya/Değirmenci,** s.56-57, **Değirmenci**, Bilişim Suçları, s.174; **Koca/Üzülmez**, Özel Hükümler, s.868.

421 **Yenidünya,** s.1025, **Tezcan/Erdem/Önok,** s.1047; **Güngör**, s.82,95; **Akbulut,** Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme, s.19.

422 **Akbulut,** Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme, s.20.

423 **Dülger**, s.315, **Şaban Cankat Taşkın**, Bilişim Suçları, Beta Yayınevi, İstanbul, 2008, s.43; **Akbulut,** Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme, s.19; **Koca/Üzülmez,** Özel Hükümler, s.867.

424 **Taşkın,** Bilişim Suçları, s.50, **Erdoğan**, Bilişim Suçları, s.194.

d. Mağdur

Sözlükte mağdur, "*suçtan ve haksız eylemden zarar gören kişi*"[425] şeklinde tanımlanmıştır. Hukuki tanımlamada mağdur ile suçtan zarar gören kavramları zaman zaman aynı öznede birleşse de bu kavramlar birbirinden farklı olup birbirleri yerine kullanılamazlar[426].

Mağdur, belirli bir suçla zarara veya tehlikeye uğratılan hak veya çıkarın sahibi olan kişidir[427]. Suçtan ve olumsuz etkilerinden doğrudan etkilenir. Suç tanımıyla korunan hak ve menfaatin dışında kalan hak ve menfaatlerin ihlal edildiği hallerde, bu hak ve menfaatlerin sahipleri ise suçtan zarar görenler olarak adlandırılır[428]. Suçun mağduru ceza ilişkisinin tarafı olduğu halde, suçtan zarar gören kişi sadece hukuki ilişkinin tarafıdır[429]. Ayrıca mağdur ile suçun konusu da birbirine karıştırılmamalıdır. Mağdur, suçun konusunun ait olduğu kişidir[430].

Doktrinde suçun mağdurunun, gerçek ve tüzel kişiler olabileceği yönünde görüşler[431] bulunmakta ise de kanaatimizce suçun mağduru suçla ihlal edilen varlık ya da değerin sahibi olan ve yaşayan kişi olabileceğinden yalnızca gerçek kişiler olabilir, tüzel kişiler, korunan haklarının zarar görmesi durumunda ancak suçtan zarar gören kişi olabilirler[432].

Madde metninde suçun mağduruna ilişkin bir özellik belirtilmediğinden, bilişim sisteminin işleyişini engelleme veya bozma suçu bakımından her gerçek kişi bu suçun

---

425 http://www.tdk.gov.tr/ (E.T: 31.01.2019).

426 **Özgenç,** Genel Hükümler, s.217.

427 **Sulhi Dönmezer/Sahir Erman,** Nazari ve Tatbiki Ceza Hukuku, Genel Kısım, C.2, 11. Baskı, İstanbul Beta Yayınevi, 1997, s.331, **Özbek/Doğan/Bacaksız/Tepe,** Genel, s.195; **Yaşar/Gökcan/Artuç**, s.7288; **Özgenç**, Genel Hükümler, s.217.

428 **Erdoğan**, Bilişim Suçları, s.195.

429 **Demirbaş**, s.518; **Özgenç**, Genel Hükümler, s.217.

430 **Gökcen**, s. 203.

431 **Demirbaş**, s.518, **Erdoğan,** Bilişim Suçları, s.195.

432 **Artuk/Gökcen/Alşahin/Çakır**, s.374-375; **Artuk/Gökcen/Yenidünya**, Türk Ceza Kanunu Şerhi s.4639,4640, Dülger, s.359, **Gökcen**, s.203; **Koca/Üzülmez**, Özel Hükümler, s.868; **Tezcan/Erdem/Önok**, s.1047.

mağduru olabilir[433]. Bu suçları oluşturan hareketlerin gerçekleştirilmesi sonucunda; bilişim sistemine ve/veya verilerle oluşturulan yazılım vb. değerlere ulaşılmasında ve kullanılmasında çıkarı bulunan ve bilişim sistemi ve/veya veriler üzerinde tasarruf yetkisi bulunan kişi bu suçun mağduru olacaktır[434]. Tasarruf yetkisine sahip olmayan, verilerin ilgili olduğu kişi ise suçun mağduru değil, suçtan zarar gören kişi olacaktır[435]. Koca/Üzülmez de devlete ait bir kurumun bilişim sisteminin saldırıya uğraması halinde ise toplumu oluşturan herkesin suçun mağduru olacağı görüşündedir[436].

e. Konu

Üzerinde suçun meydana geldiği, yasada belirtilen hareketin yönelik olduğu insan veya eşyanın maddi yapısı suçun konusunu oluşturur[437]. Fail tarafından gerçekleştirilen hareket ya bir eşyaya ya da bir insanın fiziki, maddi yapısına veya bünyesine yönelir[438].

Suçun konusunun, suç ile korunan hukuki değerden farkı ise, suç konusu hareketin yöneldiği kişi ya da şey iken, korunan hukuki değerin suç tipinin düzenlenmesi ile korunmak istenen değer olmasıdır[439].

Akbulut'a göre bu suçun konusu, bilişim sisteminin işleyişidir[440].

Artuk/Gökcen/Yenidünya ise suç konusunun *"işleyişi engellenen veya bozulan bilişim sistemi*" olduğu görüşündedir[441].

---

433 **Artuk/Gökcen/Yenidünya,** Türk Ceza Kanunu Şerhi, s.4662; **Kurt,** s.; **Güngör,** s.95; **Koca/Üzülmez,** Özel Hükümler, **s.**868.
434 **Dülger**, s.414.
435 **Akbulut,** Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme, s.21.
436 **Koca/Üzülmez**, Özel Hükümler, s.868.
437 **Artuk/Gökcen/Alşahin/Çakır**, s.377; **Dülger,** s.245, **Gökcen,** s.204.
438 **Özgenç,** Gazi Şerhi, s.215; **Özgenç,** Genel Hükümler, s.213.
439 **Artuk/Gökcen/Yenidünya,** Ceza Kanunu Özel Hükümler, s.26.
440 **Akbulut,** Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme, s.24.
441 **Artuk/Gökcen/Yenidünya,** Türk Ceza Kanunu Şerhi, s. 4662.

Dülger'e göre de bilişim sisteminin işleyişinin engellenmesi ve bozulması suçunun konusunu bilişim sistemleri oluşturur[442].

Hafızoğulları/Özen, bilişim alanının sanal aleme ait olduğunu, reel aleme ait bir malvarlığı değerinin olmadığını, yasa koyucu tarafından suçun mala zarar verme suçunun düzenlendiği, kişilere karşı suçlar arasında yer almayıp topluma karşı suçlar başlığı altında düzenlediğini, bu sebeple suçun hukuki konusunun, bilişim ortamının oluşturulmasına, geliştirilmesine, sağlıklı, güvenilir işlenmesinin sağlanmasına, istenmeyen bir zarar tehlikesinin veya zararın ortaya çıkmasının önlenmesine ilişkin kamusal yarar olduğunu ifade etmiştir[443].

Kurt'a göre suçun konusu, *"bilişim sisteminin soyut ve somut bileşenleri ile sistem içinde yer alan verilerdir*" [444].

Koca/Üzülmez de bu suçun konusunu *"bilişim sisteminin işleyişinin"* oluşturduğunu düşünmektedir[445].

Özbek/Doğan/Bacaksız/Tepe de bilgi işlem faaliyeti için yazılım-donanım uyumluluğu zorunlu olduğundan suçun hukuki konusunun, bilişim sisteminin işleyişinin bir unsuru olmak koşulu ile hem yazılım hem de donanım unsurları olduğu görüşündedir[446].

244'üncü maddenin gerekçesinde de *"aracın fizik varlığı ve işlemesini sağlayan bütün diğer unsurları suçun konusunu oluşturmaktadır"* şeklinde bir açıklama yapılmıştır. Kanaatimizce de suçun konusu gerekçeyle paralel olarak bilişim sisteminin işlerliğini

---

442 **Dülger,** s.317.

443 **Zeki Hafızoğulları/Muharrem Özen**, Türk Ceza Hukuku Özel Hükümler Topluma Karşı Suçlar. US-A Yayıncılık, Ankara, 2012, s. 48.

444 **Kurt,** s. 162 benzer görüş için bkz. **Artuk/Gökcen/Yenidünya**, Türk Ceza Kanunu Şerhi, s.4662.

445 **Koca/Üzükmez,** s.868.

446 **Özbek /Doğan / Bacaksız / Tepe,** s.961, Benzer görüş için bkz. **Taşkın**, Bilişim Suçları, s.43.

sağlayan soyut ve somut bütün unsurlarıdır"[447]. Dolayısıyla çalışabilir durumda olmayan bir bilişim sistemi ya da veri taşıma aracı bu suçun konusunu oluşturmayacaktır.

f. Suçun Nitelikli Unsurları

Suçu etkileyen haller, suçun oluşmasına etki etmeyen ancak oluşan suçun daha ağır veya daha hafif sayılmasını ve sonuçta temel cezanın arttırılıp indirilmesini gerektiren, suçun niteliğine etki etmeyen nedenlerdir[448]. Burada önemli olan husus, nitelikli suçun tespiti durumunda, suçun temel halinde yer alan unsurların sağlanıp sağlanmadığıdır[449]. Yani, suçun temel halinde belirtilen unsurlar tamamlanmadan o suçun nitelikli hali oluşmayacaktır. Suçun nitelikli hali ile basit hali, suçun objektif unsurları bakımından farklılık göstermez. Nitelikli unsurlar; *"fiilin işleniş şekli, zamanı, yeri, failin ve mağdurun vasfı, fail ile mağdur arasındaki ilişki, suçun konusu ve fiilin işlenmesinde güdülen amaç"* başlıkları altında incelenebilir[450]. Kanunda bu suç için daha az cezayı gerektiren özel bir neden düzenlenmemiştir. Bu sebeple yalnızca daha fazla cezayı gerektiren haller incelenecektir.

(1) Suçun Bir Banka veya Kredi Kurumuna ya da Bir Kamu Kurum veya Kuruluşuna Ait Bilişim Sistemi Üzerinde İşlenmesi (m. 244/3)

Ülkemizde kamu kurum ve kuruluşları, hizmetlerinin neredeyse tamamını bilişim sistemleri üzerinden gerçekleştirmektedir[451]. Benzer şekilde banka ve finans kurumları da tüm ekonomik sistemin işleyişini ilişkili oldukları kamu kurumları ve kamu bankalarıyla birlikte kesintisiz bir şekilde bilişim sistemleri üzerinden gerçekleştirmektedir[452]. Bu sistemlerde meydana gelebilecek en ufak bir aksaklık, sisteme girişin engellenmesi ya da sistemin bozulması yalnızca ilgili kurumu değil toplumun da büyük bir kesimini

---

447 **Kurt**, s. 163; **Güngör**, s.96; **Dülger**, s.318.
448 **Dülger,** s.333; **Artuk/Gökcen/Alşahin/Çakır**, s.383.
449 **Dülger,** s.266.
450 **Artuk/Gökcen/Alşahin/Çakır**, s.383.
451 **Metin Turan/Özgür Külcü,** Türkiye'de Bilişim Suçlarının Tanımlanması ve Yaşanan İhlallere Yönelik İçerik analizi, Türk Kütüphaneciliği Dergisi, C:28, S:1, 2014, s.19. http://www.tk.org.tr/index.php/tk/article/viewArticle/2394 (E.T:11.06.2018).
452 **Apaydın,** s.309.

etkileyecektir. İşte bu nedenle suç konusu eylemin verebileceği zararın yoğunluğu sebebiyle kanun koyucu tarafından TCK'nın 244/3'üncü maddesi ile bilişim sistemini engelleme ve bozma suçlarının banka veya kredi kurumuna ya da kamu kurum veya kuruluşuna ait sistemler üzerinde işlenmesi halinde verilecek cezanın yarı oranında artırılacağı düzenlenmiştir.

Kamu kurum ve kuruluşları kavramı, devletin yasama, yürütme ve yargı faaliyetlerinin gerçekleştirildiği merkez ve taşra teşkilatları ile kamu hizmeti yerine getiren yerel yönetimler ve KİT'leri, yani geniş anlamda devlet aygıtını ifade etmektedir[453].

5411 sayılı Bankacılık Kanununun *"Tanımlar ve Kısaltmalar"* başlıklı 3'üncü maddesine göre;

> *"Banka; mevduat bankaları ve katılım bankaları ile kalkınma ve yatırım bankalarını,*
>
> *Mevduat Bankası; 5411 sayılı Kanun'a göre kendi nam ve hesabına mevduat kabul etmek ve kredi kullandırmak esas olmak üzere faaliyet gösteren kuruluşlar ile yurt dışında kurulu bu nitelikteki kuruluşların Türkiye'deki şubelerini,*
>
> *Katılım bankası; 5411 sayılı Kanun'a 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; 5411 sayılı Kanun'a 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*[454]*"*

ifade etmektedir. Yine 5411 sayılı Kanunun 157'nci maddesinde bu Kanuna tabi kuruluşların TCK'nın 244'üncü maddesinde tanımlanan sistemi engelleme, bozma, verileri yok etme veya değiştirme suçu açısından banka veya kredi kurumu olarak kabul edileceği

---

453 **Osman Yaşar/Hasan Tahsin Gökçan/Mustafa Artuç**, Yorumlu, Uygulamalı Türk Ceza Kanunu**,** C.:5, Ankara, Adalet Yayınevi, 2010, s.6762; **Erdoğan,** Bilişim Suçları, s.197.

454 http://www.mevzuat.gov.tr/mevzuatmetin/1.5.5411.pdf (E.T: 11.06.2018)

düzenlenmiştir ancak, Bankacılık Kanununda kredi kurumuna ilişkin bir tanımlama yapılmamıştır.

Kredi kurumuna ilişkin tanımlama TCK'nın 158'inci maddesinin gerekçesinde; *"kredi kurumu deyiminden banka olmamasına karşın, kanunen borç vermeye yetkili kurumlar anlaşılır*" şeklinde yer almaktadır.

Kamu kurum ve kuruluşlarına ait bilişim sistemlerine yönelik suçların cezasının arttırılması, öncelikle genel ceza siyasetinden ve kamuya yönelik suçların daha vahim görülmesinden kaynaklanmaktadır[455]. Örneğin, sınav giriş başvurularının yapıldığı dönemde ÖSYM'ye ait sisteme erişimin engellenmesi ya da nüfus müdürlüklerine ya da vergi dairelerine ait sistemlerin bozulması durumunda kısa bir zaman dilimi içinde dahi çok sayıda kişi bu suçtan dolayı zarar görecektir.

(2) Suçun Terör Amacıyla İşlenmesi (3713 Sayılı TMK m.4,5)

3713 sayılı Terörle Mücadele Kanununun 4'üncü maddesinde *"Aşağıdaki suçlar 1 inci maddede belirtilen amaçlar doğrultusunda suç işlemek üzere kurulmuş bir terör örgütünün faaliyeti çerçevesinde işlendiği takdirde, terör suçu sayılır"* denilmiş ve sayılı suçlar arasında bilişim alanında işlenen suçlara da yer verilmiştir[456]. Buna göre bilişim sisteminin işleyişini engelleme veya bozma suçunun terör amacıyla işlenmesi halinde terör suçu sayılacaktır.

Aynı Kanun'un *"Terör Tanımı"* başlıklı 1'inci maddesinde ise terör;

> *"Cebir ve şiddet kullanarak; baskı, korkutma, yıldırma, sindirme veya tehdit yöntemlerinden biriyle, Anayasada belirtilen Cumhuriyetin niteliklerini, siyasî, hukukî, sosyal, laik, ekonomik düzeni değiştirmek, Devletin ülkesi ve milletiyle bölünmez bütünlüğünü bozmak, Türk Devletinin ve Cumhuriyetin varlığını tehlikeye düşürmek, Devlet otoritesini zaafa uğratmak veya yıkmak veya ele geçirmek, temel hak ve*

---

455 **Karagülmez**, s.243; **Akbulut,** Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme, s.41.

456 3713 sayılı Terörle Mücadele Kanunu, 12/04/1991 tarihli 20843 sayılı Resmi Gazete'de yayımlanmış ve yayımı tarihinde yürürlüğe girmiştir.

hürriyetleri yok etmek, Devletin iç ve dış güvenliğini, kamu düzenini veya genel sağlığı bozmak amacıyla bir örgüte mensup kişi veya kişiler tarafından girişilecek her türlü suç teşkil eden eylemler" olarak tanımlanmıştır[457].

3713 sayılı Kanunun 5'inci maddesinde ise, 4'üncü maddede sayılan suçların terör amacıyla işlenmesi halinde tayin edilecek hapis cezaları veya adlî para cezalarının yarı oranında artırılacağı, bu suretle tayin olunacak cezalarda gerek o fiil için gerek her nevi ceza için muayyen olan cezanın yukarı sınırının aşılabileceği düzenlenmiştir. Ancak bu artırım çocuklar için değil 18 yaşın üstündeki kişiler için uygulanmaktadır[458]. Örneğin, Yargıtay 16. Ceza Dairesi, 26.04.2016 tarihli ve 2016/1813 E., 2016/2611 K. sayılı kararında sanığın olay tarihinde Etimesgut İlköğretim Okuluna ait etimesgutilkögretim.meb.k12.tr uzantılı web adresine girdiği, Kürdistan ve Abdullah Öcalan lehine propaganda yaparak sistemin işleyişini engellediği iddia edilen eylemde, sanığa yerel mahkemece yalnızca TCK'nın 244'üncü maddenin birinci fıkrasından ceza verilmiş olması ancak 3713 sayılı Kanunun 4/1-a maddesinde sayılan suçlardan olan üzerine atılı suçu silahlı terör örgütünün faaliyeti çerçevesinde işlemesi nedeniyle, verilen cezada aynı Kanunun 5/1 maddesi gereğince artırım yapılmamış olmasını hukuka aykırı bulmuştur.

2. Tipikliğin Manevi Unsurları

Manevi unsur, işlenen eylem ile kişi arasındaki manevi bağdır. Bu bağ kurulmadan, gerçekleştirilen davranış ceza hukuku bakımından eylem niteliği taşımayacağından, suç oluşmaz[459]. 20'nci yüzyılın başlarından itibaren gelişmeye başlayan ve bugün ceza hukukuna hakim olan yeni anlayışla birlikte kast, kusur alanından çıkarılarak haksızlığa dahil edilmiş olup taksir ve kast-taksir kombinasyonları ile suçun manevi unsurunu oluşturmaktadır[460]. Kusur ise kişi hakkındaki kınama yargısından ibaret görülmektedir[461].

---

457 http://www.mevzuat.gov.tr/MevzuatMetin/1.5.3713.pdf (E.T: 11.06.2018).
458 **Dülger,** s.274.
459 **Dülger,** s.380, **Özgenç,** Genel Hükümler, s.236; **İçel,** s.435; **Mahmut Koca/İlhan Üzülmez,** Türk Ceza Hukuku Genel Hükümler, 10. Baskı, Seçkin Yayıncılık, Ankara, 2017, s.144.
460 **Koca/Üzülmez,** s.145 vd.; **Artuk/Gökcen/Alşahin/Çakır**, s.386.
461 **Artuk/Gökcen/Alşahin/Çakır**, s.386.

TCK'nın 21'inci maddesinde kast; *"suçun oluşması kastın varlığına bağlıdır. Kast, suçun kanuni tanımındaki unsurların bilerek ve istenerek gerçekleştirilmesidir."* şeklinde tanımlanmıştır. Böylece TCK, bir suçun gerçekleşmesi bakımından esas manevi unsuru kast olarak belirlemiştir[462]. Kast; öngörülen ve suç olan bir fiili gerçekleştirmeye yönelen iradedir[463]. Kanun, kastı doğrudan ve olası kast olarak iki gruba ayrılmıştır. Failin suçun kanuni tanımındaki maddi unsurların gerçekleşebileceğini öngörmesine rağmen, hareketine devam etmesi ve fiilin olası sonuçlarını kabullenmesi halinde olası kasttan bahsedilir[464].

Bazı suç tanımlarında suçun unsurlarına ilişkin kastın yanı sıra, failin belli bir amaç doğrultusunda veya belli bir saikle hareket etmesi, bir manevi unsur olarak aranmaktadır. Amaç veya saik, kasttan önce gelen, kastı hazırlayan bir düşüncedir[465].

TCK'nın 22'nci maddesinde suçun taksirle işlenmesi hali düzenlenmiştir. Buna göre taksir; "*dikkat ve özen yükümlülüğüne aykırılık dolayısıyla, bir davranışın suçun kanuni tanımında belirtilen neticesi öngörülmeyerek gerçekleştirilmesi"* şeklinde tanımlanmıştır. Bu tanımlamada, neticenin öngörülebilir olmasından bahsedilmiş olup bu öngörememe hali sadece neticeye değil suçun bütün maddi unsurlarına yöneliktir[466]. Kast kural, taksir ise istisnadır[467]. Dolayısıyla bir suçun taksirle işlenebileceği kanunda düzenlenmemişse, suçun taksirle işlenmesi halinde fail cezalandırılamaz[468].

Bilişim sistemlerinin engellenmesi ve işleyişinin bozulması suçunun düzenlendiği 244/1'inci maddede suçun taksirli hali düzenlenmediği için yalnızca kasten işlenebilecektir[469]. Ayrıca madde metninde herhangi bir amaç ya da saik aranmamıştır bu nedenle suçun oluşması için genel kast yeterli olacaktır. Bu suçta genel kast ise,

---

462 **Artuk/Gökcen/Alşahin/Çakır**, s.391.
463 **Demirbaş,** s.342**, Özgenç**, Genel Hükümler, s.248, 249; **İçel,** s.437.
464 **Artuk/Gökcen/Alşahin/Çakır**, s.391.
465 **Özgenç,** Genel Hükümler, s.303.
466 **Artuk/Gökcen/Alşahin/Çakır**, s.433.
467 **İçel**, s.452; **Koca/Üzülmez,** Genel Hükümler, s.144.
468 **Artuk/Gökcen/Yenidünya**, Türk Ceza Kanunu Şerhi, s.4662; **Kurt,** s.175; **Özgenç**, Genel Hükümler s.259 vd; **İnci Biçkin,** Siber Suç Sözleşmesi ve 5237 Sayılı Türk Ceza Kanununda Bilişim Suçları, Yargıtay Dergisi, C:32, S:1-2, 2006, s.157.
469 **Akbulut,** Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme, s.40.

gerçekleştirilen eylem ile bilişim sisteminin işleyişinin engellenmesi veya bozulmasıdır. Suçun doğrudan kastla işlenebileceğine ilişkin bir düzenleme bulunmadığından, olası kastla da işlenebilir[470]. Sanal Ortamda İşlenen Suçlar Sözleşmesinde de bilişim sistemine yönelik işlenen suçların kasten işlenebileceği öngörülmüştür.

3. Hukuka Aykırılık Unsuru

a. Genel Olarak

Hukuka aykırılık, işlenen ve kanundaki suç tipini ihlal eden harekete hukuk düzenince cevaz verilmemesi, bu fiilin mubah sayılmaması, bu hareketin sadece ceza hukukuyla değil, tüm hukuk düzeniyle çelişki halinde bulunması anlamına gelmektedir[471]. Ortada ihlal edici bir davranış bulunmadığında ödeve aykırılık bilinci ya da belli bir davranış ya da neticenin gerçekleştirilmesine yönelik irade mevcudiyeti yeterli değildir[472]. Hukuka aykırılık bilinci, failin davranışının hukuka aykırılık oluşturduğunu bile bile o hareketi yapması demektedir[473].

Suç tipinde hukuka aykırılığın ayrıca belirtilmesine, "hukuka özel aykırılık" denir ve burada suçun oluşması için failin bu hukuka aykırılık sebebini bilmesi aranmaktadır[474]. Yani failin kusurunun, hukuka özel aykırılık unsurunu da kapsaması gerekmektedir. Başka bir deyişle, ilgili suç tanımında fiilin hukuka aykırılığına özellikle işaret edilmiş olan hallerde, bu suç ancak doğrudan kastla işlenebilir[475]. Dolayısıyla failin hukuka aykırı hareket ettiğini bildiği tespit edilmedikçe, hukuka aykırılık unsuru ve suç oluşmaz. Sanal Ortamda İşlenen Suçlar Sözleşmesi'nde bilişim alanında işlenen suçlarda özel hukuka aykırılık aranmıştır. Buna göre, hukuka aykırılık amacı taşımayan ve sistemin güvenliği için internete

---

470 **Artuk/Gökcen/Yenidünya,** Türk Ceza Kanunu Şerhi, s.4663.

471 **Artuk/Gökcen/Alşahin/Çakır**, s.482, **Yenidünya/Değirmenci**, s.70, **Demirbaş,** s.244, **Dülger** s.384, **Özgenç,** Genel Hükümler, s.305 vd; **İçel,** s.313; **Mahmut Koca,** YTCK'da Hukuka Uygunluk Nedenleri, Ceza Hukuku Dergisi, Y:1, S:1, 2006, s.155, 116.

472 **Apaydın,** s.311

473 **Nur Centel/Hamide Zafer/Özlem Çakmut,** "Türk Ceza Hukukuna Giriş", 8. Basım, Beta Yayıncılık, İstanbul 2014, s.392.

474 **Centel/Zafer/Çakmut,** s.393; **Özgenç,** Genel Hükümler, s.312 **Yenidünya,** s.1038; **Erdoğan,** Bilişim Suçları, s.158. Hukuka özel aykırılık unsurunu kabul etmeyen görüş için bkz. **Dülger**, s.281 vd.

475 **Demirbaş**, s.249, **Özgenç**, Genel Hükümler, s.312.

erişimi engelleyen bir programın yerleştirilmesi gibi eylemler suç oluşturmayacaktır[476]. Ancak, TCK'nın 244'üncü maddesinin birinci fıkrasında suçun oluşması için hukuka özel aykırılık aranmamıştır.

b. Hukuka Uygunluk Sebepleri

Hukuka uygunluk sebepleri, hukuka aykırılığı ortadan kaldırarak, fiili hukukun uygun saydığı bir hareket haline getirirler[477]. Bu sebepler objektif bir etkiye sahip olup, sadece var olmaları etkilerini göstermeleri için yeterlidir[478]. TCK'da hukuka uygunluk sebepleri olarak; kanun hükmünün yerine getirilmesi (TCK m.24/1), meşru müdafaa (TCK m.25/1), hakkın icrası (TCK m.26/1) ve ilgilinin rızası (TCK m.26/2) yer almaktadır[479]. İnceleme konusu suç bakımından, kanun hükmünün yerine getirilmesi, meşru müdafaa ve ilgilinin rızası hukuka uygunluk sebepleri söz konusu olabilir.

TCK'nın 24'üncü maddesinin birinci fıkrasında kanun hükmünü yerine getiren kişilerin cezalandırılamayacağı öngörülmüştür. Burada önemli olan husus, yerine getirilen görevin kaynağının doğrudan kanun olması gerektiğidir. Örneğin CMK'nın 134'üncü[480] maddesi gereğince, soruşturma kapsamında delil elde etme amaçlı olarak kamu görevlisinin

---

476 **Apaydın,** s.312.

477 **Artuk/Gökcen/Alşahin/Çakır**, s.492.

478 **Yenidünya/Değirmenci,** s.71; **Artuk/Gökcen/Yenidünya**, Ceza Hukuku Özel Hükümler, s.53.

479 **Özgenç**, Genel Hükümler, s.294.

480 CMK m.134: (1) Bir suç dolayısıyla yapılan soruşturmada, somut delillere dayanan kuvvetli şüphe sebeplerinin varlığı ve başka surette delil elde etme imkânının bulunmaması halinde, hâkim veya gecikmesinde sakınca bulunan hâllerde Cumhuriyet savcısı tarafından şüphelinin kullandığı bilgisayar ve bilgisayar programları ile bilgisayar kütüklerinde arama yapılmasına, bilgisayar kayıtlarından kopya çıkarılmasına, bu kayıtların çözülerek metin hâline getirilmesine karar verilir. Cumhuriyet savcısı tarafından verilen kararlar yirmi dört saat içinde hâkim onayına sunulur. Hâkim kararını en geç yirmi dört saat içinde verir. Sürenin dolması veya hâkim tarafından aksine karar verilmesi hâlinde çıkarılan kopyalar ve çözümü yapılan metinler derhâl imha edilir.
(2) Bilgisayar, bilgisayar programları ve bilgisayar kütüklerine şifrenin çözülememesinden dolayı girilememesi veya gizlenmiş bilgilere ulaşılamaması ya da işlemin uzun sürecek olması halinde çözümün yapılabilmesi ve gerekli kopyaların alınabilmesi için, bu araç ve gereçlere elkonulabilir. Şifrenin çözümünün yapılması ve gerekli kopyaların alınması halinde, elkonulan cihazlar gecikme olmaksızın iade edilir.
(3) Bilgisayar veya bilgisayar kütüklerine elkoyma işlemi sırasında, sistemdeki bütün verilerin yedeklemesi yapılır.
(4) Üçüncü fıkraya göre alınan yedekten bir kopya çıkarılarak şüpheliye veya vekiline verilir ve bu husus tutanağa geçirilerek imza altına alınır.
(5) Bilgisayar veya bilgisayar kütüklerine elkoymaksızın da, sistemdeki verilerin tamamının veya bir kısmının kopyası alınabilir. Kopyası alınan veriler kâğıda yazdırılarak, bu husus tutanağa kaydedilir ve ilgililer tarafından imza altına alınır.

yapmış olduğu işlemler, kanun tarafından verilen bir yetkiye dayanılarak gerçekleştirildiğinden suç oluşmayacaktır[481].

TCK'nın 25'inci maddesinde ise meşru müdafaa hali düzenlenmiştir. Bu düzenlemeye göre, kendisine veya başkasına ait bir hakka yönelmiş, gerçekleşen, gerçekleşmesi veya tekrarı muhakkak olan haksız bir saldırıyı o anda hal ve koşullara göre saldırı ile orantılı biçimde defetme zorunluluğu ile işlenen fiillerden dolayı faile ceza verilemeyecektir. Meşru müdafaanın oluşması için öncelikle bir saldırının bulunması gerekir. Burada saldırının cebir, tehdit, şiddet içermesi zorunlu değildir, önemli olan savunmayı gerektiren, hukuken fiil olarak nitelendirilebilecek bir saldırının varlığıdır[482]. Yine bu saldırının haksız olması gerekmektedir ancak suç teşkil etmesi gerekmez[483]. Bu saldırının bir hakka yönelmiş olması gerekir. TCK'da hakkın niteliği konusunda bir değerlendirme yapılmamıştır ancak hukuken korunan haklar, kişilere tanınan hukuki, şahsi haklardır ve yalnızca bireysel nitelikteki hukuki değerlere yönelik (beden bütünlüğü, şeref, özel yaşamın gizliliği gibi) saldırılar savunmaya konu olabilir[484]. Meşru savunmanın olabilmesi için saldırının devam ediyor olması ve savunmada zorunluluk bulunması gerekmektedir. Savunmanın haklı kabul edilmesi, başka türlü saldırıdan kurtulma imkanının bulunmamasına bağlıdır[485]. Savunmaya yönelik hareketin zorunlu olup olmadığının değerlendirilmesi, somut olayın özelliklerine göre belirlenebilirse de, bu değerlendirmede saldırıya uğrayan hakka yönelik tehlikeyi kesin olarak ve derhal ortadan kaldırıp kaldırmadığına bakılır[486]. Avşar/Öngören, kişilerin kendileri hakkında hakaret içeren ya da suçlayıcı beyanlar bulunan web sitesini engellemesi halinde meşru müdafaa hukuka uygunluk hali gerçekleşeceğinden suçun oluşmayacağı görüşündedir[487]. Kanaatimizce bu durumda somut olaya göre

---

481 **Dülger**, s.436, **Mehmet Burak Kızıltan**, 5237 Sayılı Türk Ceza Kanununda Bilişim Sistemine Girme, Sistemi Engelleme ve Bozma Suçları, Yayımlanmamış Yüksek Lisans Tezi, İstanbul Üniversitesi SBE, İstanbul, 2007, s.85 https://tez.yok.gov.tr/UlusalTezMerkezi/ (E.T: 25.11.2018).

482 **Artuk/Gökcen/Alşahin/Çakır**, s.504.

483 **Hakan Hakeri**, Ceza Hukuku Genel Hükümler, Adalet Yayınevi, 21. Baskı, Ankara, 2017, s.341.

484 **Artuk/Gökcen/Alşahin/Çakır**, s.507.

485 **Hakeri,** s.344.

486 **Artuk/Gökcen/Alşahin/Çakır**, s.511.

487 **Zakir Avşar/Gürsel Öngören,** "Bilişim Hukuku", Türkiye Bankalar Birliği Yayını, Yayın No:270, İstanbul, s.138. https://www.tbb.org.tr/Content/Upload/Dokuman/801/BILISIM_HUKUKU.pdf (E.T: 07/02/2019)

değerlendirme yapılması gerekmektedir. 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanunun 8'inci maddesinde erişiminin engellenmesine kimlerin hangi yöntemle karar vereceği düzenlenmiştir. Kanunun öngördüğü haller ve kişiler dışında gerçekleştirilen, sistemlerin işleyişine yönelik eylemler suç oluşturacaktır. Ancak, mevcut saldırı ve etkileri değerlendirildiğinde başka türlü saldırıyı ortadan kaldırmanın mümkün olmadığı durumlarda saldırganın yaptığı eyleme müdahale edebilmek için bilişim sistemini engelleme ya da bozma meşru müdafaa kapsamında değerlendirilmelidir.

Bir diğer hukuka uygunluk sebebi ise ilgilinin rızasıdır. TCK'nın 26'ncı maddesinde, kişinin üzerinde mutlak surette tasarruf edebileceği bir hak üzerinde, kişinin rızası çerçevesinde işlenen fiillerden dolayı kimseye ceza verilemeyeceği düzenlenmiştir. Bilişim sisteminin işleyişinin engellenmesi veya bozulması durumunda, sistem üzerinde hak sahibi olan kişinin rızasının bulunması halinde, sistemin engellenmesi veya bozulması eylemini gerçekleştiren kişi cezalandırılmayacaktır. Örneğin, sistemin saldırılara dayanıklılığının test edilmesi amacıyla engellenmesi halinde, sistem üzerinde hak sahibi olan kişinin rızası doğrultusunda bu eylemi gerçekleştiren teknik sorumlu cezalandırılmayacaktır. Ancak suç, şikâyete bağlı olmadığından, mağdurun rızasının eylem öncesinde elde edilmiş olması gerekmektedir[488]. Ayrıca verilen rızanın da hata, hile, cebir, korkutma gibi sebeplerle sakatlanmamış bir irade sonucunda verilmiş olması gerekmektedir[489].

D. SUÇUN ÖZEL GÖRÜNÜŞ ŞEKİLLERİ

1. Teşebbüs

Sözlükte girişim olarak tanımlanan teşebbüs, ceza hukukunda suç tanımında belirlenmiş olan fiilin icrasına elverişli hareketlerle başlanmış olmakla birlikte bu fiile ilişkin icra hareketlerinin tamamlanamaması veya icra hareketleri tamamlanmış olmakla birlikte,

---

488 **Erdoğan,** Bilişim Suçları, s.165, **Dülger,** s.391.
489 **Artuk/Gökcen/Alşahin/Çakır**, s.549 vd.

suç tipinde ayrı bir unsur olarak belirlenmiş olan hallerde neticenin gerçekleşmemiş bulunmasını ifade etmektedir[490]. Suça teşebbüs, TCK'nın 35'inci maddesinde düzenlenmiştir. Buna göre; *"kişi, işlemeyi kastettiği bir suçu elverişli hareketlerle doğrudan doğruya icraya başlayıp da elinde olmayan nedenlerle tamamlayamaz ise teşebbüsten dolayı sorumlu tutulur."*

Bir kişinin teşebbüsten dolayı sorumlu tutulabilmesi için suç işleme kastıyla hareket etmesi, suçu işlemeye yönelik hareketleri yapmaya başlaması ve elinde olmayan nedenlerden dolayı suç tanımında yer alan eylemlerin tamamlanamamış olması gerekmektedir[491]. Belli bir suçu işlemeye teşebbüs eden failin kastı, söz konusu suçun tamamlanmasına yöneliktir[492].

Fail madde metninde yer alan eylemlerden birisini gerçekleştirince suç oluşur, bu eylemlerden birden fazlasının yapılması suç çokluğunu etkilemez[493]. Fail, eylemlerden birisini tamamlayıp diğerini tamamlayamazsa, faile tamamlanmış suçtan ceza verilmelidir[494]. Failin, bilişim sisteminin işleyişini bozma veya engelleme için icra hareketlerine başlayıp elinde olmayan nedenlerle, engelleme veya bozma sonucunu gerçekleştiremezse, suç teşebbüs aşamasında kalmış sayılacaktır[495].

Suçu tamamlama imkanına sahip failin, kendi iradesiyle icra hareketlerinin tamamlanmasından vazgeçmesi halinde TCK'nın 36'ncı maddesinde düzenlenen gönüllü vazgeçme durumu ortaya çıkacaktır. Bu düzenlemeye göre; *"Fail, suçun icra hareketlerinden gönüllü vazgeçer veya kendi çabalarıyla suçun tamamlanmasını veya neticenin gerçekleşmesini önlerse, teşebbüsten dolayı cezalandırılmaz; fakat tamam olan kısım esasen bir suç oluşturduğu takdirde, sadece o suça ait ceza ile cezalandırılır".* Dolayısıyla bilişim sisteminin işleyişini engelleme veya bozma suçu bakımından

---

490 **Artuk/Gökcen/Alşahin/Çakır**, s.676.
491 **Özgenç,** Genel Hükümler, s.417 vd.
492 **Özgenç,** Genel Hükümler, s.483; **Dülger**, s.293.
493 **Akbulut,** Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme, s.43.
494 **Yaşar/Gökcan/Artuç,** s. 6768; **Artuk/Gökcen/Yenidünya**, Şerh, s.4663.
495 **Erdoğan,** Bilişim Suçları, s.202; **Artuk/Gökcen/Yenidünya**, Türk Ceza Kanunu Şerhi, s.4664; **Yaşar/Gökcan/Artuç**, s.6768.

değerlendirildiğinde, fail bu suçu işlemek amacıyla sisteme girip, sistemi engelleyici ya da bozucu bir hareket yapmadan, vazgeçerek çıkarsa o ana kadarki eylemi TCK'nın 243'üncü maddesi kapsamında bilişim sistemine girme veya kalma suçunu oluşturacağından faile 244/1'inci maddeye teşebbüsten değil 243'üncü maddeden ceza tayin edilmesi gerekir[496].

TCK'da ayrıca, failin icra hareketlerini tamamlamasından sonra, neticenin gerçekleşmesine isteyerek engel olması hali "etkin pişmanlık" olarak düzenlenmiştir. Ancak bu durum belli suçlar için özel olarak düzenlenmiş olup, gönüllü vazgeçme gibi genel nitelikte değildir. TCK'nın 244'üncü maddesi için etkin pişmanlık hükmü düzenlenmediğinden failin bundan faydalanması mümkün değildir.

4. İştirak

İştirak; "s*uçun varlığı için normda gerekli olandan fazla failin, bir suçu birlikte işlemesi"* olarak tanımlanmıştır[497]. Başka bir ifadeyle, tek kişi ile işlenmesi olanaklı olan bir suçun, birden fazla kişi tarafından ortak bir irade ve bu iradenin planı dahilinde hareket edilerek gerçekleştirilmesidir[498]. Dolayısıyla suçun varlığı açısından zorunlu değildir, suçun ortaya çıkış bir başka deyişle suçun işleniş biçimidir[499].

Fail, kanunda tanımlanan suçu icra eden kişidir[500]. Bazı suçlar zorunlu olarak ancak birden fazla failin katılımı ile gerçekleşebilir. Bu suçlara çok failli suçlar denir[501]. Bu suçlarda fail sayısı suçun oluşumu bakımından önem taşır. Suçun birden fazla kişiyle birlikte işlenmesi halinde suç ortaklarının hepsinin belirli ölçülerde de olsa eyleme olan katkılarından dolayı sorumlulukları bulunmaktadır[502].

---

496 **Erdoğan,** Bilişim Suçları, s.202.
497 **Artuk/Gökcen/Alşahin/Çakır,** s.643.
498 **Fatih Selami Mahmutoğlu,** Kusurluluk Prensibi Açısından Azmettirenin Ceza Sorumluluğu, İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, C:63, S:1-2, 2005, s.57.
499 **Devrim Aydın,** Türk Ceza Hukunda İştirak, Yayımlanmamış Doktora Tezi, Ankara Üniversitesi Sosyal Bilimler Enstitüsü , Ankara, 2008, s.20 https://tez.yok.gov.tr/UlusalTezMerkezi/ (E.T: 25.11.2018).
500 **Gökcen**, s.279.
501 **Artuk/Gökcen/Yenidünya,** Ceza Hukuku Özel Hükümler, s.67.
502 **Dülger,** s.402.

TCK'nın 37'nci maddesinde, *"Suçun kanuni tanımında yer alan fiili birlikte gerçekleştiren kişilerden her biri fail olarak sorumlu tutulur"* şeklinde bir düzenleme ile müşterek faillik kurumuna yer verilmiştir. Dolaylı faillik ise madenin devamında *"Başka bir kimseyi üzerinde etkinlik kurmak suretiyle suç işlemekte araç olarak kullanan kişi dolayısıyla faildir."* şeklinde tanımlanmıştır. Kusur yeteneği bulunmayan veya cebir, tehdit veya hileye maruz kalmak suretiyle kusur yeteneği ortadan kalkmış olan ya da şahsi cezasızlık sebebi bulunan kişinin suç işlemek için amaç olarak kullanılması halinde dolaylı faillik söz konusu olacaktır[503].

TCK'nın 244/1'inci maddesinde yer alan bilişim sisteminin işleyişini engelleme veya bozma suçunda iştirak türlerinin hepsinin gerçekleşmesi mümkündür. Yani bu suç, iştirak açısından biz özellik göstermez[504].

5. Suçların İçtimaı

Ceza hukukunda temel kural; kaç tane fiil varsa o kadar suç, kaç tane suç varsa o kadar ceza vardır[505]. Hareket ile suç arasındaki ilişki, işlenen suçun, başka bir suçun unsuru ya da ağırlatıcı nedeni olması (TCK m.42 – bileşik suç); bir suç işleme kararıyla değişik zamanlarda, bir kişiye karşı, aynı suçun birden fazla kez işlenmesi (TCK m.43/1 – zincirleme suç); aynı suçun birden fazla kişiye karşı, tek bir fiille işlenmesi (TCK m.43/2 – zincirleme suç); tek bir fiille birden fazla suçun işlenmesi (TCK m.44 – fikri içtima) gibi şekillerde ortaya çıkmaktadır.

Bu suç açısından değerlendirilecek ilk husus zincirleme suçun oluşup oluşmayacağıdır. Bilişim sisteminin işleyişini engelleme ve bozma fiili, bir suç işleme kararının icrası kapsamında değişik zamanlarda aynı kişiye karşı birden fazla işlenirse,

---

503 **Centel/Zafer/Çakmut,** s.502, **Koca/Üzülmez,** Özel Hükümler, s.453, **İçel,** s.556.

504 **Mustafa Özen**, Suçların İçtimaı (Zincirleme Suç – Fikri İçtima – Bileşik Suç), Yayımlanmamış Doktora Tezi, Ankara Üniversitesi SBE, Ankara, 2008, s.7 https://tez.yok.gov.tr/UlusalTezMerkezi/ (E.T: 25.11.2018); **Neslihan Göktürk**, "Türk Hukuku'nda Suçların İçtimaı", Ceza Hukuku ve Kriminoloji Dergisi, C.2, S:1-2, 2014, s. 31, http://dergipark.gov.tr/download/article-file/14656 (E.T:19.04.2019); **Artuk/Gökcen/Yenidünya**, Türk Ceza Kanunu Şerhi, s.4664; **Erdoğan**, Bilişim Suçları, s.202; **Koca/Üzülmez,** Özel Hükümler**,** s.874.

505 **Demirbaş,** s.72.

zincirleme suç söz konusu olacaktır[506]. Bu durumda faile TCK'nın 43'üncü maddesi gereğince tek suçtan dolayı, cezanın artırılarak verilmesi gerekir. Ancak failin icra hareketleri arasında tek suç işleme kararından bahsedilemeyecek kadar uzun aralıklar varsa burada her eylem için ayrı ceza verilip cezaların içtimaı kuralının uygulanması gerekir[507]. Zincirleme suçun sübjektif koşulu, işlenen birden fazla suç arasında bir manevi bağın bulunmasıdır. Bu fiiller bir suç işleme kararının icrası kapsamında işlenmektedir. Burada manevi bağın tespiti her bir olayın somut işleniş koşullarına göre hâkim tarafından tespit edilecektir[508].

Yine bu suçun tek bir fiille birden fazla bilişim sisteminin engellenmesi ya da bozulması sonucunu doğuracak şekilde işlenmesi halinde TCK'nın 43/2'nci maddesinde yer alan zincirleme suç hükmü uygulanacaktır.

Suçun maddi unsuruna ilişkin yapılan değerlendirmede de belirtildiği üzere bilişim sisteminin işleyişini engelleme veya bozma suçu mütemadi bir şekilde işlenebilen bir suçtur. Bu durumda suç, temadinin kesildiği anda gerçekleşmiş olur ve zamanaşımı bu andan itibaren işlemeye başlar.

Bu konuda üzerinde durulması gereken bir diğer önemli nokta da TCK'nın 243'üncü maddesinde düzenlenen hukuka aykırı olarak bilişim sistemine girme veya kalmaya devam etme suçunun, 244/1'inci maddede düzenlenen bilişim sisteminin işleyişini engelleme veya bozma suçu bakımından geçit suç olup olmadığıdır.

Doktrinde bu konuyla ilgili farklı görüşler bulunmaktadır. Yaşar/Gökcan/Artuç'a göre; *"Bilişim sistemine girmenin araç suç olarak düzenlendiği veya bilişim sistemine girerek veya bu sistem kullanılarak suçun işlenmesinin suçun unsuru veya nitelikli hal sayıldığı durumlarda, ayrıca faile bilişim sistemine girme suçundan da ceza verilemez."*[509].

---

506 **Artuk/Gökcen/Yenidünya**, Türk Ceza Kanunu Şerhi, s.4664; **Akbulut,** Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme, s.44.

507 **Dülger**, s.402.

508 **Özgenç,** Genel Hükümler, s.604.

509 **Yaşar/Gökcan/Artuç,** s.6752.

Artuk/Gökcen/Yenidünya da,

"*Bilişim sistemine hukuka aykırı erişim ve sistemde kalmaya devam etme, bilişim sistemlerine girerek işlenmesi zorunlu bulunan başka bilişim suçlarının işlenmesi için bir araçtır. Bu itibarla 243'üncü maddede yer alan suç, daha sonra işlenen suçlar bakımından bir geçit olma özelliği taşıt ve fail sadece amaç suçtan dolayı cezalandırılır."* şeklinde benzer bir görüşe sahiptir[510].

Dülger ise burada geçit suç oluşmayacağı görüşündedir. Bu yazara göre;

"*Hukuka aykırı olarak bilişim sistemine girme veya sistemde kalma suçu inceleme konusu suç tipi açısından geçit suçu oluşturmaz. Zira 244. Maddenin 1. Ve 2. Fıkralarındaki suçların mutlaka 243. Maddedeki eylem gerçekleştirilmek suretiyle işlenmesi gerekmez. Dolayısıyla failin bu suçu işlemek için 243. Maddedeki suçu da işlemesi halinde faile her iki suçtan da ayrı ayrı ceza verilmesi gerekir"* [511].

Kanaatimizce, fail bilişim sisteminin işleyişini engellemek veya bozmak için TCK'nın 243'üncü maddesinde düzenlenen hukuka aykırı olarak bilişim sistemine girme veya kalmaya devam etme suçunu işlemişse, bir hareketle birden fazla suçun oluşmasına sebep olduğundan TCK'nın 44'üncü maddesi gereğince farklı neviden fikri içtima kuralları uygulanmalı ve bu iki suçtan, daha ağır cezanın öngörüldüğü sistemin işleyişini engelleme veya bozma suçundan dolayı cezalandırılmalıdır[512].

Sistemin, sistemde yer alan verilere müdahale sonucu bozulması durumunda TCK'nın 244/1 ve 2'nci fıkralarından hangisinin uygulanacağı sorunu ortaya çıkacaktır. Sistemin işleyişi, sistemin tümüne yönelen herhangi bir hareketle bozulabileceği gibi,

---

510 **Artuk/Gökcen/Yenidünya,** Türk Ceza Kanunu Şerhi, s.4655.

511 **Dülger,** s.338.

512 **Güler,** s.34; **İsmail Gürocak,** Bilişim Sistemine Girme Suçu (TCK m.243), http://www.ismailgurocak.av.tr/makale/ (E.T: 18.12.2018). Koca bu konuda ki açıklamalarında "*Kanaatimizce bu gibi hallerde tek fiille birden çok farklı suçun işlenmesi anlamına gelen, farklı neviden fikri içtimanın (TCK m. 44) varlığını kabul etmek gerekir. Fikri içtimada bir suçun icra hareketlerinin bir başka suçun icra hareketleriyle kısmen veya tamamen örtüşmesi gerekli ve yeterlidir. Bir bilişim sitemindeki verileri değiştirmek isteyen fail, bu su0çun icra hareketlerini gerçekleştirirken sisteme de girmekte ve dolayısıyla 243'üncü maddeyi de ihlal etmektedir. Bu itibarla failin bu suçlardan yalnızca en ağır cezayı gerektiren 244'üncü maddedeki suçtan dolayı cezalandırılması gerekecektir"* demektedir (**Mahmut Koca,** Hukukumuzda TCK'nın 244. Maddesi Kapsamında Bilişim Sistemini Engelleme, Bozma, Verileri Yok Etme veya Değiştirme Suçu, T.C. Yargıtay Başkanlığı, Bilişim Hukuku Konferansı (09-10 Ekim 2008), Ankara, s.96).

sistemde yer alan verilere veya sistemin diğer unsurlarına yönelen hareketlerle de bozulabilir[513]. Özellikle sistemde yer alan verilere yapılan müdahaleler yönünden, müdahalenin sistemin işleyişini engellememesi veya bozmaması halinde 244/2'nci maddesinin, müdahalenin sistemin işleyişini engellemesi veya bozması halinde fikri içtima kuralları gereğince TCK'nın 244/1'inci maddesinin uygulanması gerektiğini düşünüyoruz.

Bilişim sisteminin engellenmesi veya bozulmasına yönelik eylemlerin aynı zamanda TCK'nın 124'üncü maddesinde düzenlenen haberleşmenin engellenmesi suçunu oluşturması durumunda yine fikri içtima kuralları gereğince daha ağır cezayı içeren TCK'nın 244'üncü maddesinin uygulanması gerekmektedir.

Doktrinde suçun bilişim sistemlerinin fiziki unsurlara karşı, fiziki hareketle gerçekleştirilebilip gerçekleştirilemeyeceği hususu da tartışılmaktadır. Böyle bir durumda hangi maddenin uygulanacağına ilişkin TCK'nın 151'inci maddesinde yer alan mala zarar verme suçu ile TCK'nın 244/1'inci maddesinde yer alan bilişim sisteminin işleyişinin engellenmesi veya bozulması suçu arasındaki ilişki bakımından görüş farklılıkları bulunmaktadır. Mahmutoğlu'na göre,

> "*bu suçla korunan hukuksal değer soyut olarak sadece veriler olmayıp aynı zamanda somut olarak bilişim sistemine ait donanımlardır. Bu sebeple bilişim sisteminin donanımlarına zarar verilmesi halinde hem mala zarar verme hem de TCK md.244 oluşacaktır. Buradaki sorun özel normun genel norma önceliği prensibi gereği bilişim sistemini özel olarak koruyan bir norm olan TCK md.244'ün uygulanması ile çözülecektir*."[514].

Özgenç, sistemin somut unsurlarına verilen zararlar, mala zarar verme suçu, sistemin fiziki varlığına zarar vermeksizin elektronik ortamda verilen zararlar ise bilişim suçu oluşturacağını ifade etmiştir[515].

---

513 **Erdoğan,** Bilişim Suçları, s.173.

514 **Fatih Selami Mahmutoğlu,** Türk Ceza Kanununda Yer Alan Bilişim Alanındaki Suçlar ve Karşılaşılan Sorunların Yargı Kararları Işığında Değerlendirilmesi, İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, C:71 S:1, 2013, s.19.

515 **Özgenç**, Gazi Şerhi, s. 989.

Artuk/Gökcen/Yenidünya'ya göre; *"Bilişim sisteminin işleyişinin bozulması, TCK'nın 151 inci maddesinde yer alan mala zarar verme suçunu da oluşturmaktadır. Bu ihtimalde TCK'nın 44 üncü maddesi uyarınca bir sonuca ulaşılması yerinde olur."*[516].

Kurt ise, failin asıl amacının bilişim sistemini bozmak olduğu durumlarda eylemin fiziki saldırı şeklinde gerçekleştirilmesi halinde, tek bir fiil ile TCK'nın 151'inci ve 244'üncü maddeleri ihlal edileceğinden, fikri içtima hükümleri uygulanarak en ağır cezayı gerektiren suçtan hüküm kurulması gerektiğini ifade etmektedir[517].

Dülger'e göre "*mala zarar verme suçunda suçun konusunu başkasının taşınır ya da taşınmaz malı oluşturur. Bilişim alanındaki suçun konusu ise bilişim sistemidir. Bu nedenle iki madde birbirinden tamamen farklı iki suç tipini düzenler ve aralarında genel – özel hüküm ilişkisi bulunmamaktadır."*[518].

Erdoğan bu konudaki görüşünü;

> *"244/1 madde metninde sistemin işleyişinin engellenmesi veya bozulması sonucunu doğuracak eylemlere ilişkin bir sınırlama getirilmemiştir. Bu nedenle failin kastı, doğrudan bilişim sisteminin işleyişine dönükse, soyut unsurlara zarar verilmesi halinde doğrudan TCK 244/1 maddesi tatbik edilmelidir; somut unsurlara zarar verilmesi halinde ise fail tek eylemle hem mala zarar vermeyi düzenleyen 151. Maddeyi hem de 244/1. Maddeyi ihlal etmiş olduğundan fikri içtima hükümleri uygulanarak daha ağır cezayı gerektiren 244. Madde uygulanmalıdır"* şeklinde ifade etmektedir[519].

Bilişim sistemi, hem soyut hem de fiziki unsulardan oluştuğundan, yalnızca sistemin soyut yani yazılım unsuruna yapılan müdahale ile değil aynı zamanda donanım unsuruna yapılan müdahalelerle de gerçekleşebilmektedir. Dolayısıyla bilişim sisteminin donanım unsuruna yapılan müdahaleler, sistemin işleyişini engelleme veya bozma kastıyla yapılmış ve bu sonucu doğmuşsa, burada bir eylemle iki suç oluştuğundan bilişim sisteminin

---

516 **Artuk/Gökcen/Yenidünya,** Ceza Hukuku Özel Hükümler, s.700.
517 **Kurt**, s.165
518 **Dülger,** s.338
519 **Erdoğan,** Bilişim Suçları, s.175, 176

işleyişinin engellenmesi suçu ile TCK'nın 151'inci maddesinde yer alan mala zarar verme suçu arasında içtima ilişkisi oluşacağı ve bu durumda daha ağır cezayı öngören 244'üncü maddenin uygulanması gerektiği düşüncesindeyiz.

TCK'nın 245/A maddesinde, 244'üncü maddede yer alan suçların işlenmesi için bir cihazın, bilgisayar programının, şifrenin veya sair güvenlik kodunun 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 kişinin cezalandırılacağı öngörülmüştür. Bu durumda fail bu eylemleri gerçekleştirdikten sonra, 244/1'inci maddede yer alan suçu da işlemişse bu durumda gerçek içtima hükümleri uygulanacak ve fail her iki suçtan dolayı da cezalandırılacaktır[520].

E. KUSURLULUK

Kusurluluk, suçun yapısı açısından tipikliğin maddi ve manevi unsurları ile hukuka aykırılık unsurunun varlığının tespitinden sonra, üçüncü aşamada suçun gerçekleşip gerçekleşmediği açısından değil, failin kınanabilirliği açısından incelenir[521]. Buna göre, cezalandırılabilmesi için failin yalnızca tipiklik ile hukuka aykırılık unsurunu gerçekleştirmesi yeterli değildir; ayrıca işlemiş olduğu eylemden dolayı kınanabilmesi de gerekir[522].

Ceza sorumluluğunun esası kusura dayanmaktadır[523]. Bir kişinin kusurlu kabul edilebilmesi için, kusur yeteneğine sahip olmalı ve somut olayda kusurluluğu kaldıran hallerden biri var olmamalıdır[524]. Kusur yeteneği, failin işlediği fiilin hukukî anlam ve sonuçlarını algılama veya bu fiille ilgili olarak davranışlarını yönlendirmeyle ilgili iken, isnat

---

520 **Akbulut,** Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme, s.47; **Akbulut,** Bilişim Alanında Suçlar, s.212.

521 **Artuk/Gökcen/Alşahin/Çakır,** s.570, **Özgenç**, Gazi Şerhi, s.245, **İçel,** s.409; **Dülger,** s.288.

522 **Koca/Üzülmez,** Genel Hükümler, s.306.

523 **Güner Hande Ulutürk,** "Türk Ceza Hukukunda Akıl Hastalığı ve Kusur Yeteneğine Etkisi", Bahçeşehir Üniversitesi SBE, Yayımlanmamış Yüksek Lisans Tezi, İstanbul, 2009, s.13 https://tez.yok.gov.tr/UlusalTezMerkezi/ (E.T: 25.11.2018).

524 **Özbek/Doğan/Bacaksız/Tepe,** Genel Hükümler, s.339

yeteneği ise daha geniş manada fiilin bir insana atfedilebilmesi veya onun fiil nedeniyle sorumlu veya sorumsuz sayılabilmesi için bulunması gereken unsurlardır[525]. Kusur yeteneği, kusurlu hareket edebilmenin ön koşulunu oluşturur[526]. Kusurluluk, aynı zamanda "*failin fiil ile olan ilişkisi"*ni ortaya koyar[527]. Suç oluşturan bir haksızlığın işlenmesinden dolayı failin kusurluluğunun bulunması halinde, uygulanacak yaptırım teknik anlamda ceza niteliğindeyken, failin kusur ehliyetinin bulunmaması veya genel olarak kusursuz olması halinde faile uygulanacak yaptırım güvenlik tedbiri niteliğinde olacaktır[528].

Kişi gerçekleştirdiği eylemin bütün unsurlarını bilmekle beraber, bu eylemin haksızlık ve dolayısıyla suç oluşturduğunu bilmeyebilir, bu durumda kişi kasten hareket etmiş olmasına rağmen işlediği kasten haksızlık nedeniyle kusurlu sayılmaz çünkü kişide haksızlık bilinci bulunmaz[529]. Kişinin işlemiş olduğu eylemden dolayı cezalandırılabilmesi için eylemin haksızlık oluşturduğunu bilmesi gerekir[530]. Ancak, hareketinin toplum nazarında bir haksızlık teşkil ettiğinin bilincinde olan kişinin, bunun herhangi bir pozitif hukuk metniyle cezalandırıldığını bilmesi şart değildir[531]. Haksızlık bilinci de kusurluluğun kabul edilebilmesi için tek başına yeterli değildir. Ayrıca failin davranışlarını yönlendirme yeteneğine de sahip olması gerekir. İrade ürünü olmayan davranışların eylem kabul edilmesi ve kınanabilmesi mümkün değildir[532].

Bu kapsamda örneğin, cebir veya tehdit yoluyla bir bilişim sisteminin işleyişini engelleyen veya bozan kişiye ceza verilemeyecektir. Yine, eşine ait bilişim sisteminde, eşinin sadakat yükümlülüğünü yerine getirmediğine dair veriler bulan kişinin, eşine ait bilişim

---

525 **Selami Turabi,** "Kusurluluk ve Kusurluluğu Etkileyen Haller" TBB Dergisi, S:101, 2012, s.271, http://tbbdergisi.barobirlik.org.tr/m2012-101-1205 (E.T: 19.04.2019); **Özbek/Doğan/Bacaksız/Tepe,** Genel, s. 340.

526 **Dülger,** s.289.

527 **Özbek/Doğan/Bacaksız/Tepe,** Genel Hükümler, s.333.

528 **Koca/Üzülmez,** Genel Hükümler, s.306; **Dülger,** s.289.

529 **Koca/Üzülmez,** Genel Hükümler, s.165.

530 **Dülger,** s.290.

531 **Artuk/Gökcen/Alşahin/Çakır**, Genel Hükümler, s.572.

532 **Koca/Üzülmez,** s.311, 312; **Özgenç,** Genel Hükümler, s.290.

sisteminin işleyişini engellemesi veya bozması durumunda haksız tahrik indirimi uygulanması mümkün olabilecektir.

Bilişim sisteminin işleyişini engelleme veya bozma suçunda, TCK'da yaş küçüklüğüne ilişkin hükümler de uygulama alanı bulabilecektir. Buna göre, fiili işlediği sırada on iki yaşını doldurmamış çocuklar ile on iki yaşını doldurmuş olup da on beş yaşını doldurmamış olanlardan işlediği fiilin hukuki anlam ve sonuçlarını algılayamayacak olanlar için ceza kovuşturması yapılamayacak, işlediği fiilin hukuki anlam ve sonuçlarını algılayanlar ile on beş yaşını doldurmuş olup da on sekiz yaşını doldurmamış olanlar için ise verilecek cezada indirim yapılacaktır.

Bilişim sisteminin işleyişini engelleme veya bozma suçunda haksızlık hatasının da incelenmesi gerekmektedir. TCK'nın 30/4'üncü maddesinde; *"İşlediği fiilin haksızlık oluşturduğu hususunda kaçınılmaz bir hataya düşen kişi, cezalandırılmaz."* denilmektedir. İşlenen fiilin hukuken uygun görülmediğini bilmek, kusurluluğun temelini oluşturmaktadır[533]. Hatanın kaçınılabilir olup olmadığının tespitinde *"kişinin sosyal konumu, bilgi düzeyi, eğitimi, yetiştiği sosyal çevre ve sahip olduğu bilgiyi kullanmasının ondan beklenip beklenmeyeceği"* gibi kriterlerden faydalanılmaktadır[534]. Bu kriterler bakımından örneğin, bir bilgisayar mühendisinin ya da teknik sorumlunun sistemin işleyişine yönelik bir suç işleme durumunda kaçınılmaz hataya düşmesi ileri sürülemeyecektir.

F. SORUŞTURMA USULÜ, GÖREVLİ VE YETKİLİ MAHKEME, YAPTIRIM, ZAMANAŞIMI

TCK'nın 244'üncü maddesinde bilişim sisteminin işleyişini engelleme veya bozma suçunu işleyen failler için "*bir yıldan beş yıla kadar hapis cezası"* öngörülmüştür. Madde metninde yalnızca hürriyeti bağlayıcı ceza öngörülmüş olup, ceza TCK'nın 61'inci

---

533 **Artuk/Gökcen/Alşahin/Çakır**, s.580

534 **Demirbaş**, s.424; **Ragıp Barış Erman,** Yanılmanın Ceza Sorumluluğuna Etkisi, Yayımlanmamış Doktora Tezi, İstanbul Üniversitesi SBE, İstanbul, 2006, s.311 https://tez.yok.gov.tr/UlusalTezMerkezi/ (E.T: 25.11.2018).

maddesinde yer alan düzenleme doğrultusunda hâkimin takdir yetkisi ile bireyselleştirilecektir. Yine şartlarının bulunması halinde ceza tayininde TCK'nın 62'nci maddesi gereğince takdiri indirim yapılması mümkündür[535].

TCK'nın 244'üncü maddesinin üçüncü fıkrasında daha fazla cezayı gerektiren nitelikli hal düzenlenmiş olup, fiillerin bir banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinde işlenmesi halinde, verilecek ceza yarı oranında artırılacaktır.

Faile verilen cezanın iki yıldan az olması halinde Ceza Muhakemesi Kanunu'nun 231'inci maddesi gereğince hükmün açıklanmasının geri bırakmasına karar verilebilir[536]. Hükmün açıklanması geri bırakılmazsa TCK'nın 51'inci maddesinde yer alan diğer şartların da bulunması halinde cezanın ertelenmesine karar verilebilir. Failin bir yıldan az ceza alması halinde yine hükmün açıklanmasının geri bırakılması ve cezanın ertelenmesi kararı verebileceği gibi TCK'nın 50'nci maddesinde yazılı seçenek yaptırımlara ve tedbirlere de çevrilebilir.

Yine TCK'nın 54 ve 55'inci maddelerinde yer alan şartların bulunması halinde eşya ve kazancın müsaderesi mümkündür.

Fail başlığında ifade edildiği gibi tüzel kişiler suçun faili olamazlar dolayısıyla bir cezai yaptırımla da karşılaşmazlar ancak tüzel kişiler hakkında güvenlik tedbiri uygulanabilecektir. Ancak bu uygulama TCK'nın 60'ıncı maddesinin dördüncü fıkrasında ifade edildiği üzere yalnızca kanunda açıkça belirtildiği hallerde söz konusu olacaktır.

---

535 *Madde 62- (1) Fail yararına cezayı hafifletecek takdiri nedenlerin varlığı halinde, ağırlaştırılmış müebbet hapis cezası yerine, müebbet hapis; müebbet hapis cezası yerine, yirmibeş yıl hapis cezası verilir. Diğer cezaların altıda birine kadarı indirilir.*
(2) Takdiri indirim nedeni olarak, failin geçmişi, sosyal ilişkileri, fiilden sonraki ve yargılama sürecindeki davranışları, cezanın failin geleceği üzerindeki olası etkileri gibi hususlar göz önünde bulundurulabilir. Takdiri indirim nedenleri kararda gösterilir.

536 5271 Sayılı Ceza Muhakemesi Kanunu, 04/12/2004 tarihinde kabul edilmiş, 17/12/2004 tarihli 25673 sayılı Resmi Gazetede yayımlanarak 01.06.2005 tarihinde yürürlüğe girmiştir. http://www.mevzuat.gov.tr/MevzuatMetin/1.5.5271.pdf (E.T: 05.03.2019)

TCK'nın 246'ncı maddesinde *"Bu bölümde yer alan suçların işlenmesi suretiyle yararına haksız menfaat sağlanan tüzel kişiler hakkında bunlara özgü güvenlik tedbirlerine hükmolunur."* şeklinde bir düzenlenme yer almaktadır. Tüzel kişi, Türk Medeni Kanununun[537] 47'inci maddesinde **"***Başlıbaşına bir varlığı olmak üzere örgütlenmiş kişi toplulukları ve belli bir amaca özgülenmiş olan bağımsız mal toplulukları*" olarak tanımlanmıştır. TCK'da tüzel kişilerin cezai sorumluluğu kabul edilmemiştir[538]. TCK'nın 20/2'nci maddesinde *"Tüzel kişiler hakkında ceza yaptırımı uygulanamaz. Ancak, suç dolayısıyla kanunda öngörülen güvenlik tedbiri niteliğindeki yaptırımlar saklıdır."* şeklinde bir düzenleme ile güvenlik tedbiri uygulanacağı kabul edilmiştir.

Tüzel kişiler hakkında uygulanabilecek güvenlik tedbirleri ise TCK'nın 60'ıncı maddesine göre faaliyet izninin iptali ve müsaderedir. Ancak, güvenlik tedbiri uygulanmasının işlenen fiile nazaran daha ağır sonuçlar ortaya çıkarabileceği durumlarda, hâkim bu tedbirlere hükmetmeyebilir.

TCK'da dava zamanaşımı süreleri, işlenen suçun kanunda öngörülen yaptırımına ve failin yaşına göre çeşitli ihtimallerle düzenlenmiştir. Buna göre kural olarak fiili işlediği sırada on sekiz yaşını bitirmiş herkes ceza sorumluluğuna sahiptir. Bilişim sisteminin işleyişini engelleme veya bozma suçunun üst sınırı beş yıl hapis cezası olarak belirlendiğinden TCK'nın 66/1'inci maddesi uygulanacak ve suç sekiz yıllık zamanaşımına tabi olacaktır. Ancak 244'üncü maddenin üçüncü fıkrasında fiillerin bir banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinde işlenmesi halinde, verilecek ceza yarı oranında artırılacağı düzenlenmiş olup bu durumda dava zamanaşımı süresinin tespitinde esas alınacak ceza, artırılmış olan cezadır. Dolayısıyla suçun fiillerin bir banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinde işlenmesi halinde öngörülen cezanın üst sınırı yedi yıl altı ay olacak ve bu

---

537 4721 sayılı Türk Medeni Kanunu 22/11/2001 tarihinde kabul edilmiş, 08/12/2001 tarihli 24607 sayılı Resmi Gazete'de yayımlanarak 01.01.2002 tarihinde yürürlüğe girmiştir. https://www.mevzuat.gov.tr/MevzuatMetin/1.5.4721.pdf (E.T:05.03.2019)

538 **Dülge**r, s.248, **Akbulut,** Ceza Hukuku Genel Hükümler, s.338; **Özgenç,** Genel Hükümler, s.207; **Demirbaş,** s.622

durumda zamanaşımı süresi TCK'nın 66'ncı maddesine göre beş yıldan fazla hapis cezası gerektirdiği için on beş yıl olacaktır.

TCK'nın 244/1'inci maddesinde düzenlenen suçlar bakımından şikâyete ilişkin bir düzenleme bulunmamaktadır. Bu sebeple suç şikâyete bağlı olmayıp resen dikkate alınacak ve resen soruşturulacak suçlardandır. Cumhuriyet savcısı ihbar veya başka bir suretle bilişim sisteminin işleyişini engelleme veya bozma suçlarının işlendiği izlenimini veren bir hali öğrendiği anda gerekli araştırma ve delil toplama sürecini tamamlayıp, şüpheli veya şüpheliler tarafından suçun işlendiği konusunda yeterli şüphe oluşuyorsa iddianame düzenler[539]. Ceza yargılamasının esas amacı maddi gerçeğin ortaya çıkarılması olduğundan, yargılama yeterli araştırma neticesinde tamamlanmalı ve deliller bu alanda uzman kişiler tarafından incelenmelidir. Nitekim, Yargıtay kararlarının çoğunda bozma sebebi olarak eksik inceleme ile hüküm kurulması gösterilmiştir[540].

Bununla birlikte TCK'nın 11'inci maddesine göre Türk vatandaşının yabancı ülkede işlediği bir suçta, failin Türkiye'de olması ve suçun aşağı sınırı olarak bir yıldan az hapis cezasının öngörülmesi halinde suç, takibi şikayete bağlı hale gelir ve şikayetin, vatandaşın ülkeye girdiği andan itibaren altı ay içinde yapılması gerekir.

5235 sayılı Adli Yargı İlk Derece Mahkemeleri ile Bölge Adliye Mahkemelerinin Kuruluş, Görev ve Yetkileri Hakkında Kanunun[541] 10, 11 ile 12'nci maddelerine göre, öngörülen cezanın üst sınırı beş yıl olduğundan bu suç için görevli mahkeme Asliye Ceza Mahkemeleridir[542].

---

539 **Apaydın**, s.215

540 Örneğin, Yargıtay 15. Ceza Dairesi, 10.04.2018 tarihli ve 2017/30950 E., 2018/2420 K.; Yargıtay 11. Ceza Dairesi, 25.04.2018 tarihli ve 2016/7914 E., 2018/3844 K.; Yargıtay 8. Ceza Dairesi, 26.04.2018 tarihli ve 2018/182 E., 2018/4812 K. sayılı kararlarında eksik inceleme ile hüküm kurulması bozma sebebi olarak değerlendirilmiştir. https://www.lexpera.com.tr/ (10.05.2019)

541 5235 sayılı Adli Yargı İlk Derece Mahkemeleri ile Bölge Adliye Mahkemelerinin Kuruluş, Görev ve Yetkileri Hakkında Kanun, 26/09/2004 tarihinde kabul edilmiş, 07/10/2004 tarihli 25606 sayılı Resmi Gazetede yayımlanarak 01/06/2005 tarihinde yürürlüğe girmiştir.

542 **Özbek/Doğan/Bacaksız/Tepe**, s.807.

Suç yeri kavramı, bilişim suçlarında en çok sorun teşkil eden kavramlardan biridir. Bilişim suçlarının yapısı itibariyle klasik suçlarda olduğu gibi belirgin bir zaman ve mekan kavramı yoktur. Bilişim sistemlerine ve verilere yapılan müdahalenin fiziksel temas ile yapılması durumunda ortada bir sorun yoktur zira eylem nerede yapılmışsa suç orada işlenmiş kabul edilecektir. Ancak, fiziksel temas olmadan, sistem ağları üzerinden yapılan müdahaleler ile suçun işlenmesi durumunda failin bulunduğu yer ve neticenin gerçekleştiği yer birbirinden farklı noktalar olabilecektir. TCK ve CMK'da yetki ve uygulanacak hukuk bakımından bilişim suçlarına özgü bir düzenleme yer almadığından genel kurallar uygulanacaktır.

Yetkili mahkeme CMK'nın 12'nci maddesi gereğince suçun işlendiği yer mahkemesidir[543]. Ancak bu maddede suçun işlendiği yerin belli olmaması durumunda kademeli bir yetki kuralı belirlemiştir. Buna göre, şüpheli veya sanığın yakalandığı yer, yakalanmamışsa yerleşim yeri mahkemesi, şüpheli veya sanığın Türkiye'de yerleşim yeri yoksa, Türkiye'de en son adresinin bulunduğu yer mahkemesi, bu da mümkün değilse ilk usul işleminin yapıldığı yer mahkemesi yetkili kılınmıştır. Suçun işlendiği yer, TCK'nın 8'inci maddesine göre belirlenmektedir. Buna göre, hareketin kısmen veya tamamen işlendiği veya neticenin gerçekleştiği yer suçun işlendiği yerdir. Yetkili mahkeme de bu doğrultuda hareketin kısmen ya da tamamen işlendiği veya neticenin gerçekleştiği yerdir. Bilişim suçlarında kişinin beden olarak bulunduğu yer ile hareketin ortaya çıktığı yerler çoğunlukla farklı yerlerdedir ve her iki yer de hareket yeridir[544]. Bu durumda failin suç teşkil eden hareketi gerçekleştirdiği yer tespit edilebilmekteyse, yetkili mahkeme hareketin icra edildiği yer mahkemesidir. Ancak hareketin gerçekleştirildiği yer tespit edilemiyorsa, bu durumda neticenin gerçekleştiği yer mahkemesi yetkili kabul edilmelidir. [545]".

---

543 "Madde 12 – (1) Davaya bakmak yetkisi, suçun işlendiği yer mahkemesine aittir.
(2) Teşebbüste son icra hareketinin yapıldığı, kesintisiz suçlarda kesintinin gerçekleştiği ve zincirleme suçlarda son suçun işlendiği yer mahkemesi yetkilidir…"

544 **Akbulut,** Bilişim Alanında Suçlar, s.216. Yaşar/Gökcan/Artuç'a göre bu durumda, bilişim sistemine nereden girildiği yer belli ise, yetkili mercii girilen yerdeki mercii, nereden girildiği belli değil ise sistemin bulunduğu yerdeki merciidir. (**Yaşar/Gökcan/Artuç**, s.6770)

545 **Özbek/Doğan/Bacaksız/Tepe**, s.976.

Suçun uluslararası nitelik taşıması durumunda TCK'nın 8'inci maddesine göre fiilin kısmen veya tamamen Türkiye'de işlenmesi veya neticenin Türkiye'de gerçekleşmesi hakinde Türkiye'de işlenmiş sayılacak ve Türk hukuku uygulanacaktır. Ancak, Türk hukukunun yetkili sayıldığı bir durumda başka bir ülkenin de kendisini yetkili kabul etmesi mümkündür. Bu ve benzeri durumlarda uluslararası iş birliği önem taşımaktadır. Sanal Ortamda İşlenen Suçlar Sözleşmesi'nin bir amacı da Avrupa Konseyine üye ülkeler ve bu belgeyi imza eden diğer ülkeler arasında iş birliği sağlamak olup buna yönelik düzenlemeler yer almaktadır[546]. Ancak bu iş birliğinin uygulamaya geçirilmesi yeterince mümkün olmamıştır.

[546] **Erdoğan,** Bilişim Suçları, s.295.

II. BİLİŞİM SİSTEMİNDEKİ VERİLERİ BOZMA, YOK ETME VEYA ERİŞİLMEZ KILMA, SİSTEME VERİ YERLEŞTİRME, SİSTEMDE VAR OLAN VERİLERİ BAŞKA BİR YERE GÖNDERME SUÇU

A. GENEL OLARAK

Günümüzde bilişim sistemlerinin ve internetin yaşamın tüm alanlarına girmesi, iletişimlerin neredeyse tamamının bu sistemler aracılığıyla sağlanması ve kişilere ilişkin neredeyse bütün verilerin bu sistemlerde saklanması, verilerin korunması konusunun önemini de artırmıştır[547]. Veri, bilişim sistemlerin, üzerinde işlem yapabildiği, bu işlemlere dayalı sonular üretebildiği, saklayabildiği, sakladıklarını sonradan tekrar okuyup işleyebildiği ve diğer bilişim sistemlerine iletebildiği her türlü bilgi olarak tanımlandığından[548] hem bireysel hem de kamu güvenliği ve kamu düzeni açısından korunması en önemli olgulardan biridir. Bu sebeple, TCK'nın 244/2'inci maddesinde, bir bilişim sistemindeki verileri bozan, yok eden, değiştiren veya erişilmez kılan, sisteme veri yerleştiren, var olan verileri başka bir yere gönderen kişinin cezalandırılması öngörülmüştür.

B. KORUNAN HUKUKİ DEĞER

TCK'nın 244/2'inci maddesiyle korunan hukuki değerlere ilişkin olarak sınırlayıcı bir açıklama yapmak mümkün değildir. Burada öncelikle belirtilmesi gereken husus, korunan verilerin sistemin doğrudan işleyişini etkileyen veriler olmadığıdır[549]. Dolayısıyla eğer eylem, sistemin işleyişine etki eden verilere yönelikse bu durumda ilk fıkrada düzenlenen bilişim sisteminin işleyişinin engellenmesi veya bozulması suçu oluşacaktır. Bu fıkrada korunan veriler, sistemin yapıtaşı olmayan, sistemden çıkarıldığı, yok edildiği ya da sisteme

---

547 **Kurt**, s.41; **Alp**, s.2.
548 **Dülger,** s.79.
549 **Erdoğan,** Bilişim Suçları, s.215.

yerleştirildiği takdirde işleyişi bozmayan verilerdir[550]. Dolayısıyla suça konu olan verinin sahip olduğu değere göre korunan hukuki değer de farklılık gösterecektir[551].

Akbulut'a göre bu suçla korunan hukuki değer, veriler üzerinde tasarruf yetkisi olan kişilerin verilerin bozulmadan, engel çıkartılmadan, verilere müdahale olmadan kullanılmasındaki yarardır[552].

Artuk/Gökcen/Yenidünya bu suçun korunan hukuki değerini; *"kişisel verilerin ele geçirilmesi, başka yere gönderilmesi halinde, özel hayatın gizliliği de ihlal edilmiş olmaktadır. Ayrıca programların ve dolayısıyla sistemin işleyişi engellendiğinde haberleşme özgürlüğüne de haksız bir müdahalede bulunulmuştur*." şeklinde açıklamıştır [553].

Kurt'a göre ise, verilerin bozulması, yok edilmesi, değiştirilmesi, erişilmez kılınması, sisteme veri yerleştirilmesi, var olan verilerin başka yere gönderilmesi eylemleri ile mülkiyet hakkı ihlal edilmekte aynı zamanda bu veriler özgün bir çalışmayı içeriyorsa fikri mülkiyet hakkı da ihlal edilmektedir. Eser niteliği taşımayan kişisel verilere yönelik olması halinde ise özel hayatın gizliliği ilkesine zarar verilmiş olmaktadır[554] .

Sanal Ortamda İşlenen Suçlar Sözleşmesi açıklayıcı raporuna göre bu hükmün amacı, bilgisayar verilerini ve bilgisayar programlarını da, fiziksel nesneler gibi, kasıtlı hasar verme girişimlerine karşı koruma altına almaktır. Burada koruma altına alınan değer, saklanan verinin bütünlüğü, uygun biçimde çalışması ve kullanımıdır[555].

---

550 **Erdoğan,** Bilişim Suçları, s.190
551 **Kurt**, s.162
552 **Akbulut,** Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme, s.17.
553 **Artuk/Gökcen/Yenidünya**, Türk Ceza Kanunu Şerhi, s.4665, 4666.
554 **Kurt,** s.162.
555 https://www.ozgureralp.av.tr/avrupa-konseyi-siber-suc-sozlesmesi-aciklayici-memorandum-internet-ve-hukuk-platformu-i-v-h-p-cevirisi/ (E.T: 10/02/2019)

Burada belirtilmesi gereken bir husus da TCK'nın 244'üncü maddesinin ikinci fıkrasındaki suç tipiyle, TCK'nın 135 ve 136'ncı maddeleri arasındaki farkın özellikle korunan hukuksal değerden kaynaklandığıdır[556]. TCK'nın 244/2'nci maddesinde bilişim sisteminde yer alan verilerin varlığı, düzgünlüğü, doğruluğu ve erişilebilirliği korunmaktayken, 135 ve 136'ncı maddelerde kişisel verilerin bizzat kendisi korunur. 244/2'nci maddede sistemde yer alan her türlü veri korunurken, 135 ve 136'ncı maddelerde yalnızca kişisel veriler korunur. Bu bağlamda 135 ve 136'ncı maddelerde her türlü yer ve araçta kayıtlı kişisel veriler korunurken, 244/2'nci maddede yalnızca bilişim sisteminde yer alan veriler korunur[557].

C. SUÇUN UNSURLARI

1. Tipikliğin Maddi Unsurları

a. Fiil

Artuk/Gökcen/Yenidünya'ya göre, bilişim sistemindeki verilere zarar verme suçu seçimlik hareketli bir suçtur. Seçimlik hareketlerden birinin yapılması halinde suç oluşur ve birden fazla seçimlik hareketin yapılması halinde, yine tek suç oluşup ceza tayininde TCK'nın 61'inci maddesine göre alt sınırdan uzaklaşılır[558].

Yaşar/Gökcan/Artuç ve Özbek/Doğan/Bacaksız/Tepe de aynı şekilde suçun seçimlik hareketli bir suç olduğu görüşündedir[559].

Kanaatimizce, 244'üncü maddenin birinci fıkrasında olduğu gibi ikinci fıkrasında da belirtilen hususlar hareketin kendisi değil neticeleridir. Dolayısıyla bu suç serbest

---

556 **Dülger,** s.315.

557 **Erdoğan,** Bilişim Suçları, s.208.

558 **Artuk/Gökcen/Yenidünya,** Türk Ceza Kanunu Şerhi, s.4666.

559 Yaşar/Gökcan/Artuç; maddenin ikinci fıkrasında düzenlenen suç da seçimlik hareketli bir suçtur, seçimlik hareketleri oluşturan, bozma, yok etme, değiştirme, erişilmez kılma, sisteme veri yerleştirme, var olan veriyi başka yere gönderme eylemlerinden birinin yapılması ile suç tamamlanır, hepsinin bir arada yapılmasına gerek yoktur, bu hareketlerden birden fazlasının yapılması, suç tekliğini etkilemez şeklinde ifade etmiştir. (**Yaşar/Gökcan/Artuç,** s. 6761); **Özbek/Doğan/Bacaksız/Tepe**, s.964.

hareketli bir suç olup herhangi bir şekilde işlenebilir ve burada önemli olan husus yapılan hareket sonucunda yukarıda sayılan neticelerden birinin gerçekleşmesidir. Fail, Truva atı yöntemiyle, virüslerle ve benzeri pek çok şekilde sistemdeki verileri yok edebilir veya mail yoluyla ya da bir CD aracılığıyla sisteme veri yerleştirebilir. Dolayısıyla kanunda öngörülen neticeler pek çok şekilde gerçekleştirilebilmektedir. Burada önemli olan, eylemin bilişim sisteminin donanımına karşı değil, verilere karşı yapılmasıdır[560]. Suç, aynı zamanda icrai hareketle işlenebilen bir suçtur.

(1) Bilişim Sistemindeki Verileri Bozma

Bozma eylemi sözlükte[561], "*Bir şeyi kendisinden beklenilen işi yapamayacak duruma getirmek; Biçimini ve kullanılışını değiştirmek…"* şeklinde tanımlanmış olup TCK'nın 244/2'inci maddesi kapsamında, bilişim sisteminde yer alan bir verinin, yok edilmeden, işe yaramayacak ve kendisinden beklenilen faydayı sağlayamayacak duruma getirilmesini, verinin içeriğine veya yapısına müdahale etmek suretiyle verinin kısmen veya tamamen kullanılmaz hale getirilmesini ifade eder[562].

Bozma, verilerin niteliğinin değiştirilmesi şeklinde gerçekleştirilebileceği gibi, verinin tamamen veya kısmen tahrip edilmesi biçiminde de işlenebilir[563]. Bilişim sistemine yapılan fiziki müdahale sonucunda sistem içindeki verilerin zarar görmesi halinde verilerin bozulmasından bahsedilebilir[564].

Bilişim sisteminin işleyişinin bozulması, verilerin bozulması yoluyla gerçekleşebilir[565]. Bu durumda tek fiille kanunun birden fazla hükmü ihlal edileceğinden

---

560 **Erdoğan**, Bilişim Suçları, s.219
561 http://tdk.gov.tr/ (E.T:02/07/2019)
562 **Yaşar/Gökcan/Artuç**, s.6759-6760; **Dülger,** s.322; **Akbulut,** Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme, s.32; **Koca/Üzülmez,** Özel Hükümler, s.871; **Ketizmen,** s.139.
563 **Koca/Üzülmez,** Özel Hükümler, **s.** 871; **Artuk/Gökcen/Yenidünya, Özel Hükümler**, s.770.
564 **Artuk/Gökcen/Yenidünya,** Türk Ceza Kanunu Şerhi, s.4666; **Kurt**, s.167. **Koca/Üzülmez**, Özel Hükümler, s.871.
565 **Güngör**, s.97.

(244/1 ve 244/2) fikri içtima hükümleri uygulanmalı ve daha ağır olan birinci fıkradan ceza tayin edilmelidir[566].

Verinin bozulmasıyla yok edilmesi arasındaki fark ise şu şekildedir; veriye yönelik müdahale sonucunda verinin bozulması durumunda, bozuk da olsa bir veri bulunmaktadır, ancak işlevini tamamen ya da kısmen yitirmiştir ve onarılma imkânı bulunmaktadır. Yok edilme halinde ise, veri sahibinin veriye ulaşması mümkün olmamaktadır[567].

(2) Bilişim Sistemindeki Verileri Yok Etme

Sözlükte yok etmek; "*varlığına son vermek, ortadan kaldırmak*" şeklinde tanımlanmıştır[568]. Bilişim sisteminde yer alan verileri siber uzay kapsamında tamamen ortadan kaldırmak ya da varlığına son vermek mümkün değildir. Burada mantıksal bir yok oluş söz konusudur[569].

Doktrinde, verilerin silinerek geri dönüşüm kutusuna gönderilmesi durumunda verinin yok edilmiş sayılıp sayılmayacağı konusunda görüş farklılıkları bulunmaktadır. Bu görüşlerden biri[570] bir dosyanın sil komutu verilerek geri dönüşüm kutusuna atılması halinde, verinin sistemde tutulmakla birlikte o verilere ulaşımı sağlayan anahtar verilerin değiştirildiği, veriye normal yollarla ulaşımının engellendiği, belirli bir uğraştan sonra verilere tekrar erişilmesinin mümkün olacağı, bu sebeple verilerin yok olmasından söz edilemeyeceğini ifade etmektedir. Doktrindeki diğer görüş ise[571]; bilişim sistemlerinde gerçek anlamda bir silme işlemi değil mantıki bir silmenin söz konusu olduğu, bu şekilde verilere ulaşılmasının engellendiği, bu durumda mağdurun verilerine ulaşamamasının artık

---

566 **Erdoğan,** Bilişim Suçları, s.220; **Dülger,** s.323.
567 **Kurt,** s.168; **Ketizmen**, s.139; **Yaşar/Gökcan/Artuç**, s.6760, **Erdoğan**, Bilişim Suçları, s.220.
568 http://www.tdk.gov.tr/ (E.T: 10/02/2019)
569 **Dülger,** s.323; **Erdoğan**, Bilişim Suçları, s.222; **Akbulut,** Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme, s.32; **Koca/Üzülmez,** Özel Hükümler, s.872.
570 **Kurt,** s.168**; Koca/Üzülmez**, Özel Hükümler, s.872; **Akbulut,** Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme, s.33.
571 **Özbek/Doğan/Bacaksız/Tepe** s. 965; **Erdoğan**, Bilişim Suçları, s.222; **Güngör,** s.99.

onun açısından verilerin yok edilmiş olması anlamına geleceğini belirterek veriye tekrar ulaşabilme imkanının suçun oluşmasını engellemediğini ifade etmektedir.

Kanaatimizce, bilişim sistemleri içerisinde oluşturulan bir verinin silme yoluyla fiziken yok olması mümkün olmamakla birlikte, ortadan kaldırılma durumunda eğer verinin birtakım araçlar yardımıyla geri getirilme imkanı yoksa yok edilmiş sayılacak fakat, geri getirilme imkanı varsa, telafisi mümkün olduğundan yok edilmiş sayılmayacak ancak şartlar oluşmuşsa erişilmez kılınmış sayılabilecektir.

Yok etmek sisteme fiziksel müdahale yoluyla yapılabileceği gibi sisteme bir bilişim ağı vasıtasıyla bağlanmak suretiyle de gerçekleştirilebilecektir[572].

(3) Bilişim Sistemindeki Verileri Değiştirme

Sözlükte "değiştirmek" kavramı, "*Başka bir biçime sokmak, değişikliğe uğratmak, başka bir duruma, başka bir görünüme getirmek*." şeklinde tanımlanmaktadır[573].

Akbulut'a göre verilerin değiştirilmesi, kaydedilmiş verilerin başka bir bilgi içeriği almasını ifade etmektedir[574].

Artuk/Gökcen/Yenidünya, değiştirmek hareketini "*verilerin başka biçimlere sokulması, yeni içerik kazandırılması, niteliklerinin değiştirilmesi şeklinde veriler üzerinde yapılan manipülasyon*" olarak tanımlamıştır[575].

Dülger ise verilerin değiştirilmesi hareketini; "*bir veri ya da veri grubu yerine başka verilerin konulması"* şeklinde ifade etmektedir[576].

---

572 **Artuk/Gökcen/Yenidünya,** Türk Ceza Kanunu Şerhi, s.4666; **Erdoğan**, Bilişim Suçları, s.223.
573 http://www.tdk.gov.tr/ (E.T: 11/02/2019)
574 **Akbulut,** Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme, s.34.
575 **Artuk/Gökcen/Yenidünya,** Türk Ceza Kanunu Şerhi, s.4667.
576 **Dülger,** s.324.

Kurt'a göre ise "*verilerin değiştirilmesi durumunda verilerin orijinal halinden başka bir hale dönüştürülmesidir*"[577].

Koca/Üzülmez ise verilerin değiştirilmesini, "*verinin içeriğinin değiştirilmesi, bir veri yerine başka bir verinin konması, bir verinin başka bir görünüm veya konuma getirilmesi"* şeklinde tanımlamıştır[578].

Mevcut verinin kullanılmasını engellemeyen fakat verinin içeriğini veya orijinalliğini ortadan kaldıran her türlü değişiklik bu anlama gelmektedir[579]. Değiştirmenin orijinal verilerde yapılması gerekir, kopyalanmış verilerde yapılan değişikliklerde bu hüküm uygulanmaz[580]. Verilerin değiştirilmesi, kısmen ya da verilerin tamamına yönelik olabilir[581]. Örneğin; bir bilişim sisteminde yer alan dosyaların ya da kayıtların yerine başka verilerin koyulması halinde verilerin değiştirilmesi söz konusu olacaktır. Sonuç olarak veri sahibi bu durumda, bilişim sistemine erişebilmekte ancak istediği veriye ulaşamamakta, onun yerine başka bir veriye erişmektedir[582].

(4) Bilişim Sistemindeki Verileri Erişilmez Kılma

Sözlükte erişmek kavramı; "*Varılması zamana, emeğe bağlı olan veya uzakta bulunan bir amaca varmak, ulaşmak, Bir yere ulaşmak, varmak"* şeklinde tanımlanmıştır[583].

Doktrinde bilişim sistemindeki verilerin erişilmez kılınması, *"verinin içerdiği bilgi ya da enformasyona müdahale edilmeden, veriye olağan şekilde erişimin engellenmesi[584]; verilerin malikinin ya da ilgilisinin istediği zaman istediği verilere ulaşmasının engellenmesi[585]; verinin içerdiği bilgiye ve veriye dokunmadan, veriye ulaşım için gereken*

---

577 **Kurt, s**.168.
578 **Koca/Üzülmez,** Özel Hükümler, s.872.
579 **Ketizmen**, s.140; **Koca/Üzülmez**, Özel Hükümler, s.872.
580 **Akbulut,** Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme, s.35; **Akbulut,** Bilişim Alanında Suçlar, s.198.
581 **Kurt,** s.169, **Erdoğan**, Bilişim Suçları, s.224; **Dülger,** s.324.
582 **Güngör,** s.99.
583 http://www.tdk.gov.tr/index (E.T: 11/02/2019)
584 **Özbek/Doğan/Bacaksız/Tepe,** s.966.
585 **Dülger,** s.324; **Koca/Üzülmez,** Özel Hükümler, s.872.

işlem bağının koparılarak bilişim sistemi üzerinde hak sahibi olan kimsenin olağan şekilde veriye istediği zaman ulaşmasının engellenmesi[586]*"* şeklinde tanımlanmıştır.

Erişilmez kılma halinde, veri sistemde bulunmaktayken hak sahibi tarafından veri üzerinde istenilen faaliyetler gerçekleştirilememektedir[587]. Yok olma halinde ise veri sistem üzerinde bulunamamaktadır.

Bilişim sistemindeki verilerin erişilmez kılınması suçunun oluşması için erişimin engellenmesinin geçici ya da daimî olması arasında bir fark bulunmamaktadır[588]. Bu eylem veriye erişimi sağlayan yolların silinmesi veya değiştirilmesi biçiminde olabilir, bu durumda veriler mağdurun sisteminde olduğu halde, failin eylemleri sebebiyle mağdurun kendi verilerine ulaşması imkânsız hale gelmektedir[589]. Burada veriye erişme yetkisi olan kişinin veri üzerindeki somut kullanım iradesinin tespiti zorunlu değildir. Eylemin, yetkili kişinin potansiyel erişim imkanını kaldırması yeterlidir[590].

(5) Bilişim Sistemine Veri Yerleştirme

Sözlükte yerleştirmek; *"Yerleşmesini sağlamak, Yerine koymak"* şeklinde tanımlanmıştır[591].

Doktrinde ise bilişim sistemine veri yerleştirmek, "*bilişim sistemindeki mevcut verilere dokunmadan, onlara herhangi bir zarar vermeden, değiştirmeden, bozmadan, yok etmeden, onlara erişimi engellemeden, bilişim sistemine ek olmak üzere önceden bulunmayan bazı verileri ilave etmek*[592]*; sistemde yer alan verilere herhangi bir zarar vermeden, onlara ulaşma imkanını ortadan kaldırmadan sisteme veri eklemek*[593]*; fail*

---

586 **Yaşar/Artuç/Gökcan**, s.6760.
587 **Hafızoğulları/Özen,** Özel Hükümler, s.451.
588 **Dülger**, s.324, **Ketizmen**, s.140.
589 **Artuk/Gökcen/Yenidünya**, Türk Ceza Kanunu Şerhi, s.4667; **Güngör**, s.100.
590 **Akbulut,** Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme, s.35.
591 http://www.tdk.gov.tr/ (E.T: 11/02/2019)
592 **Yaşar/Artuç/Gökcan,** s.6761.
593 **Artuk/Gökcen/Yenidünya,** Türk Ceza Kanunu Şerhi, s.4667.

tarafından bilişim sistemine ya da veri taşıma aracına dışarıdan ve sistemin maliki ya da ilgilisinden izin alınmaksızın çeşitli verilerin sisteme kaydedilmesi, yüklenilmesi ya da eklenmesi[594]*"* şeklinde tanımlanmıştır.

Bilişim sistemine veri yerleştirme, doğrudan veri girişi yoluyla ya da CD, flash bellek gibi veri taşıma araçlarıyla verinin sisteme aktarılması ya da internet ortamından sisteme verinin yüklenmesi, kaydedilmesi yoluyla gerçekleştirilebilir[595].

Ayrıca suçun oluşması için failin sisteme hukuka uygun ya da hukuka aykırı olarak girmesi önem taşımamaktadır[596]. Önemli olan failin sisteme veri ekleme hakkının olup olmadığıdır. Somut olayda kişi sisteme hukuka uygun olarak girmiş ancak veri yükleme hakkı bulunmuyorken sisteme veri yerleştirmişse suç oluşacaktır[597].

Sisteme yerleştirilen veriler, daha sonra oluşturulan bir belgenin içeriğini etkilemişse, fail ayrıca belgede sahtecilikten sorumlu tutulur[598].

(6) Bilişim Sisteminde Var Olan Verileri Başka Bir Yere Gönderme

Göndermek eylemi sözlükte *"Bir yere doğru yola çıkarmak, yollamak, ulaşmasını, gitmesini sağlamak, Yetki vererek gitmesini sağlamak, Bir kaynaktan çıkıp gelmek, ulaşmak"* şeklinde tanımlanmıştır[599].

Bilişim sisteminde var olan verileri başka bir yere gönderme eylemi ise doktrinde; "*failin, bilişim sisteminde bulunan bir veriyi, bilişim sistemi içinde bir yere veya başka bir bilişim sistemine göndermesi*[600] *mağdura ait verilerin gerek mağdurun bilişim sisteminde farklı bir dosyaya gerekse de farklı bir bilişim sistemine gönderilmesi*[601]*; bilişim sistemi*

---

594 **Dülger,** s.328.
595 **Cengiz Apaydın**, Bilişim Suçları ve Bilişim Ceza Hukuku, Acar Matbaacılık, İstanbul, 2017 s.304; **Akbulut,** Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme, s.31; **Koca/Üzülmez,** Özel Hükümler, s.872.
596 **Erdoğan,** Bilişim Suçları, s.226; **Güngör**, s.100.
597 **Dülger**, s.328; **Hafızoğulları/Özen,** Özel Hükümler, s.451.
598 **Artuk/Gökcen/Yenidünya,** Türk Ceza Kanunu Şerhi, s.4667.
599 http://www.tdk.gov.tr (E.T: 11/02/2019)
600 **Yaşar/Gökcan/Artuç**, s.6761.
601 **Artuk/Gökcen/Yenidünya,** Türk Ceza Kanunu Şerhi, s.4668.

içerisindeki verilerin başka bir bilişim sistemine ya da veri taşıma cihazına aktarılması, kaydedilmesi ya da kopyalanması[602]*"* şeklinde tanımlanmıştır.

Başka yere göndermek ile kastedilen, verilerin kayıt edilmesi, kopyalanması ya da aktarılmasıdır[603]. Ayrıca suçun oluşması için, verilerin gönderildiği bilişim sisteminin mağdura ait olup olmaması da önem taşımamaktadır[604]. Yani mağdura ait verilerin mağdurun rızası dışında sistemden çıkması halinde gönderilen sistemin mağdura ait olması durumunda hatta sistem içerisinde başka bir yere gönderilmesi durumunda yine suç oluşacaktır[605].

Bilişim sisteminde var olan verinin başka yere gönderilmesi halinde, veri aslı sistemden kaldırılmamaktadır. Eğer gerçekleştirilen eylem verinin ortadan kalkması sonucunu doğurursa bu durumda verinin yok edilmesi suçu söz konusu olacaktır[606].

Yine hak sahibinin rızası dışında bir verinin kopyalanarak alınması[607] ya da veri fotoğraf, resim gibi bir belge ise çıktısının alınması gibi durumlarda[608] da suç oluşacaktır.

Bu seçimlik hareket, doktrinde, bilişim sisteminde gerçekleşecek her türlü işlem için mutlak surette bir veri iletiminin gerçekleştirilmesi, her türlü veri iletiminin de verinin başka bir yere gönderilmesi sonucunu oluşturması, madde metninin bu açıdan muğlak olup sınırlarının net bir şekilde çizilmediği gerekçesi ile eleştirilmiştir[609].

b. Netice

Fiil başlığı altında da ifade edildiği gibi kanunda öngörülen, bilişim sistemleri içerisinde yer alan verileri bozma, yok etme, değiştirme, erişilmez kılma, sisteme veri yerleştirme ve sistemde var olan verileri başka bir yere gönderme eylemleri suçun hareket

---

602 **Dülger,** s.328.
603 **Dülger,** s.328, **Yaycı,** s.92; **Ketizmen,** s.140; **Koca/Üzülmez,** Özel Hükümler, s.873; **Özbek/Doğan/Bacaksız/Tepe,** s.967.
604 **Güngör,** s.101.
605 **Artuk/Gökcen/Yenidünya,** Türk Ceza Kanunu Şerhi, s.4668.
606 **Erdoğan,** Bilişim Suçları, s.227.
607 **Yaşar/Gökcan/Artuç,** s.6761.
608 **Erdoğan**, Bilişim Suçları, s.205.
609 **Özbek/Doğan/Bacaksız/Tepe**, s.967.

unsurunu değil netice unsurunu oluştururlar. Zira bozma, yok etme ve maddede öngörülen diğer neticeler başka eylemlerin gerçekleştirilmesine bağlıdır. Bu suç kapsamında bir hareket birden fazla neticenin gerçekleşmesine sebep olabilecektir ancak, bu durumda da tek suç oluştuğundan, tek ceza tayin edilmelidir[610].

Kanaatimizce maddede öngörülen eylemler için suçun tehlike ve zarar suçu bakımından bir ayrıma gidilmesi gerekmektedir. Maddeden öngörülen, verileri bozma, yok etme, değiştirme ve erişilmez kılma eylemleri netice bakımından bir zarar suçudur. Zira, bu neticelerin gerçekleşmesi halinde fiille suçun konusuna mutlak suretle zarar verilmiş olunmaktadır[611]. Ancak sisteme veri yerleştirme ve var olan verilerin başka yere gönderilmesi eylemleri suçun konusuna bir zarar vermemiş olsa bile suç oluşacaktır. Yani bu eylemlerin suç oluşturması için zarar doğması aranmaz[612].

c. Fail

Kanun maddesinde fail açısından herhangi bir özellik belirtilmediğinden, herkes bu suçun faili olabilir[613]. Ancak; suçun işlenip işlenmediğinin tespitinde ayrıca bilişim sisteminin kullanım hakkıyla ilgili değerlendirme yapılmalıdır. Veri taşıyıcısının mülkiyeti ile kullanım hakkının birbirinden ayrıldığı durumlarda, tasarruf yetkisi ilgililerin arasındaki hukuki ilişkiye göre belirlenmelidir[614]. Veri taşıyıcısının sahibi, verilerde tasarruf yetkisine sahip olan kişinin verilerine zarar verirse bu durumda suçun faili olacaktır.

---

610 **Erdoğan,** Bilişim Suçları, **s**.220.
611 **Erdoğan,** Bilişim Suçları, **s**.220.
612 Benzer görüş için bkz. **Yaşar/Gökcan/Artuç,** s.6761.
613 **Dülger,** s.316; **Erdoğan,** Bilişim Suçları, s.228. Fail ile ilgili detaylı açıklamalarımız için bkz. s.83 vd.
614 **Akbulut,** Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme, s.20.

d. Mağdur

Suç tipi, mağdur bakımından da bir özellik göstermemektedir[615]. Ancak bilişim sistemi ile sistem içerisindeki veriler üzerindeki hak sahibinin farklı kişiler olması halinde her ikisinin de suçun mağduru olabileceğidir[616].

e. Konu

Bilişim sistemindeki verileri bozmak, yok etmek, değiştirmek veya erişilmez kılmak, sisteme veri yerleştirmek, sistemde var olan verileri başka bir yere göndermek suçunun konusu, bilişim sistemi içinde bulunan verilerdir[617]. Bu suçun birinci fıkrada yer alan sistemin işleyişini engelleme veya bozma suçundan farkı hukuki konusudur zira birinci fıkrada konu bilişim sistemleriyken, ikinci fıkrada sistemlerin içerisinde yer alan verilerdir[618].

Bilişim sistemi, sistemde yer alan donanım ve yazılım unsurları ile bir bütündür. Donanım kavramı içerisinde çevre giriş ve çıkış birimleri de yer almaktadır[619]. Dolayısıyla veri girişini sağlayan disk, disket, USB (Universal Serial Bus) bellek aygıtı gibi anakart üzerindeki veri yollarına takılmak suretiyle kullanılan birimlerde yer alan verilerin de bu suçun konusu kapsamında değerlendirilmesi gerekmektedir[620].

f. Suçun Nitelikli Unsurları

TCK'nın 244'üncü maddesinin üçüncü fıkrasında, bu suçun bir banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinde işlenmesi

---

615 **Akbulut,** Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme, s.21; **Erdoğan,** Bilişim Suçları, s.229**; Özbek/Doğan/Bacaksız/Tepe,** s.962; **Koca/Üzülmez,** s.867; **Tezcan/Erdem/Önok**, s.1047. Mağdur ile ilgili Fail ile ilgili detaylı açıklamalarımız için bkz. s.85.

616 **Artuk/Gökcen/Yenidünya**, Türk Ceza Kanunu Şerhi, s.4668; **Dülger,** s.316; **Özbek/Doğan/Bacaksız/Tepe,** s.962 **Koca/Üzülmez,** s.868; **Tezcan/Erdem/Önok**, s.1047.

617 **Artuk/Gökcen/Yenidünya**, Türk Ceza Kanunu Şerhi, s.4668, **Yaşar/Gökcan/Artuç**, s. 6759, Özbek/Doğan/ Bacaksız/Tepe, s.960; **Dülger**, s.317; **Akbulut,** Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme, s.24.

618 **Erdoğan**, Bilişim Suçları, s.229; **Dülger**, s.317; **Özbek/Doğan/Bacaksız/Tepe**, s.961; **Koca/Üzülmez,** s.867.

619 Çevre giriş ve çıkış birimlerine ilişkin açıklamalar için bkz. s.9.

620 Benzer görüş için bkz. **Akbulut,** Bilişim Alanında Suçlar, s.189; Suçun konusunu oluşturan verilerin mutlaka sistemde yer alan veriler olması gerektiği görüşü için bkz. **Koca/Üzülmez, s**.826.

halinde cezanın yarı oranında artırılacağı belirtilerek cezada artırım yapılması öngörülmüştür. Bu artırım sebebi birinci fıkra içinde geçerli olup, yapılan açıklamalar burada da geçerlidir. Ayrıca, 3713 Sayılı Kanunun 5'inci maddesinde, 4'üncü maddede sayılan suçların terör amacıyla işlenmesi halinde tayin edilecek hapis cezaları veya adlî para cezalarının yarı oranında artırılacağı, bu suretle tayin olunacak cezalarda gerek o fiil için gerek her nevi ceza için muayyen olan cezanın yukarı sınırının aşılabileceği düzenlendiğinden suçun terör amaçlı işlenmesi halinde artırım yapılacaktır.

2. Tipikliğin Manevi Unsurları

Bilişim sistemindeki verilerin bozulması, yok edilmesi, değiştirilmesi, erişilmez kılınması veya sisteme veri yerleştirilmesi ya da var olan verilerin başka bir yere gönderilmesi suçu, kasten işlenebilen bir suçtur[621]. Burada kanun koyucu özel bir kast, saik öngörmediğinden suç, genel kastla işlenebilecektir. Yani failin, fiili gerçekleştirirken neticeyi bilmesi ve istemesi, cezalandırılması için yeterli olacaktır. Suç doğrudan kastla işlenebildiği gibi olası kastla da işlenebilecektir[622].

Madde metninde suçun taksirli hali düzenlenmemiştir. Suçların taksirli haline ilişkin kanunda bir belirleme yapılmadığında cezalandırılmaları mümkün değildir ancak, sisteme hukuka aykırı giriş yapılması nedeniyle sistemdeki verilerin yok olması veya değişmesi hali, yani fiilin taksirli şekli TCK'nın 243'üncü maddesinin üçüncü fıkrasında netice sebebiyle ağırlaşmış hal olarak yaptırım altına alınmıştır[623]. Örneğin CMK'nın 134'üncü maddesi gereğince şüphelinin bilgisayarından örnek alan kolluğun bu sırada taksirle sistemde yer alan verileri silmesi haline, suçun taksirle işlenmesi hali düzenlenmediği için ve sisteme hukuka aykırı olarak girmediği için taksirli eylemi cezalandırılmayacaktır.

---

621 **Kurt,** s.175; **Artuk/Gökcen/Yenidünya,** Türk Ceza Kanunu Şerhi, s.4669; **Taşkın**, Bilişim Suçları, s.52; **Tezcan/Erdem/Önok**, s.1050.

622 **Artuk/Gökcen/Yenidünya,** Türk Ceza Kanunu Şerhi, s.4669.

623 **Akbulut,** Bilişim Alanında Suçlar, s.204.

3. Hukuka Aykırılık Unsuru

Bilişim sistemindeki verileri bozma, yok etme, erişilmez kılma, değiştirme, sisteme veri yerleştirme ya da var olan verileri başka yere gönderme suçunda hukuka uygunluk nedenlerinden ilgilinin rızası ve görevin ifası söz konusu olabilir[624]. Suçun oluşup oluşmaması konusunda rızanın kapsamı önem taşımaktadır. Bilişim sisteminin kullanım hakkı devredildiğinde, bilişim sisteminin içinde bulunan verilere, kullanım hakkını devralan kişi tarafından zarar verme kastıyla müdahalede bulunması halinde suç gerçekleşmiş olur[625]. Burada artık kullanım hakkının devredildiği kişiye baştan verilen rızanın sınırları aşılmış ve bu kişinin yaptığı eylem hukuka aykırı bir hal almıştır. Ya da sisteme girme ve verilere erişme yetkisi belli bir amaçla verilmişse bu amacın dışında verilerek yönelik gerçekleştirilen eylemler de rızanın kapsamı dışında kalacağından suç oluşacaktır. Örneğin, bir üniversite öğretim üyesinin, asistanına öğrencilerin sınav notlarını girmesi için sisteme girme izni vermesi durumunda, asistanın sistemde yer alan diğer verileri değiştirmesi veya yok etmesi durumunda bu eylemin rıza kapsamının dışında olması sebebiyle suç oluşacaktır.

Görevin ifası kapsamında hareket edilen hallerde de suç oluşmaz. Örneğin, CMK'nın bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve el koymaya ilişkin 134'üncü maddesi kapsamında bir bilişim sisteminde yer alan verileri kopyalayan kolluğun eylemi suç sayılmayacaktır.

D. SUÇUN ÖZEL GÖRÜNÜŞ ŞEKİLLERİ

1. Teşebbüs

Bilişim sisteminde yer alan verilerin yok edilmesi veya değiştirilmesi suçunda teşebbüs mümkündür. Bu durum, icra hareketlerine başlandıktan sonra bu hareketlerin yarıda kalması şeklinde ya da suçun icrasına ilişkin eylemler tamamlandıktan sonra suçun oluşumu

---

624 Hukuka uygunluk sebeplerine ilişkin açıklamalar için bkz. s.90.
625 **Erdoğan**, Bilişim Suçları, s.231; **Dülger,** s.335.

için aranan zarar meydana gelmeden failin elinde olmayan nedenlerle suçun gerçekleşmemesi şeklinde de olabilecektir[626].

Fail, bilişim sistemindeki verileri bozmak, yok etmek, değiştirmek, erişilmez kılmak, sisteme veri yerleştirmek veya var olan verileri başka yere göndermek için harekete geçip bu sonuçları kendisi dışında bir nedenle elde edemez ise, eylem teşebbüs aşamasında kalmış sayılır[627]. Örneğin failin amaca elverişli bir virüsü sisteme sokup faal hale getirmesine karşın, anti virüs programı sayesinde veriler tahrip olmamışsa hareketin teşebbüs aşamasında kaldığının kabulü gerekir. Ancak bu durumun tespiti oldukça zordur.

Madde metninde öngörülen neticelerden birinin gerçekleşmesi halinde, neticelerden diğerleri teşebbüs aşamasında kalsa dahi faile tam ceza verilmesi gerekir[628].

4. İştirak

Bilişim sistemindeki verileri bozma, yok etme, değiştirme, erişilmez kılma, sisteme veri yerleştirme veya var olan verileri başka yere gönderme suçu iştirak bakımından bir özellik göstermemektedir[629]. Bu sebeple iştirake ilişkin genel hükümler uygulanacaktır.

5. Suçların İçtimaı

Fail, aynı suç işleme kararını yerine getirmek için, fıkrada sayılan eylemlerden birini veya birkaçını değişik zamanlarda, aynı mağdura ait veriler üzerinde gerçekleştirirse, zincirleme suç hükümleri uygulanır[630]. Yargıtay, sanığın, mağdura ait birden fazla bilişim sistemine erişimini bir suç işleme kastıyla engellemesi eyleminde zincirleme suç hükümlerinin uygulanması gerektiği yönünde karar vermiştir[631]. Yine benzer şekilde sanığın,

---

626 **Erdoğan,** Bilişim Suçları, s.232; **Dülger**, s.336; **Yaşar/Gökcan/Artuç,** s.7319,7320.

627 **Artuk/Gökcen/Yenidünya**, Türk Ceza Kanunu Şerhi, s.4663, **Yaşar/Gökcan/Artuç**, s.6768, **Dülge**r, s.336, **Erdoğan,** Bilişim Suçları, s.232.

628 **Erdoğan,** Bilişim Suçları, s.211.

629 **Artuk/Gökcen/Yenidünya**, Türk Ceza Kanunu Şerhi, s.4669; **Dülger**, s.336; **Kurt**, s.170; **Koca/Üzülmez**, Özel Hükümler, s.874.

630 **Yaşar/Gökcan/Artuç, s.**6769; **Dülger**, s.336,337.

631 "Sanık ...'ın, ayrılmış olduğu kız arkadaşının kuzeni olan mağdur ...'ya ait elektronik posta adresinin ve bu adresle bağlantı kurulan facebook hesabının önceden bildiği internet şifrelerini, mağdurun bilgisi ve rızası dışında

birçok kişiye çalışmadığı halde çalışıyormuş gibi sistem üzerinden sigorta işe giriş bildirgesi düzenlemesi eyleminin zincirleme şekilde sisteme veri yerleştirme suçunu oluşturacağı yönünde karar vermiştir[632].

TCK'nın 243'üncü ve 244'üncü maddeleri arasındaki içtima ilişkisi bilişim sistemlerinin engellenmesi veya bozulması suçuna ilişkin değerlendirmede açıklanmış olup kanaatimizce fikri içtima kurallarının uygulanması ve daha ağır cezayı gerektiren 244'üncü maddenin uygulanması gerekmektedir[633].

Bilişim sistemlerinin işleyişinin bozulması eyleminin verilere yönelik müdahaleler sonucunda meydana gelmesi halinde hangi hükmün uygulanacağı konusunda doktrinde görüş ayrılığı bulunmaktadır. Bu görüşlerden birine[634] göre, uygulanacak hüküm failin kastına göre belirlenecek olup fail sistemin işleyişini engellemek veya bozmak amacıyla verilere müdahale etmişse birinci fıkra, fail doğrudan verileri bozmak amacıyla hareket

---

değiştirerek, hakkı bulunmadığı halde giriş yaptığı mağdurun facebook hesabı üzerinden eski kız arkadaşının üvey annesi ile iletişim kurup, hukuka aykırı olarak sistemde kalmaya devam ederek, mağdurun hesaplarına erişimini engellemesi eylemlerinin TCK'nın 244/2. maddesinde tanımlanan sistemi engelleme, bozma, verileri yok etme veya değiştirme suçunu oluşturduğu ve elektronik posta hesabı ile Facebook hesabının iki farklı bilişim sistemi olmasından dolayı bir suç işleme kararının icrası kapsamında değişik zamanlarda mağdura karşı aynı eylemi birden fazla işleyen sanık hakkında TCK'nın 43/1. maddesinde düzenlenen zincirleme suç hükmünün uygulanması gerektiği gözetilmeden…" **Yargıtay 12. Ceza Dairesi, 01.03.2017 tarihli ve 2015/10388 E., 2017/1556 K. sayılı kararı** https://www.lexpera.com.tr/ (E.T: 18.12.2018)

632 "Sanığın ortağı ve yetkili müdürü olduğu şirketin faaliyeti 01.03.2008 tarihinde sonlandırılmasına rağmen haklarındaki hükümler kesinleşen diğer sanıklarla fikir ve eylem birliği içerisinde Şubat 2009 tarihine kadar birçok kişiyi çalışmadıkları halde çalışıyorlarmış gibi göstererek sistem üzerinden sigorta işe giriş bildirgeleri düzenlediklerinin iddia ve kabul olunduğu davada; şifre ile bilgisayar ortamında işe giriş bildirgelerinin verilmesinden ibaret eylemin TCK'nın 244/2, 43/1. maddelerinde yazılı zincirleme şekilde sisteme veri yerleştirme suçunu oluşturacağı gözetilmeden…" **Yargıtay 11. Ceza Dairesi, 25.12.2017 tarihli ve 2017/4942 E., 2017/9307 K. sayılı kararı** https://www.lexpera.com.tr/ (E.T: 18.12.2018)

633 "Şikayetçinin mail hesabına izinsiz girip hesabın şifresini değiştirmek suretiyle bilişim sistemine girmesini engellediğinden bahisle açılan davada; IP numarası şikayetçi tarafından verilmiş olup sanığın şikayetçinin hesabına girdiği ve e-mail şifresinin değiştirildiğine dair dosya içerisinde bir tespitin bulunmaması, sanığa ait bilgisayar incelendiğinde şikayetçi ile ilgili aramaların şikayet tarihinden sonra olduğunun anlaşılması karşısında, suç tarihinden şikayet tarihine kadar olan dönemde, bu adresin faal olup olmadığı, şikayetçi tarafından kendi adresine erişim sağlanıp sağlanmadığı, sanık tarafından adrese ait şifrenin değiştirilip değiştirilmediği, değiştirilmişse hangi tarihte ve hangi IP numarası ile erişim sağlandığı Microsoft şirketinden sorulup, sonucuna göre katılana ait mail adresinin erişilmez kılındığı takdirde TCK.nun 244/2., mail adresine girildiği ancak; bu adrese erişimin engellenmemesi ve katılanın mail adresinde kalmaya devam ettiğinin tespiti halinde aynı yasanın 243/1. maddesi kapsamındaki suçun oluşacağı dikkate alınarak tüm deliller birlikte değerlendirilip gerektiğinde bilirkişiden de görüş alınarak sanığın hukuki durumunun takdir ve tayini gerekirken, eksik araştırmaya dayanarak yazılı şekilde hüküm kurulması, bozmayı gerektirmiştir." **Yargıtay 8. Ceza Dairesi, 27.09.2017 tarihli ve 2016/11236 E., 2017/10500 K. sayılı kararı** https://www.lexpera.com.tr/ (E.T: 18.12.2018)

634 **Kurt**, s.167; **Dülger,** s.337.

etmişse ikinci fıkra uygulanacaktır. Diğer bir görüşe göre ise[635] ikinci fıkrada yer alan eylemlerin birinci fıkrada belirtilen neticeyi ortaya çıkaracak seviyede olmaması gerektiği, bilişim sistemindeki verileri bozma, yok etme, değiştirme, erişilmez kılma, sisteme veri yerleştirme veya var olan verileri başka yere gönderme seçimlik hareketleriyle sistemin işleyişi engelleniyor ya da bozuluyorsa bu durumda birinci fıkranın uygulanması gerektiği ifade edilmiştir. Kanaatimizce, tek fiille birden fazla hüküm ihlal edildiğinden fikri içtima hükümlerinin uygulanarak daha fazla ceza öngörülen birinci fıkradan ceza verilmesi gerekmektedir[636].

TCK'nın 151'inci ve 244'üncü maddeleri arasındaki ilişki de doktrinde tartışmalı bir konudur. Özgenç'e göre, sistemin somut unsurlarına verilen zararların mala zarar verme suçunu, sistemin fiziki varlığına zarar vermeksizin elektronik ortamda verilen zararların ise bilişim suçunu oluşturacağını, bu ayrımın ise suçları oluşturan malvarlığı değerlerinden kaynaklandığını ifade etmektedir[637].

Dülger; 151'inci maddeyle 244'üncü maddenin birbirinden tamamen farklı iki suç tipi olduğunu ve iki farklı hukuksal değeri koruduğunu bu sebeple aralarında özel – genel hüküm ilişkisi bulunmadığından içtima hükümlerinin uygulanamayacağını ifade etmektedir[638].

Erdoğan ise TCK'nın 151'inci maddesinin oluşabilmesi için zarar gören şeyin "mal" olması gerektiği, veriler ise mal olarak değerlendirilemeyeceğinden, bu durumda suçta ve

---

635 **Karagülmez,** s.239.

636 **Apaydın,** s.319; **Ali İhsan Erdağ,** Bilişim Alanında Suçlar (Türk ve Alman Ceza Hukukunda), Gazi Üniversitesi Hukuk Fakültesi Dergisi C.14, S.2, 2010, s. 290.
"Dosya kapsamına göre sanığın, katılanın elektronik posta adresinin ve Facebook hesabının şifresini kırarak, hesaba giriş şifrelerini değiştirerek erişimini engellemesi şeklinde gerçekleşen eyleminin TCK'nın 244/2. maddesi kapsamında kaldığı gözetilmeksizin suç vasfında hataya düşülerek aynı yasanın 244/1.maddesinden mahkumiyet hükmü kurulması bozmayı gerektirmiştir." Yargıtay 15. Ceza Dairesi, 20.03.2018 tarihli ve 2017/3157 E., 2018/1848 K. sayılı kararı
https://www.lexpera.com.tr/ (E.T:18.12.2018)

637 **Özgenç**, Gazi Şerhi, s.989.

638 **Dülger**, s.338.

cezada kanunilik ve kıyas yasağı gereği TCK'nın 151'inci maddesinin uygulanamayacağı görüşündedir[639].

Kanaatimizce, bilişim sistemi, hem soyut hem de fiziki unsulardan oluştuğundan, bilişim sistemindeki verileri bozma, yok etme, değiştirme, erişilmez kılma, sisteme veri yerleştirme veya var olan verileri başka yere gönderme eylemleri yalnızca sistemin soyut yani yazılım unsuruna yapılan müdahale ile değil aynı zamanda donanım unsuruna yapılan müdahalelerle de gerçekleşebilmektedir. Dolayısıyla bilişim sisteminin donanım unsuruna yapılan müdahaleler, madde metninde öngörülen neticelerin doğmasına sebep oluyorsa ve failin kastı da bu yönde ise bu durumda hem TCK'nın 151'inci maddesinde yer alan mala zarar verme suçu hem de 244/2'nci maddesinde yer alan bilişim sistemindeki verileri bozma, yok etme, değiştirme, erişilmez kılma, sisteme veri yerleştirme veya var olan verileri başka yere gönderme suçu oluşacak ve bu durumda fikri içtima kuralları gereği daha ağır cezayı öngören 244'üncü madde uygulanacaktır.

Bir bilişim sistemindeki verilerin başka bir yere gönderilmesi aynı zamanda TCK'nın 136'ncı maddesindeki kişisel verileri hukuka aykırı olarak bir başkasına vermek, yaymak veya ele geçirmek fiillerinin zeminini oluşturabilir[640]. Ancak, 244'üncü maddede yer alan veri kavramı sistemde yer alan bütün verileri ifade etmekteyken, 136'ncı madde kapsamındaki veriler yalnızca kişisel verilerdir. Kanaatimizce, kişisel verilerin bilişim sistemleri kullanılarak oldukları yerden başka bir yere gönderilmeleri durumunda hukuka aykırı olarak verme veya yayma da söz konusu ise, hem 136'ncı maddede tanımlanmış olan suç, hem de 244'üncü maddede düzenlenmiş olan suç oluşacaktır. Bu durumda tek bir fiille birden fazla suç işlenmiş olacağından fikri içtima hükümleri uyarınca, en ağır olan suçun cezasıyla cezalandırılacaktır. Ancak, kişisel verilerin, hukuka aykırı olarak verilmesi, yayılması veya ele geçirilmesi söz konusu olmaksızın, bu nitelikteki verilerin 244'üncü

639 **Erdoğan**, Bilişim Suçları, s.215.
640 **Artuk/Gökcen/Yenidünya,** Türk Ceza Kanunu Şerhi, s.4670.

maddede sayılmış olan fiillerle bozulmaları, yok edilmeleri, değiştirilmeleri veya erişilmez kılınmaları halinde 244'üncü madde tek başına uygulama alanı bulacaktır[641].

Yine maddede yer alan sisteme veri yerleştirme eylemi ile kişisel verilerin kaydedilmesi fiilinin aynı anlama gelebilmesi mümkün olabilmektedir. Dolayısıyla burada fail tek bir hareketiyle hem 135'inci maddede yer alan kişisel verilerin kaydedilmesi suçunu hem de 244'üncü maddede yer alan sisteme veri yerleştirme suçunu işlemiş olacağından, fikri içtima hükümleri gereğince işlemiş olduğu en ağır olan suçun cezası ile cezalandırılacaktır[642].

Ayrıca failin, verilerin hukuka aykırı olarak ele geçirilmesi aynı zamanda TCK'nın 134'üncü maddesinde düzenlenen özel hayatın gizliliğini ihlal suçunu oluşturuyorsa yine bu durumda da fikri içtima kurallarının uygulanması gerekecektir[643].

TCK'nın 245/A maddesinde, 244'üncü maddede yer alan suçların işlenmesi için bir cihazın, bilgisayar programının, şifrenin veya sair güvenlik kodunun 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 kişinin

---

641 **Nil Melek Gültekin,** Kişisel Verilerin Ceza Hukuku Yönünden Korunması, Yayımlanmamış Yüksek Lisans Tezi, Galatasaray Üniversitesi SBE, İstanbul, 2012, s.177 https://tez.yok.gov.tr/UlusalTezMerkezi/ (E.T: 25.11.2018).

642 **Şeyma Sert,** Kişisel Verilerin 5237 Sayılı Türk Ceza Kanunu Kapsamında Korunması, Yayımlanmamış Yüksek Lisans Tezi, Atatürk Üniversitesi SBE, Erzurum, 2018, s.107 https://tez.yok.gov.tr/UlusalTezMerkezi/ (E.T: 25.11.2018).

643 "Oluşa ve dosya kapsamına göre; sanık ...'ın, kız arkadaşı olan mağdur ... ile aralarındaki arkadaşlık ilişkisi sona erdikten sonra, mağdura ait facebook hesabının önceden bildiği internet şifresini, onun bilgisi ve rızası dışında değiştirerek, hakkı bulunmadığı halde giriş yaptığı mağdurun facebook hesabında, beraber oldukları dönemde mağdurun bilgisi dahilinde kaydettiği cinsel içerikli görüntülerini yayımlayıp, mağdurun facebook hesabına erişimini engellemesi biçiminde sübut bulan eylemlerinin TCK'nın 244/2. maddesindeki sistemi engelleme, bozma, verileri yok etme veya değiştirme ve aynı Kanun'un 134/2. madde ve fıkrasındaki özel hayatın gizliliğini ihlal suçlarını oluşturduğuna dair yerel mahkemenin kabulünde bir isabetsizlik görülmemiştir." **Yargıtay 12. Ceza Dairesi, 24.05.2017 tarihli ve 2015/13308 E., 2017/4272 K. sayılı kararı** https://www.lexpera.com.tr/ (E.T: 18.12.2018)
"Dosya kapsamına göre; sanığın, katılanın cep telefonunu katılandan habersiz kendi kullandığı bilgisayara bağlayarak içerisinde bulunan rehber ve media dosyalarının tamamını ele geçirdiği ve cep telefonundaki kayıtları sildiği iddia ve kabul edilen olayda, sanığın sübut bulan eylemleri nedeniyle TCK'nın 244/2. maddesinde düzenlenen sistemi engelleme, bozma, verileri yok etme veya değiştirme, aynı Kanunun 134/1 maddesinde düzenlenen özel hayatın gizliliğini ihlal ve 136/1 maddesinde düzenlenen verileri hukuka aykırı olarak verme veya ele geçirme suçlarını oluşturduğu gözetilmeden sadece TCK'nın 136/1. maddesinde düzenlen verileri hukuka aykırı olarak verme veya ele geçirme suçundan sanığın mahkumiyete karar verilmesi aleyhe temyiz olmadığından bozma nedeni yapılmamıştır. **Yargıtay 12. Ceza Dairesi, 18.10.2017 tarihli ve 2016/10576 E., 2017/7642 K. sayılı kararı** https://www.lexpera.com.tr/ (E.T: 18.12.2018)

cezalandırılacağı öngörülmüştür. Bu durumda fail bu eylemleri gerçekleştirdikten sonra, 244/2'nci maddede yer alan suçu da işlemişse bu durumda gerçek içtima hükümleri uygulanacak ve fail her iki suçtan dolayı da cezalandırılacaktır[644].

E. KUSURLULUK

Bir kişinin kusurlu kabul edilebilmesi için, kusur yeteneğine sahip olmalı ve somut olayda kusurluluğu kaldıran hallerden biri var olmamalıdır[645]. Bilişim sistemindeki verileri bozma, yok etme veya erişilmez kılma, sisteme veri yerleştirme, sistemde var olan veriyi başka bir yere gönderme suçu bakımından da somut olaya göre kusurluluğu kaldıran veya azaltan haller söz konusu olabilir[646]. Bu durumda kişiye verilecek ceza bu durumlar göz önünde bulundurularak belirlenecektir.

F. SORUŞTURMA USULÜ, GÖREVLİ VE YETKİLİ MAHKEME, YAPTIRIM, ZAMANAŞIMI

Bir bilişim sistemindeki verileri bozan, yok eden, değiştiren veya erişilmez kılan, sisteme veri yerleştiren, var olan verileri başka bir yere gönderen kişinin, altı aydan üç yıla kadar hapis cezası ile cezalandırılması öngörülmüştür. Failin durumu, fiilin meydana getirdiği zarar gibi değişkenler cezanın TCK'nın 61'inci maddesi gereğince alt – üst sınır arasında bireyselleştirilmesinde etkili olacaktır. Yine şartlarının bulunması halinde ceza tayininde TCK'nın 62'nci maddesi gereğince takdiri indirim yapılması mümkündür.

TCK'nın 244/3'üncü maddesinde bu fiillerin bir banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinde işlenmesi halinde, verilecek ceza yarı oranında artırılacağı düzenlenmiştir[647]. Faile verilen cezanın iki yıldan az olması

---

644 **Akbulut,** Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme, s.47.

645 **Özbek/Doğan/Bacaksız/Tepe,** Genel Hükümler, s.339

646 Kusurluluğu azaltan veya ortadan kaldıran hallere ilişkin yaptığımız açıklamalar için bkz. s.105.

647 "Sanıkların okul ders notlarını ve devamsızlık durumlarını değiştirmek için bilişim sisteminin Milli Eğitim Bakanlığı'na bağlı okullarda kullanılan e-okul bilişim sistemi şifreleri ele geçirmek suretiyle yükletilen suçu işledikleri kabul edilmesi nedeniyle hükmolunan cezasının sitenin kamu kurumuna ait olması nedeniyle TCK.nun 244/3. maddesi gereğince cezaların arttırılması gerektiği gözetilmeden yazılı şekilde hükümler kurulması bozulmayı

halinde Ceza Muhakemesi Kanunu'nun 231'inci maddesi gereğince hükmün açıklanmasının geri bırakmasına karar verilebilir[648]. Hükmün açıklanması geri bırakılmazsa TCK'nın 51'inci maddesinde yer alan diğer şartların da bulunması halinde cezanın ertelenmesine karar verilebilir. Failin bir yıldan az ceza alması halinde yine hükmün açıklanmasının geri bırakılması ve cezanın ertelenmesi kararı verebileceği gibi TCK'nın 50'nci maddesinde yazılı seçenek yaptırımlara ve tedbirlere de çevrilebilir. Yine TCK'nın 54 ve 55'inci maddelerinde yer alan şartların bulunması halinde eşya ve kazancın müsaderesi mümkündür.

TCK'nın 246'ncı maddesinde yer alan düzenlemeye göre bilişim alanında suçlar bölümünde yer alan suçların işlenmesi suretiyle yararına haksız menfaat sağlanan tüzel kişiler hakkında bunlara özgü güvenlik tedbirlerine hükmolunacaktır. Dolayısıyla bu koşulların oluşması halinde TCK'nın 60'ıncı maddesinde yer alan faaliyet izninin iptali ve müsadere tedbirlerinin uygulanması mümkündür. Ancak, güvenlik tedbiri uygulanmasının işlenen fiile nazaran daha ağır sonuçlar ortaya çıkarabileceği durumlarda, hâkim bu tedbirlere hükmetmeyebilir.

Bilişim sistemindeki verileri bozma, yok etme, değiştirme, erişilmez kılma, sisteme veri yerleştirme veya var olan verileri başka yere gönderme suçuna ilişkin cezanın üst sınırı 3 yıl hapis cezası olarak belirlendiğinden TCK'nın 66/1-e maddesi gereğince 8 yıllık dava zamanaşımına tabi olacaktır.

Bilişim sistemindeki verileri bozma, yok etme, değiştirme, erişilmez kılma, sisteme veri yerleştirme veya var olan verileri başka yere gönderme suçu şikâyete bağlı bir suç olmadığından, resen soruşturulmakta ve kovuşturulmaktadır.

Madde metninde öngörülen ceza miktarı ile 5235 s. Adlî Yargı İlk Derece Mahkemeleri İle Bölge Adliye Mahkemelerinin Kuruluş, Görev ve Yetkileri Hakkında

---

gerektirmiştir." **Yargıtay 8. Ceza Dairesi, 15.02.2017 tarihli ve 2016/3794 E., 2017/1405 K. sayılı kararı** https://www.lexpera.com.tr/(E.T: 18.12.2018)

[648] 5271 Sayılı Ceza Muhakemesi Kanunu, 04/12/2004 tarihinde kabul edilmiş, 17/12/2004 tarihli 25673 sayılı Resmi Gazetede yayımlanarak 01.06.2005 tarihinde yürürlüğe girmiştir. http://www.mevzuat.gov.tr/MevzuatMetin/1.5.5271.pdf (E.T: 05.03.2019)

Kanunun 10,11 ve 12’nci maddeleri hep birlikte değerlendirildiğinde görevli mahkeme asliye ceza mahkemeleri olacaktır.

III. BİLİŞİM SİSTEMİ ARACILIĞIYLA KENDİSİNİN YA DA BAŞKASININ YARARINA HAKSIZ BİR ÇIKAR SAĞLAMA SUÇU

A. GENEL OLARAK

TCK'nın 244'üncü maddesinin birinci fıkrasında bilişim sistemlerinin işleyişini engelleme veya bozma, ikinci fıkrasında verileri bozma, yok etme, değiştirme, erişilmez kılma, sisteme veri yerleştirme veya var olan verileri başka yere gönderme eylemleri suç olarak düzenlenmiş olup maddenin dördüncü ve son fıkrasında da bu eylemler neticesinde haksız bir çıkar elde etmek cezai bir yaptırıma bağlanmıştır.

Bu düzenleme Sanal Ortamda İşlenen Suçlar Sözleşmesi'nin 8'inci maddesinde "*sahtekarlık yoluyla kendisi veya başkasına haksız maddi menfaat sağlamak amacıyla, bilgisayar verilerine herhangi bir şekilde yeni veriler ekleme, bilgisayar verilerini herhangi bir şekilde değiştirme, silme veya erişilmez kılma*" yer alan hükme paralel olarak yapılmıştır[649].

Doktrinde TCK'nın 244'üncü maddesinin birinci ve ikinci fıkraları neticesinde haksız menfaat elde etmenin, ilk iki fıkranın nitelikli hali mi yoksa bağımsız bir suç mu olduğuna ilişkin görüş farklılıkları bulunmaktadır. Özbek/Doğan/Bacaksız/Tepe'ye göre, yasa yapma tekniği ve madde metninde "yukarıdaki fıkralarda tanımlanan fiillerin işlenmesi suretiyle" ifadesinden yola çıkarak söz konusu fiiller işlenerek haksız çıkar sağlanması, suçun temel şeklinde bağlı nitelikli hal olarak kabul edilmelidir[650].

Diğer bir görüş ise[651] bu fıkranın, eylemin başka bir suç oluşturmaması halinde uygulanacak olması sebebiyle tali norm olduğu ve bağımsız bir suç olduğu şeklindedir.

---

649 https://www.tbmm.gov.tr/sirasayi/donem24/yil01/ss380.pdf (E.T:11.06.2018)

650 **Özbek/Doğan/Bacaksız/Tepe**. s.968, Benzer görüşler için bkz. **Avşar/Öngören,** s.139; **Pallı,** s.167.

651 **Eker**, s.127; **Yılmaz**, 5237 Sayılı TCK'nın 244. Maddesinde Düzenlenen Bilişim Alanında Suçlar, s.86; **Koca/Üzülmez**, Özel Hükümler, s.876; **Tezcan/Erdem/Önok,** s.1049; Ketizmen de bu konuyla ilgili olarak; "*Bu tür fiillerin ayrı bir suç olarak düzenlenmesinin nedeni, veri, program ya da sisteme müdahale olarak ortaya çıkan hileli hareketlerin kişiye karşı yapılmadan, malvarlığına ilişkin bir değerin elde edilebilir olmasıdır. Dolandırıcılık suçunda söz konusu olan, kişiye karşı hileli hareketlerin gerçekleştirilmesi ve bu yolla bir kişinin aldatılması ya da*

Kanaatimizce de bilişim sistemleri aracılığıyla haksız çıkar sağlama, bağımsız bir suç olarak düzenlenmiştir. Zira madde metninde suçun unsurlarının tamamına yer verilmiştir[652]. Ayrıca kanunun gelen sistematiği göz önünde bulundurulduğunda suçların nitelikli hallerine ilişkin düzenlemelerde, alt–üst sınırı olan bir cezai yaptırım öngörülmemekte, temel cezaya atıf yapılarak bir oran belirlenmektedir. Madde metninde yer alan, başka suç oluşturmama unsuru, suçun tali norm olarak düzenlenmesinden kaynaklanmaktadır[653].

B. KORUNAN HUKUKİ DEĞER

Doktrinde bu suç ile korunan hukuki değer konusunda da görüş ayrılığı bulunmaktadır.

Artuk/Gökcen/Yenidünya'nın görüşüne göre;

"*Suç tipinde korunan hukuksal değer, kişilerin özel hayatlarının gizliliğinden, malvarlığı haklarının korunmasına kadar geniş bir çerçevede ele alınabilir. Burada bilişim sistemlerine haksız müdahalelerde bulunarak kişilerin maddi ve manevi haklarına yapılan saldırılar önlenmek istenmiştir*"[654].

Dülger ise

"*İnceleme konusu suç tipini oluşturan eylemlerin gerçekleştirilmesi nedeniyle mağdurun mal varlığında bir zararın meydana gelmesi durumunda ise genellikle ya dolandırıcılık suçu ya da hırsızlık suçu gerçekleşmiş olacaktır. Dolayısıyla bu suç tipinin yeni düzenlemesi karşısında suçla korunan hukuksal değerin mağdurun manevi bir hakkının olması da olası görülmektedir*"

---

hataya düşürülmesinin söz konusu olmaması, bunun yerini bilişim sisteminin işleyişine ya da veriye teknik bir müdahalenin alması, bilişim sistemi aracılığıyla yarar sağlamaya yönelik fiillerin ayrı bir suç olarak düzenlenmesine yol açmıştır" demiştir. (**Ketizmen,** s.148).

652 **Erdoğan,** Bilişim Suçları, s.245.

653 **Apaydın**, s.199.

654 **Artuk/Gökcen/Yenidünya**, Türk Ceza Kanunu Şerhi s.4671.

demek suretiyle suç ile korunan hukuki değerin manevi haklar olduğunu belirtmektedir[655].

Ketizmen, bu suçla korunan hukuki değeri, *"madde gerekçesinde ağırlıklı olarak malvarlığına ilişkin bir değerin saldırıya uğramasına ve ihlal edilmesine vurgu yapılmış olup, bu sebeple buradaki düzenleme de topluma ait olmaktan çok kişiye ait yararın korunmasına yöneliktir"* şeklinde ifade etmiştir.[656].

Özbek/Doğan/Bacaksız/Tepe ise, mülkiyet hakkının da korunduğu görüşündedir[657].

Kanaatimizce, 244/4'üncü maddede yer alan suç, verilere veya bilişim sisteminin işleyişine müdahale edilerek haksız çıkar sağlama şeklinde işlendiğinden, malvarlığına karşı işlenen bir suçtur. Dolayısıyla korunan değerlerden biri gerçek ve tüzel kişilerin maddi menfaatleridir. Ayrıca bu hüküm 244'üncü maddenin bir ve ikinci fıkrasına atıf yapılmak suretiyle düzenlendiği için dolaylı olarak ilk iki fıkrada yer alan suçların koruduğu hukuki değerleri de korumaktadır.

C. SUÇUN UNSURLARI

1. Tipikliği Maddi Unsurları

a. Fiil

TCK'nın 244'üncü maddesinin dördüncü fıkrasında, birinci ve ikinci fıkrada yer alan fiillerin işlenmesi suretiyle kişinin kendisi ya da başkasının yararına haksız çıkar sağlaması aranmaktadır. Burada hem bilişim sistemine veya veriye müdahale edilmesi hem de çıkar sağlanması arandığından suç, çok hareketli bir suçtur[658]. Bilişim sisteminin

---

655 **Dülger**, s.341.
656 **Ketizmen**, s.163.
657 **Özbek/Doğan/Bacaksız/Tepe**, s.959.
658 **Akbulut,** Bilişim Alanında Suçlar, s.234.

işleyişinin engellenmesi veya bozulması suçlarının maddi unsurlarını oluşturan eylemler, bu suçun da eylem unsurunu oluşturmaktadır[659]. Dolayısıyla bu suç, bağlı hareketli bir suçtur[660].

Madde metninde 244'üncü maddenin ilk iki fıkrasında yer alan fiillere atıf yapılmış olduğundan yani suç ilk iki fıkrada düzenlenen fiiller aracılığıyla gerçekleşeceğinden, suç seçimlik hareketli bir suçtur[661].

Sözlükte çıkar kavramı; *"Dolaylı bir biçimde elde edilen kazanç, menfaat, yarar"* şeklinde tanımlanmıştır[662]. Hukuken tasvip edilmeyen her türlü menfaat, haksız çıkar kavramı içinde mütalaa edilebilir. O halde, failin elde ettiği bu çıkar, haklı olarak elde edilmiş bir çıkar ise, anılan suç oluşmayacaktır[663]. Fail, çıkar sağlamaya yönelik hareketi bir rızaya dayanarak gerçekleştirmişse, çıkarın haksızlığından söz edilemez[664]. Bu çıkar maddi ya da manevi olabilir[665]. Ayrıca bu suçun oluşması için failin elde ettiği yarar karşısında mağdurun uğradığı zararın da maddi ya da manevi olması önem taşımamaktadır. Yine elde edilen haksız yararın fail lehine ya da üçüncü bir kişi lehine olması da suçun oluşumuna etki etmez[666]. Ancak, sisteme yönelik hareketlerle elde edilen yarar arasında bir nedensellik ilişkisinin bulunması gerekir[667]. Suçun oluşması için failin çıkar üzerine hakimiyet kurmuş, çıkarı sağlamış olması gerekmektedir. Örneğin, bilişim sistemine girilmesi gereken verilen yanlış veya eksik girilmesi durumunda 244/2'nci madde aracılığıyla haksız çıkar elde edilmesi mümkündür. Yine, sistemde yer alan programların işleyişinin değiştirilmesi sonucunda

---

659 **Apaydın,** s.202, **Dülger,** s.344. Bu eylemler 244'üncü maddenin 1 ve 2'inci fıkralarına ilişkin değerlendirmede detaylı olarak açıklanmıştır.

660 **Koca/Üzülmez,** Özel Hükümler, s.882

661 **Erdoğan,** Bilişim Suçları, s.252; **Dülger, s**.344.

662 http://www.tdk.gov.tr/ (E.T: 13.02.2019)

663 **Yaşar/Gökcan/Artuç,** s.6763.

664 **Akbulut,** Bilişim Alanında Suçlar, s.234.

665 **Dülger,** s.349.

666 **Dülger**, s.349; "Sanığın, katılana ait banka hesabında bulunan parayı internet üzerinden üçüncü bir kişi hesabına havale etmesi biçiminde geçekleşen olayda; sanığın katılana ait parayı kendi veya üçüncü bir kişinin hesabına aktarmasıyla paranın katılanın hakimiyetinden çıktığı ve suçun tamamlandığı gözetilmeden, sanık hakkında TCK'nın 35. maddesinde düzenlenen teşebbüs hükümlerinin uygulanması suretiyle eksik ceza tayini bozmayı gerektirmiştir." **Yargıtay 2. Ceza Dairesi, 16.05.2017 tarihli ve 2014/35237 E., 2017/5611 K. sayılı kararı** https://www.lexpera.com.tr/ (E.T: 18.12.2018)

667 **Akbulut,** Bilişim Alanında Suçlar, s.235.

(banka faiz hesaplama programının işleyişini değiştirmek gibi) elde edilen haksız menfaat de bu suç kapsamında olacaktır.

b. Netice

Yasa koyucu bilişim sistemi aracılığıyla hukuka aykırı yarar sağlamak suçunun gerçekleşmesi için failin gerçekleştirdiği eylemler neticesinde haksız bir çıkar sağlanmasını aramıştır[668]. Fail bu suçta bilişim sistemi veya veriler üzerinde gerçekleştirdiği fiil sonucunda haksız menfaat elde etmektedir ve bu menfaat elde edilemezse bu suç oluşmayacaktır. Yine bu fiiller neticesinde, mağdurda maddi ya da manevi bir zarar meydana gelmektedir. Dolayısıyla suç, zarar suçudur.

c. Fail

Kanun maddesinde fail açısından herhangi bir özellik belirtilmediğinden, herkes bu suçun faili olabilir[669]. Burada failin tespiti açısından sistem ve veriler üzerinde tasarruf yetkisinin kimde olduğunun tespiti önem taşımaktadır. Örneğin, veriler üzerinde tasarruf yetkisine sahip kişi ile sistem sahibi farklı ise sistem sahibi, veriler üzerinde tasarruf yetkisine sahip olmayıp sadece kullanım yetkisi sahibi suçun faili olabilecektir.

d. Mağdur

Kanun maddesinde mağdur açısından da herhangi bir özellik belirtilmemiştir. Bu sebeple herkes suçun mağduru olabilir[670]. Artuk/Gökcen/Yenidünya'ya göre "*Failin müdahalede bulunarak haksız çıkar sağladığı bilişim sisteminin yahut verinin sahibi suçun mağdurudur*"[671]. Ancak, önceki bölümlerde de belirtmiş olduğumuz gibi bu sahiplik kavramının dar yorumlanmaması gerekir zira yalnızca sistem ya da veriler üzerinde hak

---

668 **Dülger,** s.348.

669 **Erdoğan,** Bilişim Suçları, s.253; **Koca/Üzülmez,** Özel Hükümler, s.881, **Dülger,** s.342; **Güngör**, s.107.

670 **Koca/Üzülmez**, Özel Hükümler, s.881; **Dülger**, s.342; **Erdoğan,** Bilişim Suçları, s.253; **Onur Sarı,** Uluslararası Hukuk ve Türk Ceza Hukuku Bağlamında Siber Güvenlik ve Bilişim Sistemine Yönelik Suçlar, Yayımlanmamış Yüksek Lisans Tezi, Harp Akademileri Stratejik Araştırmalar Enstitüsü, İstanbul, 2013, s.201 https://tez.yok.gov.tr/UlusalTezMerkezi/ (E.T: 25.11.2018).

671 **Artuk/Gökcen/Yenidünya**, Türk Ceza Kanunu Şerhi, s.4673.

sahibi olunması durumunda da suçtan doğrudan zarar görülmesi mümkündür[672]. Mağdurun bu suç kapsamında uğradığı zarar maddi ya da manevi olabilecektir.

e. Konu

Bu suçun konusu, bilişim sistemi veya bilişim sisteminde yer alan veriler üzerindeki maddi veya manevi yarardır[673]. Madde metninde haksız bir çıkar belirtilmiş olup bu çıkarın maddi ya da manevi oluşuna ilişkin bir sınırlama getirilmemiştir. Çıkar kelimesi sözlükte, "*dolaylı bir biçimde elde edilen kazanç, herhangi bir menfaat veya yarar*" şeklinde tanımlanmaktadır[674]. Dolayısıyla suçun oluşumu bakımından yararın türü önem taşımamakta, haksız bir şekilde elde edilmiş olması gerekmektedir[675].

f. Suçun Nitelikli Unsurları

Kanaatimizce TCK'nın 244/4'üncü maddesinde, ilk iki fıkra için düzenlenen ağırlatıcı neden uygulanamayacaktır. Kaldı ki dördüncü fıkranın madde metninde üçüncü fıkranın uygulanacağına dair bir atıf da bulunmamaktadır. Dolayısıyla birinci veya ikinci fıkradaki eylemler neticesinde haksız çıkar sağlanırken, üçüncü fırkadaki kurum ve kuruluşlara ait bilişim sistemlerinin kullanılması halinde dahi üçüncü fıkrada yer alan artırım uygulanamayacaktır. Bu durum sonuç itibariyle failin daha az cezalandırılmasına neden olabileceği için eleştirilmektedir[676].

Ayrıca, 3713 Sayılı Kanunun 5'inci maddesinde ise, 4'üncü maddede sayılan suçların terör amacıyla işlenmesi halinde tayin edilecek hapis cezaları veya adlî para cezalarının yarı oranında artırılacağı, bu suretle tayin olunacak cezalarda gerek o fiil için gerek her nevi ceza için muayyen olan cezanın yukarı sınırının aşılabileceği düzenlendiğinden suçun terör amaçlı işlenmesi halinde artırım yapılacaktır.

---

672 **Erdoğan,** Bilişim Suçları, s.253; **Dülger**, s.342.
673 **Erdoğan**, Bilişim Suçları, s.255; **Yılmaz,** 5237 Sayılı TCK'nın 244. Maddesinde Düzenlenen Bilişim Alanındaki Suçlar, s.86.
674 http://www.tdk.gov.tr/ (E.T: 13.02.2019)
675 **Koca/Üzülmez**, Özel Hükümler, s.881; **Dülger,** s.343.
676 **Erdoğan,** Bilişim Suçları, s.256**; Kurt,** s.244.

2. Tipikliğin Manevi Unsurları

Bu suçun manevi unsuru hakkında doktrinde bir görüş birliği bulunmamaktadır. Artuk/Gökcen/Yenidünya, suçun kasten işlenebileceğini, doğrudan kasta ve saike işaret eden herhangi bir ibare yer almadığını ifade etmiştir[677].

Karagülmez'e göre ise, failin kendisinin ya da başkasının yararına haksız bir çıkar sağlama suçunu işlemesinde özel kast söz konusudur[678]. Kurt da benzer şekilde suçun oluşabilmesi için failin kendisine veya başkasına çıkar sağlama kastıyla hareket etmesi gerektiğini ifade etmiştir[679].

Dülger ise suçta kast dışında bir amaç unsurunun aranmadığı düşüncesindedir[680].

Kanaatimizce de bu suç kasten işlenebilecek bir suçtur. Failin suçun tüm unsurlarını bilmesi ve istemesi gerekli ve yeterlidir[681]. Madde metninde açıkça taksirden dolayı ceza verilebileceği düzenlenmediğinden, fiilin taksirle işlenmesi halinde fail cezalandırılmaz[682]. Ayrıca failin bu fiillerden kendisine veya başkasına çıkar sağladığını ve bu çıkarın da haksız olduğunu bilmesi gerekir. Failin, elde ettiği çıkarın haksız olduğunu bilmesi gerektiğinden suç ancak doğrudan kastla işlenebilecektir. Zira suç tipinde fiilin haksızlığına ilişkin belirleme yapıldığından, çıkarın haksızlığı noktasında failde bulunması gereken bilgi kast kapsamındadır. Elde ettiği çıkarın haksız olduğunu bilmiyorsa, tipiklik oluşmaz[683].

3. Hukuka Aykırılık Unsuru

TCK'nın 244'üncü maddesinin dördüncü fıkrasında, ilk iki fıkradaki suçlara atıf yapılmış olduğundan, o suçlara ilişkin hukuka uygunluk sebepleri burada da geçerlidir. Ancak bu fıkrada failin haksız çıkar elde etme hususunun açıkça belirtilmesi sebebiyle,

---

677 **Artuk/Gökcen/Yenidünya,** Türk Ceza Kanunu Şerhi, s.4673.
678 **Karagülmez,** s.244.
679 **Kurt,** s.175.
680 **Dülger,** s.351; **Erdoğan,** Bilişim Suçları, s.257.
681 **Koca/Üzülmez,** Özel Hükümler, s.883; **Tezcan/Erdem/Önok**, s.1050.
682 **Artuk/Gökcen/Yenidünya** Türk Ceza Kanunu Şerhi, s.4673**, Erdoğan,** Bilişim Suçları, s.258.
683 **Akbulut,** Bilişim Alanında Suçlar, s.261.

bilişim sistemi ya da veri üzerinde hak sahibi olan kişinin rızası bulunması halinde yapılan eylemler suç teşkil etmeyecektir. Ancak hukuka uygunluk sebebinin gerçekleşmesi için rıza gösteren kişinin sıfatı önem taşıdığından her somut olayda sistemin ya da verilerinin malikinin ya da ilgilisinin ayrı ayrı tespit edilip mağdurunun belirlenmesi gerekir[684].

Kanunen verilen veya sözleşmeyle öngörülen yetkiye dayanılarak fiilin gerçekleştirilmesi halinde fiil hukuka aykırılık teşkil etmeyecektir. Örneğin, devletin belirli döneme ait veya bazı şartların gerçekleşmesi nedeniyle, vergi borçlarının silinmesi yolunda karar alması ve buna dayanılarak vergi borçlarının silinmesi durumunda fiil suç oluşturmayacaktır[685].

D. SUÇUN ÖZEL GÖRÜNÜŞ ŞEKİLLERİ

1. Teşebbüs

TCK'nın 244'üncü maddesinin dördüncü fıkrasında düzenlenen suç, maddenin ilk iki fıkrasında belirtilen hareketlerin yapılması neticesinde haksız çıkar elde etme ile tamamlanır. Failin kastının hukuka aykırı yarar elde etmek olduğunun tespit edildiği ancak 244'üncü maddenin birinci veya ikinci fıkralarında yer alan eylemler tamamlandıktan sonra haksız yarar elde etme neticesinin failin elinde olmayan sebeplerle gerçekleşmemesi durumunda failin dördüncü fıkraya teşebbüsten cezalandırılması gerekmektedir. Failin böyle bir durumda dördüncü fıkraya ilişkin kastının belirlenememesi halinde ise tamamladığı suçtan dolayı cezalandırılması gerekir[686]. Failin birinci veya ikinci fıkradaki eylemlere

---

684 **Dülger**, s.352.

685 **Akbulut,** Bilişim Alanında Suçlar, s.260.

686 **Dülger**, s.352. **Özbek/Doğan/Bacaksız/Tepe** bu konuda "Haksız bir çıkar sağlanmış değilse teşebbüsten söz edilemez; artık bu halde unsurları oluştu ise 1 ya da 2. f daki suçlardan o da mümkün değil ise TCK m.243'ten ceza vermek gerekir" demektedir. (**Özbek/Doğan/Bacaksız/Tepe**, s.973)
"Sanık ...'nun ... Eczanesi sahibi,sanık ... ile ...'ün ise kalfa olarak çalıştıkları, Medula sistemini kullanmaya yetkili sanıklar ... ile ...'ün olay tarihlerinde kendi çalıştıkları ... Eczanesi'nin şifresi ve katılan ...'ya ait ... Eczanesi'nin haksız şekilde elde ettikleri Medula sistemine giriş şifresi ile önce hayali bir reçetenin eczanelerden birinin şifresiyle Medula Eczane sistemine giriş yapıldığı, hayali reçete Medula Eczane Sistemine kayıtlı iken bu kez diğer eczanenin sisteminden giriş yapılarak gerçek reçetenin sisteme kaydedildiği, hayali reçetenin sisteme kaydedilmesi ile hasta muayene ücretinin çıktığı, ancak hayali reçete sistemde kayıtlı bulunduğu halde diğer eczaneden gerçek reçetenin girişi yapıldığında muayene ücretinin çıkmadığı ve reçetenin karşılandığı, bu kez gerçek reçete karşılandıktan sonra hayali reçetenin sistemden silindiği ve hastaya ait muayene ücretinin bu işlemle bir sonraki ilaç alışına kadar

başlayıp elinde olmayan sebeplerle tamamlayamaması halinde de yine dördüncü fıkraya yönelik bir kasıt tespit edilebiliyorsa dördüncü fıkraya teşebbüsten, tespit edilemiyorsa birinci veya ikinci fıkraya teşebbüsten, somut olaya göre bunun da mümkün olmaması durumunda 243'üncü maddenin birinci fıkrasından cezalandırılmalıdır. Ancak burada belirleyici unsur failin kastı olduğundan tespit açısından zorluklar ortaya çıkmaktadır.

4. İştirak

Bu suç iştirak açısından bir özellik göstermemektedir[687]. TCK'nın 37 ve devamında yer alan genel iştirak hükümleri bu suçta da geçerlidir.

5. Suçların İçtiması

TCK'nın 42'nci maddesinde bileşik suç tanımlanmıştır. Buna göre; "*Biri diğerinin unsuru veya ağırlatıcı nedenini oluşturması dolayısıyla tek fiil sayılan suça bileşik suç denir. Bu tür suçlarda içtima hükümleri uygulanmaz"*.

Yaşar/Gökcan/Artuç, bu konu ile ilgili

> *"TCK m. 244'ün dördüncü fıkrasında öngörülen suçun işlenebilmesi için öncelikle failin, birinci veya ikinci fıkrada düzenlenen eylemlerden birisini gerçekleştirmesi gerekir. Burada failin birinci veya ikinci fıkrada belirlenen eylemlerden birisini gerçekleştirmesi ve bu eylemleri gerçekleştirdikten sonra, kendisi veya başkası yararına haksız bir çıkar sağlaması gerekir. Anılan suç bu özelliği gereği, bileşik suç niteliğindedir. Burada birinci ve ikinci fıkrada düzenlenen suçlar, üçüncü fıkrada düzenlenen suçun unsuru haline gelmiştir."* şeklinde bir açıklama yapmıştır[688].

ötelenerek bilişim sistemindeki verileri bozma, yok etme, sisteme veri yerleştirme suçunu işlediklerinden bahisle açılan davada; sanıkların sübut bulan eylemlerinde, dosya kapsamından yapılan işlemlerin katılan kurumun alacağını geciktirmekten ibaret olduğu, ortadan kaldırmadığı, bu surette bir haksız menfaat elde edilmediğinin anlaşılması karşısında, katılan ...'ya ait eczanenin şifresini haksız ele geçirip bunun vasıtasıyla ...'na ait bilişim sistemine giriş yapıp sahte veri yerleştirip amacına ulaştıktan sonra silmek şeklindeki eylemin TCK.nun 244/2 ve 3. maddelerindeki suç kapsamında değerlendirilmesi gerektiği gözetilmeden anılan maddenin 4. fıkrasıyla hüküm kurulması bozmayı gerektirmiştir." **Yargıtay 8. Ceza Dairesi, 31.05.2017 tarihli ve 2016/12437 E., 2017/6369 K. sayılı kararı** https://www.lexpera.com.tr/ (E.T: 18.12.2018)

687 **Dülger**, s.353; **Koca/Üzülmez,** Özel Hükümler, s.864.

688 **Yaşar/Gökcan/Artuç,** s.6736. Benzer görüş için bkz. **Artuk/Gökcen/Yenidünya,** Türk Ceza Kanunu Şerhi, s.4673.

Kanaatimizce de suç bileşik suç niteliğinde olduğundan, bilişim sisteminin işleyişini engellemek veya bozmak ya da bilişim sistemindeki verileri bozmak, yok etmek, değiştirmek veya erişilmez kılmak, sisteme veri yerleştirmek, verileri başka yere göndermek suretiyle kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlaması durumunda, eylemin başka bir suç oluşturmaması halinde[689] yalnızca dördüncü fıkra uygulanacaktır. Eylemin başka bir suç oluşturması halinde ise her durumda o hükmün uygulanması gerekmektedir[690]. Bu sebeple suç tali norm özelliği taşımaktadır. Bu durumda bilişim sistemleri aracılığıyla haksız çıkar sağlama şeklinde bir olayla karşılaşıldığında öncelikle fiilin, örneğin; dolandırıcılık, hırsızlık, güveni kötüye kullanma veya zimmet gibi başka bir suçu oluşturup oluşturmadığı araştırılmalıdır. Eylem bu suçlardan birinin tanımına uyuyorsa fikri içtima kurallarına gidilmeden ve bu suçun daha ağır bir ceza gerektirip gerekmediği dikkate alınmaksızın bu hükmün uygulanması gerekir[691].

TCK'nın 43'üncü maddesinde zincirleme suç hükümleri yer almaktadır. Buna göre failin bir suç işleme kararı ile aynı suçu bir kişiye karşı farklı zamanlarda işlemesi halinde tek ceza verilecek ve cezada artırıma gidilecektir. Yine failin bu suçu birden fazla kişiye karşı, tek bir fiille işlemesi halinde de tek ceza verilerek cezada artırım yapılacaktır[692].

---

689 **Artuk/Gökcen/Yenidünya,**, Türk Ceza Kanunu Şerhi, s.4672 Kurt, s.244.

690 **Erdoğan,** Bilişim Suçları, s.264; **Ketizmen,** s.177; **Değirmenci,** 2004 Türk Ceza Kanunu'nun Bilişim Suçları Bakımından Değerlendirilmesi, s.206; **Necati Meran**, Yeni Türk Ceza Kanununda Sahtecilik – Malvarlığı – Bilişim Suçları ile Ekonomi ve Ticaret Alanında Suçlar, Seçkin Yayıncılık, Ankara, 2005, s.373.

691 **Apaydın**, s.210.

692 "*Dolandırıcılık suçunda unsur olan hileli davranışların gerçek kişiye yönelmesi ve bunun sonunda onun veya başkasının malvarlığı aleyhine sanığın veya başkasının yararına haksız bir menfaat sağlanması gerekeceği, somut olayda ise, sanığın mağdur Murat'ın ... Bankası ... Şubesindeki hesabına ait internet şifresini kırarak, 21.11.2006 tarihinde hesapta bulunan 4500 YTL'yi İskenderun'da bulunan Veli'den aldığı bilgisayar bedeli olarak havale etmesi, 22.11.2006 günü ise 3700 YTL'yi İstanbul ili Beşiktaş ilçesinde bulunan Tuncay'dan sipariş ettiği televizyon bedeli olarak aynı yöntemle havale etmesinden ibaret eyleminde, gerçek kişiye yönelen hileli bir davranış bulunmaması nedeniyle fiilin zincirleme şekilde 5237 sayılı TCK'nın 244/4 maddesine uygun "bilişim sistemini engelleme, bozma, verileri yok etme veya değiştirme suretiyle haksız çıkar sağlama" suçunu oluşturduğu gözetilmeden, suç vasfının tayininde yanılgıya düşülerek yazılı şekilde bilişim sistemlerinin aracı olarak kullanılması suretiyle dolandırıcılık suçundan mahkumiyetine karar verilmesi.."* Yargıtay 11. Ceza Dairesi, 10.03.2008 tarihli 2008/362 E. 2008/1377 K. sayılı kararı www.kazanci.com (E.T:10.07.2019)

Bu suçun mütemadi şekilde işlenmesi de mümkündür. Bu durumda suç, devam eden eylemin bittiği zaman gerçekleşmiş sayılır ve zamanaşımı da bu andan itibaren işler[693].

TCK'nın 247'nci maddesinde düzenlenmiş olan zimmet, bir kamu görevlisinin görevi nedeniyle kendisine devredilmiş olan veya koruma ve gözetimiyle yükümlü olduğu malı kendisinin veya başkasının mülkiyetine sokması suçudur[694]. Bu suçun konusu da madde gerekçesinde ifade edildiği üzere taşınır veya taşınmaz mallardır. Veriler, fiziki bir varlığa sahip olmadıklarından, ekonomik değer taşısa bile mal olarak kabul edilemeyecektir. Dolayısıyla, devlet kurumunda çalışan bir memur, görev nedeniyle ulaşabildiği bir kısım verilerin kopyasını daha sonra kullanmak kastıyla alsa, veri bir mal sayılmayacağından bu durumda zimmet suçu oluşmayacaktır[695].

---

693 **Dülger**, s.354, **Erdoğan,** Bilişim Suçları, s.265.

694 *"Madde 247- (1) Görevi nedeniyle zilyedliği kendisine devredilmiş olan veya koruma ve gözetimiyle yükümlü olduğu malı kendisinin veya başkasının zimmetine geçiren kamu görevlisi, beş yıldan oniki yıla kadar hapis cezası ile cezalandırılır. (2) Suçun, zimmetin açığa çıkmamasını sağlamaya yönelik hileli davranışlarla işlenmesi halinde, verilecek ceza yarı oranında artırılır. (3) Zimmet suçunun, malın geçici bir süre kullanıldıktan sonra iade edilmek üzere işlenmesi halinde, verilecek ceza yarı oranına kadar indirilebilir."*

695 **Kurt,** s.172;
Suç tarihinde SGK... İl Müdürlüğü Mali Hizmetler Sosyal Güvenlik Merkezi veri hazırlama ve kontrol işletmeni olarak görev yapan sanığın, kurumdan sadece yetim aylığı alma hakkı bulunan diğer sanık ...'un banka hesabına 79 adet sahte muhasebe işlem fişi düzenleyerek 1.056.869,69 TL ödeme yaptığı, daha sonra ise ...'un banka kartını kullanmak veya kendi hesabına para transferi yapmak suretiyle bu miktarı zimmetine geçirdiğinin iddia ve kabul edildiği olayda; sanığın savunmasında emanet hesaplarda duran paraları kurumun kendisine vermiş olduğu şifre ile sisteme giriş yapıp aktardığını beyan etmesi karşısında, öncelikle ödemeleri kurumun hangi hesapları üzerinden yaptığının açıkça tespit edilmesi, sanığın bu hesaplar üzerindeki tasarruf yetkisi kurumdan sorularak yasal tevdii unsurunun oluşup oluşmadığı ile muhafaza ve gözetim sorumluluğu bulunup bulunmadığının değerlendirilmesi, yapmış olduğu işlemleri kurumun MOSİP sistemi üzerinden banka hesaplarına başka bir işleme gerek kalmadan giriş ile mi yoksa internet bankacılığı vasıtası ile mi ya da bankaya verdiği bir talimat ile mi gerçekleştirdiğinin tespit edilmesi, yine aktarmış olduğu paralar için öncesinde tahakkuk ve benzeri ödemeye esas teşkil edecek işlemler yapıp yapmadığının tespitiyle onaylı örneklerinin dosya arasına alınmasından sonra dosyanın kül halinde konunun uzmanı Sayıştay uzman denetçilerinden oluşan bilirkişiler kuruluna tevdi edilerek; iddia, savunma ve tüm kanıtlar birlikte değerlendirilip sanığın zimmetinde kuruma ait para bulunup bulunmadığı varsa zimmetin ne şekilde gerçekleştiği hususlarında rapor alınması, sanığın ödemeleri yapmış olduğu hesaplar nazara alındığında 5237 sayılı TCK'nın 247. maddesinde düzenlenen zimmet suçunun oluşması için "kamu görevlisinin veya özel mevzuatları gereği kamu görevlisi gibi cezalandırılabilen kişilerin görevi nedeniyle zilyetliği kendisine devredilmiş olan veya koruma ve gözetimiyle yükümlü olduğu malı kendisinin veya başkasının yararına zimmetine geçirmesinin" gerektiği, yasal tevdii unsurunun ve koruma yükümlülüğünün bulunmaması halinde eylemin kamu kurumu zararına dolandırıcılık suçunu oluşturacağı, yine sanığın aktarmış olduğu paralara ilişkin yaptığı işlemler neticesinde sistem tarafından otomatik olarak düzenlenen 79 adet sahte muhasebe işlem fişinin ne şekilde hazırlandığı saptanarak bu işlemleri yapabilmesi için elektronik imza kullanıp kullanmadığı elektronik imza ile imzalanmış ise evrakların hukuki geçerliliğinin olacağı, kullanmaması halinde ise söz konusu muhasebe işlem fişlerinin fiziki çıktılarının alınmaması ve yetkili kişiye de imzalatılmaması sebebiyle sahte oluşturulmuş maddi varlığı haiz somut bir belge olmadığından eylemin TCK'nın 244. maddesinin 2. fıkrasında düzenlenen sisteme veri yerleştirme suçunu oluşturacağı gözetilmeden eksik inceleme ve yetersiz gerekçe ile yazılı şekilde mahkumiyet hükümleri kurulması

Bu suçun hırsızlık suçu ile içtimaı;

Hırsızlık suçu, TCK'nın 141'inci maddesinde tanımlanmıştır. Buna göre; "*zilyedinin rızası olmadan başkasına ait taşınır bir malı, kendisine veya başkasına bir yarar sağlamak maksadıyla bulunduğu yerden alma"* eylemi yaptırıma bağlanmıştır.

Hırsızlık suçunun bilişim sistemleri aracılığıyla işlenmesi ise TCK'nın 142/2-e maddesinde suçun nitelikli hali olarak düzenlenmiştir[696]. Buna göre, hırsızlık suçunun bilişin sistemlerinin kullanılması suretiyle işlenmesi halinde daha ağır cezaya (beş yıldan on yıla kadar) hükmedilecektir.

Hırsızlık suçunun konusunu taşınır mal oluşturmaktadır. Taşınır mal, insanın yaşam ve ilişkilerinde herhangi bir gereksinim için kullandıkları taşınabilir şey olarak tanımlanmaktadır[697]. Burada önemli olan, malın fiziki bir yapısının olmasıdır.

Bir suçun nitelikli halinin oluşması için öncelikle temel halinin ihlal edilmesi gerekir. Temel suç tipi gerçekleşmeden, suçun nitelikli hali işlenemez[698]. Dolayısıyla eylemin bilişim sistemi aracılığıyla gerçekleştiğini söylemek için TCK'nın 141'inci maddesinde yer alan unsurların da gerçekleşmiş olması gerekir. Bu maddede aranan unsurlar ise; yarar sağlama maksadı, malın taşınır olması, zilyedin rızasının olmaması, malın bulunduğu yerden alınmasıdır. Bilişim sisteminde yer alan verinin ele geçirilmesi ile ifade edilmek istenen, verinin içerdiği kodların kopyalanarak başka bir yere aktarılmasıdır. Bu sebeple veri TCK'nın 141'inci maddesi anlamında taşınır mal sayılamayacaktır[699].

---

bozmayı gerektirmiştir. **Yargıtay 5. Ceza Dairesi, 26.03.2018 tarihli ve 2018/529 E., 2018/2134 K. sayılı kararı** https://www.lexpera.com.tr/ (E.T: 18.12.2018)

696 **Ahmet Gökcen/Selim Erdin/Büşra Şenerdoğan,** Hırsızlık Suçu (m.141), Malvarlığına Karşı Suçlar (m.141-169), Adalet Yayınevi, Ankara 2018, s.47.

697 **Özbek/Doğan/Bacaksız/Tepe,** s.597.

698 **İsa Başbüyük,** Hırsızlık ve Dolandırıcılık Suçlarının Bilişim Sistemlerinin Araç olarak Kullanılması Suretiyle İşlenmesi, Ceza Hukuku Dergisi, Aralık 2010, Sayı:4, s.5.

699 "Verilerin hukuka aykırı olarak ele geçirilip, bundan da yarar sağlanmasının; ekonomik değer taşısa dahi veriyi taşınır mal haline getirmeyeceği, bu itibarla; suçun sübutu halinde eylemin, 5237 sayılı TCK'nın 244/4. maddesindeki suçu oluşturacağı gözetilmeksizin suç vasfında yanılgıya düşülerek yazılı şekilde hüküm kurulması bozmayı gerektirmiştir." **Yargıtay 13. Ceza Dairesi, 10.10.2017 tarihli ve 2016/2155 E., 2017/10403 K. sayılı kararı** https://www.lexpera.com.tr/ (E.T: 18.12.2018)

Hırsızlık suçunun bilişim sistemleri aracılığıyla işlenmesi, suçun işlenişinde sağladığı kolaylık ve başkaca hukuki yararların da ihlalini içerdiği için, nitelikli hal olarak öngörülmüştür[700]. Tezcan/Erdem/Önok, bu hükmün uygulama imkanı olmadığı görüşündedir. Yazara göre;

> "*her ne kadar bentte "bilişim sistemlerinin" kullanılarak hırsızlık suçunun işlenmesi, bu suçun nitelikli hali olarak kabul edilmiş ise de; bilişim sistemleri kullanılmak suretiyle haksız bir yarar elde edilmesi durumunda daha çok dolandırıcılık veya diğer bilişim suçları gündeme gelebilir ise de; hırsızlık suçunun oluşması çoğu durumda mümkün gözükmediği için hükmün uygulama alanı oldukça sınırlı gözükmektedir."*[701].

TCK'nın 142/2-e ile m.244/4'üncü maddelerinin uygulanması konusunda doktrinde esas alınan bir kıstas bulunmaktadır. Buna göre uygulanacak hüküm yararın sağlandığı an esas alınarak belirlenecektir. Eğer haksız yarar, mal elde edilmeden sağlanabiliyorsa bu durumda TCK'nın 244/4'üncü maddesi uygulanacaktır. Ancak bilişim sistemine müdahale edilmesine rağmen yararın elde edilmesi için taşınır malın bulunduğu yerden alınması gerekiyorsa bu durumda TCK'nın 142/2-e maddesindeki nitelikli halin uygulanması gerekir[702]. Yargıtay internet üzerinden başkasının hesabından para aktarılması konusunda önceleri yararın elde edildiği an kıstasına göre TCK'nın 244/4'üncü maddesinin uygulanması gerektiği yönünde kararlar verirken, Yargıtay Ceza Genel Kurulunun 17.11.2009 gün ve 2009/11-193 esas ve karar sayılı ilamında internet bankacılığı üzerinden bir hesaptan başka bir hesaba hukuka aykırı şekilde para aktarılmasında, amacın var olan verinin başka bir yere gönderilmesinden ziyade verinin temsil ettiği parayı alarak mal edinmeye yönelik olduğu gerekçesi ile nitelikli hırsızlık suçunu oluşturduğuna karar vermiştir[703].

---

700 **Başbüyük**, s.5, **Erdoğan**, Bilişim Suçları, s.278; **Koca/Üzülmez**, Özel Hükümler, s.603.

701 **Tezcan/Erdem/Önok,** s.538 Aksi görüş için bkz. **Ketizmen,** s.181.

702 **Başbüyük**, s.5; **Ketizmen,** s.182; **Erdoğan** Bilişim Suçları, s.280.

703 Sanık Volkan'ın; firari Saim ile birlikte hareket ederek, daha önceden haksız bir şekilde ele geçirdikleri katılan firmanın internet bankacılık şifresini kullanmak suretiyle, katılanın Ş...bank Ankara K... Şubesindeki hesabından 10.750 YTL'yi Ş...bank-İstanbul Z... Şubesinde sanık Volkan adına açtırdıkları hesaba havale edip, aynı gün banka şubesinden çekmek şeklinde gerçekleştirdiği eylemdeki kastı, katılan firmanın banka hesabında bulunan, taşınır nitelikteki parayı bilişim sistemini kullanmak suretiyle kendi banka hesaplarına geçirmeye, katılanın rızasına aykırı olarak malvarlığında azalmaya neden olmaya; başka bir anlatımla var olan veriyi başka bir yere göndermekten

Yargıtay tarafından verilen yeni tarihli kararlarda TCK'nın 244/4'üncü maddesinin tali norm olması ve madde metninde eylemin başka bir suç oluşturmaması halinde uygulanabilir olması gerekçesi ile öncelikle 142/2-e maddesinin değerlendirilmesi, bu suçun oluştuğunun anlaşılması halinde ise bu madde kapsamında karar verilmesi gerektiğine hükmedilmiştir.[704]

Online satış hizmetlerinde, başkasına ait şifrenin ve diğer bilgilerin ele geçirilerek alış veya satış yapılması mümkün olabilmekte ve bu şekilde haksız menfaat elde edilebilmektedir. Bu durumda, banka ve kredi kartları kullanılmadan, TCK'nın 244'üncü maddesinin bir veya ikinci fıkrasında belirtilen fiiller gerçekleştirilerek haksız çıkar sağlanması durumunda 244'üncü maddenin dördüncü fıkrası uygulanacaktır. Ancak, 244'üncü maddenin birinci veya ikinci fıkrasında yer alan eylemler gerçekleştirilmeden haksız çıkar sağlanmışsa bu durumda 142/2-e maddesi uygulanacaktır[705].

---

ziyade, bu verinin temsil ettiği parayı alarak mal edinmeye yöneliktir. Kaldı ki sanığın katılanın internet bankacılık hesabında bulunan parasına ulaşmak için bilişim sistemlerini araç olarak kullanmaktan başka alternatifi de yoktur. Dolayısıyla olayımızda, 5237 sayılı TCY'nin 142/2-e maddesinde düzenlenmiş bulunan bilişim sistemi kullanılmak suretiyle hırsızlık" suçunun gerçekleştiği kabul edilmelidir. Şu halde, sanığın eyleminin 5237 sayılı TCY'nin 142/2-e maddesindeki nitelikli hırsızlık suçunu oluşturduğunun kabul edilmesi karşısında; 244. maddenin 4. fıkrası uyarınca uygulama yapma olanağı da bulunmamaktadır. **Yargıtay Ceza Genel Kurulu, 17.11.2009 tarihli ve 2009/11-193 E., 2009/268 K. sayılı kararı** https://www.lexpera.com.tr/ (E.T:18.12.2018)

704 "Sanığın, internet bankacılığı aracılığıyla katılana ait banka hesabından, kendi hesabına para aktarma biçimindeki eyleminin, TCK'nın 142/2-e maddesinde düzenlenen hırsızlık suçunu oluşturduğu gözetilmeden suç vasfının değerlendirilmesinde yanılgıya düşülerek aynı Kanun'un 244/4. maddesi gereğince yazılı şekilde hüküm kurulması bozmayı gerektirmiştir." **Yargıtay 2. Ceza Dairesi, 30.05.2017 tarihli ve 2014/37954 E., 2017/6242 K. sayılı kararı** https://www.lexpera.com.tr/ (E.T: 18.12.2018)
"Katılanın bilgisi ve rızası dışında Garanti Bankası .... Şubesindeki hesabındaki parasının, internet bankacılığı kullanılarak başka hesaplara havale edilmesi şeklinde gerçekleşen eylemin, 5237 sayılı TCK'nın 142/2-e maddesinde düzenlenen "bilişim sistemlerinin kullanılması suretiyle hırsızlık" suçunu oluşturduğu gözetilmeden; suç vasfında yanılgı sonucu aynı Yasa'nın 244/4. maddesi gereğince uygulama yapılması bozmayı gerektirmiştir." **Yargıtay 2. Ceza Dairesi, 02.05.2018 tarihli ve 2016/8236 E., 2018/5425 K. sayılı kararı** https://www.lexpera.com.tr/ (E.T: 18.12.2018)
"Sanıkların, katılanın bilgisi ve rızası dışında ING Bankası .... Şubesindeki parasının, internet bankacılığı kullanılarak sanıkların hesaba havale edilmek suretiyle çalınması şeklindeki eyleminin, 5237 sayılı TCK'nın 142/2-e maddesinde düzenlenen "bilişim sistemlerinin kullanılması suretiyle hırsızlık" suçunu oluşturduğu gözetilmeden; sanıklar hakkında ayrıca aynı kanunun 244/2 maddesi gereğince cezalandırılmalarına karar verilmesi bozmayı gerektirmiştir." **Yargıtay 2. Ceza Dairesi, 22.05.2018 tarihli ve 2015/6619 E., 2018/6656 K. sayılı kararı** https://www.lexpera.com.tr/ (E.T: 18.12.2018)

705 WEB sitesi üzerinde, verilerin bozulduğuna, yok edildiğine, değiştirildiğine veya erişilmez kılındığına, sisteme veri yerleştirildiğine, var olan verilerin başka bir yere gönderildiğine ilişkin bir iddia bulunmadığı gibi buna ilişkin bir tespite de rastlanmamıştır. WEB sitesine girişte abone olan katılan tarafından kullanılan kullanıcı adı ve parola bilgilerinin sanık tarafından ele geçirilmesi sonucu WEB sitesinden "tek şifre" uygulamasından faydalanarak site tarafından abonelerine ücreti karşılığı sunulan ürün ve servis hizmetlerinden olan oyun satın alıp indirme

Bu kapsamda son zamanlarda gittikçe önem kazanan kripto paralar ve bunların en çok kullanılanı olan bitcoinlerin suç konusu olması halinde uygulanacak hükmün değerlendirilmesi gerekmektedir.

Mal ve hizmetlerin mübadele edilmesinde kullanılan takas yönteminden, emtia paraya, sonra altın/gümüşe, daha sonra altın karşılığı olan değerli kağıtlara, oradan altın karşılığı bulunmayan güvene dayalı itibari paraya derken, paranın evrimi dijital ve sanal paralara doğru yol almaktadır[706]. Dijital paralar, elektronik olarak saklanan ve transfer edilebilen paralardır[707]. Banka hesaplarındaki dijital para, kâğıt paraların temsili olup bankaların her yerde bulunması, elektronik paranın yaygınlaşması ve fiziki paranın kullanımdan neredeyse kalkması, dijital parayla gerçek fiziki paranın arasındaki farkı ortadan kaldırmak üzeredir. Altından, altına dayalı kâğıt paraya, ondan itibari paraya, sonrasında ise dijital paraya geçiş, bilişim teknolojilerinin gelişmesi ile mümkün olmuştur[708]. Sanal paralar da bir dijital paradır ancak temsil ettikleri bir fiziksel gerçeklik yoktur. Kripto-paralar ise alternatif para birimi olup, dijital ve aynı zamanda sanal paradırlar[709]. Bitcoin ve türevleri dışındaki dijital ve sanal paralar, kendi başlarına para birimi değillerdir, temsil ettikleri ülkenin ulusal para birimine dayalıdırlar ve o ülkenin merkezi otoritelerince düzenlenip denetlenebilirler[710]. Bitcoin ise kendiliğinden bir para birimidir, merkezi otorite tarafından düzenlenip denetlenemez[711].

---

bölümünden oyun satın alarak, buna ilişkin ücretin katılanın internet faturasına yansıtılması suretiyle haksız menfaat temin etmek şeklindeki eyleminin, bilişim suretiyle hırsızlık suçunu oluşturacağı gözetilmeden suç vasfında yanılgıya düşülerek oluşa uygun olmayan kabulle yazılı şekilde hüküm kurulması bozmayı gerektirmiştir. **(Yargıtay 8. Ceza Dairesi, 22.12.2015 tarihli ve 2015/7063 E., 2015/26040 K. sayılı kararı)** www.lexpera.com (E.T: 07.07.2019)

706 **Abdurrahman Çarkacıoğlu,** Kripto-Para Bitcoin, Sermaye Piyasası Kurulu Araştırma Dairesi, Ankara 2016, s.1. http://www.spk.gov.tr/SiteApps/Yayin/YayinGoster/1130 (E.T: 03.07.2019)

707 **Andrew Wagner,** Digital vs. Virtual Currencies, Bitcoine Magazine, S:22 Ağustos 2014, https://bitcoinmagazine.com/articles/digital-vs-virtual-currencies-1408735507 (E.T:13.07.2019)

708 **Çarkacıoğlu,** s.6; **Mert Yılmaz Özbaş,** Elektronik Para ve Sanal Para:, Bitcoin Geleceğin Para Birimi Olabilir Mi? İşletme Ekonomi ve Yönetim Araştırmaları Dergisi, S:1, 2019 https://dergipark.org.tr/download/article-file/620428 (E.T:13.07.2019).

709 **Carter Graydon**, What is Cryptocurrency?, Eylül 2014, https://www.ccn.com/cryptocurrency/ (E.T: 13.07.2019)

710 Çarkacıoğlu, s.9; **Mahmut Yardımcıoğlu/Gamze Şerbetçi,** Bitcoin'in Yapısı ve Yasa Dışı Kullanımı, Al Farabi Sosyal Bilimler Dergisi, C:2, S:4, 2018, s.173 https://dergipark.org.tr/farabi/issue/41933/466512 (E.T:13.07.2019).

711 **Sarah Rotman**, Bitcoin Versus Electronic Money, World Bank Document, 2014,

25 Kasım 2013 tarihinde Bankacılık Düzenleme ve Denetleme Kurumu Bitcoin ile ilgili bir açıklama yapmıştır. Bu açıklamada, bir dijital para olan Bitcoin'in 6493 sayılı "Ödeme ve Menkul Kıymet Mutabakat Sistemleri, Ödeme Hizmetleri ve Elektronik Para Kuruluşları Hakkında Kanun" kapsamında olmadığını ve elektronik para olarak değerlendirilmediği için gözetim ve denetiminin mümkün olmadığını, Bitcoin sisteminde kimliklerin bilinmemesi sebebiyle yasadışı faaliyetlerde kullanılabileceği, dijital cüzdanların çalınabilmesi, kaybolabilmesi, usulsüz kullanılabilmesi ve işlemlerin geri döndürülemez olmasının risklere açık olduğu ifade edilmiştir[712].

Dolayısıyla, kanun kapsamında bir menkul değer olmayan bitcoinlerin bilişim sistemleri aracılığıyla başka bir hesaba aktarılması gibi durumlarda 244'üncü maddenin dördüncü fıkrasında yer alan bilişim sistemi aracılığıyla kendisinin ya da başkasının yararına haksız çıkar sağlama suçu söz konusu olacaktır.

Yine dijital oyun karakterleri ile bu karakterlerin sanal unsurlarının[713] suç konusu olması durumunda uygulanacak hüküm konusunun da değerlendirilmesi gerekmektedir.

Günümüzde online oyunlar, yalnızca vakit geçirme ve eğlence amaçlı kullanılmamakta aynı zamanda bu oyun karakterleri için önemli miktarlarda para harcanarak yine önemli miktarlarda para kazanılması sağlanmaktadır. Özellikle Knight Online, LoL, Metin 2, Dota gibi online strateji ve savaş oyunlarında karakterler ve karakter özellikleri yüksek ücretlerle satılabilmektedir. Ceza hukuku açısından söz konusu sanal nesnelerin hepsi bir veri niteliği taşımaktadır. Dijital oyunlarda karşılaşılan suç tiplerinin büyük çoğunluğu oyuncuların paralarının ve diğer sanal unsurlarının ele geçirilmesi şeklinde gerçekleşmektedir. Dolayısıyla bu unsurların yani verilerin bozulması, yok edilmesi veya

---

https://openknowledge.worldbank.org/bitstream/handle/10986/18418/881640BRI0Box30WLEDGENOTES0Jan02014.pdf?sequence=1&isAllowed=y (E.T:13.07.2019)

712 https://www.bddk.org.tr/ContentBddk/dokuman/duyuru_0512_01.pdf (E.T: 13.07.2019)

713 "İngilizce olan "item" sözcüğünün dilimizdeki karşılığı olan sanal unsur, "madde", "eşya" anlamını taşımaktadır. Dijital oyun dünyasında, oyuncuların sahip oldukları unsurlar item olarak ifade edilmektedir." **Gözde Modoğlu,** Dijital Oyunların Ceza Hukuku ve 5651 Sayılı Kanun Kapsamında Erişim Engelleme Kararları Açısından Değerlendirilmesi, Yayımlanmamış Yüksek Lisans Tezi, İstanbul Bilgi Üniversitesi SBE, İstanbul, 2015, s.5 https://tez.yok.gov.tr/UlusalTezMerkezi/ (E.T: 25.11.2018).

erişilmez kılınması suçtur. Bu eylemler neticesinde failin maddi ya da manevi bir yarar elde etmesi durumunda söz konusu veriler her ne kadar ekonomik değer taşısalar da kanun kapsamında menkul bir değer olmadıklarından TCK'nın 142/2-e maddesi yerine 244'üncü maddenin dördüncü fıkrası uygulanacaktır. Nitekim Yargıtay da vermiş olduğu bir kararda her ne kadar ekonomik değer taşısa da sanal oyun karakterinin veri niteliği taşıdığından hırsızlık suçuna konu olamayacağına bu sebeple suçun 244'üncü maddenin dördüncü fıkrasındaki suçu oluşturacağına karar vermiştir [714].

Dolandırıcılık suçu bakımından içtima hali ise şu şekildedir;

TCK'nın 157'nci maddesinde hileli davranışlarla bir kimseyi aldatıp, onun veya başkasının zararına olarak, kendisine veya başkasına bir yarar sağlama eylemi dolandırıcılık suçu olarak düzenlenmiştir. 158'inci maddede ise bu suçun nitelikli halleri düzenlenmiş olup maddenin birinci fıkrasının (f) bendinde suçun, bilişim sistemlerinin, banka veya kredi kurumlarının araç olarak kullanılması suretiyle işlenmiş olması halinde daha ağır cezaya hükmedileceği ifade edilmiştir.

Bu çerçevede hileli davranışlarla bir kimseyi aldatmak eylemin hareket kısmını; mağdurun veya başkasının zararına olarak, kendisine veya başkasına bir yarar sağlamış olmak ise eylemin netice kısmını oluşturur[715]. Yani suçun oluşması için fesada uğratılmış bir insan iradesinin varlığı gerekmektedir[716].

---

714 **Yargıtay 13. Ceza Dairesi, 06.04.2016 tarihli ve 2015/1926 E., 2016/6115 K. sayılı kararı** http://cankattaskin.av.tr/?p=1603 (E.T:13.07.2019)

715 **Özbek/Doğan/Bacaksız/Tepe**, s.706; **Koca/Üzülmez**, Özel Hükümler, s.703; **Esra Gül Can,** Dolandırıcılık Suçu, Yayımlanmamış Yüksek Lisans Tezi, Çankaya Üniversitesi SBE, Ankara, 2014, s.65 https://tez.yok.gov.tr/UlusalTezMerkezi/ (E.T: 25.11.2018); **Emin Gürsoy,** Bilişim Yoluyla Dolandırıcılık ve Korunma Yöntemleri, Yayımlanmamış Yüksek Lisans Tezi, Afyon Kocatepe Üniversitesi Fen Bilimleri Enstitüsü, Afyon 2015, s.59 https://tez.yok.gov.tr/UlusalTezMerkezi/ (E.T: 25.11.2018).

716 **Erdoğan**, Bilişim Suçları, s.268; **Fırat Tüysüz,** Dolandırıcılık Suçu, Yayımlanmamış Yüksek Lisans Tezi, Başkent Üniversitesi SBE, Ankara 2017, s.87 https://tez.yok.gov.tr/UlusalTezMerkezi/ (E.T: 25.11.2018). Somut olayda; sanığın, katılan Mücahit S'in kimlik bilgilerine göre düzenlenip kendi fotoğrafı yapıştırılmış ele geçirilemeyen sahte nüfus cüzdanını kullanarak katılan A A.Ş.nin Yenigün Şubesi'nde hesap açtırarak diğer katılan Murat Ç'ın bankada bulunan para hesabındaki var olan verileri (bilgileri) sahte kimlikle açtırdığı hesaba internet yoluyla havale edip hesap cüzdanı ibraz ederek banka şubesinden çektiğinin iddia ve kabul olunması karşısında; eyleminin, paranın sanığın açtırdığı hesaba intikaline kadar katılan Murat Ç'a yöneltilmiş hile bulunmaması ve tamamen bilişim sistemi içinde gerçekleştirilmesi nedeniyle 5237 sayılı TCK. nun 244/4 maddesine uyan suçu oluşturduğu gözetilmeden,

Özbek'in bu konu ile ilgili görüşü şu şekildedir;

"Bilindiği üzere dolandırıcılık sucunun islendiğinin kabulü için "hileli davranışların bir kimseyi aldatmış" olması gerekir. Dolayısıyla aldatmaya yönelik hareketler bir "kişi"ye yani bir insana yöneliktir. Halbuki bu nitelikli hal bakımından söz konusu olan dolandırıcılık eyleminin bilişim sistemi üzerinde gerçekleştirilmesidir. Deyim yerinde ise bu durumda "bilgisayar ya da bilişim sistemi" dolandırılmaktadır. Bu halde ise artık m.158 değil, m.244'den söz etmek gerekir. Hukukumuzda bilgisayar dolandırıcılığı olarak da adlandırılabilecek olan düzenleme m.244'tür"[717].

Somut olayda uygulanacak maddenin tespiti bakımından doktrinde genel olarak kabul edilen ayrım burada yarar ile ilişkilidir. Failin bilişim sistemine ya da veriye müdahalesi ile elde ettiği yarar kendiliğinden ortaya çıkıyorsa TCK'nın 244//4'üncü maddesi, yararın ortaya çıkması için bir gerçek kişinin müdahalesi gerekiyorsa TCK'nın 158/1-f maddesi uygulanmalıdır[718]. Bir diğer deyişle bilişim sisteminin bir gerçek kişinin aldatılmasında araç olarak kullanılması 158/1-f maddesi kapsamındayken, hileli davranışların gerçek kişi yerine bilişim sistemine yönelik gerçekleştirilmesi halinde bu nitelikli hal değil 244'üncü maddede düzenlenen suç oluşacaktır[719].

---

vasıflandırılmada yanılgıya düşülerek unsurları oluşmayan banka aracı kılınmak suretiyle nitelikli dolandırıcılık suçundan mahkûmiyet hükmü kurulması bozmayı gerektirmiştir. (Yargıtay 11. Ceza Dairesi, 22.01.2008 tarihli ve 2007/8423 E., 2008/117 K. sayılı kararı) www.lexpera.com (E.T: 07.07.2019)

717 **Özbek,** Banka veya Kredi Kartlarının Kötüye Kullanılması Suçu (TCK m.245), s.1059.

718 **Erdoğan,** Bilişim Suçları, **s**.247.

719 **Ahmet Gökcen/Murat Balcı,** Dolandırıcılık Suçu (m.157-159), Malvarlığına Karşı Suçlar (m.141-169), Adalet Yayınevi Ankara 2018, s.229. Sanığın, olay tarihinde katılan ...'in arkadaşı olan ...'ın e-mail ve buna bağlı oluşturduğu Facebook hesabının şifrelerini kırarak, katılan ... ile ...'mış gibi görüşerek kendi adına kayıtlı cep telefonu hattını vererek cebe havale yolu ile 400 TL para göndermesini istediği, katılanın da görüştüğü kişinin arkadaşı olduğunu düşünerek parayı gönderdiği, bu suretle sanığın bilişim sistemlerinin araç olarak kullanılması suretiyle dolandırıcılık ve bilişim sistemindeki verileri bozma, yok etme, erişilmez kılma, veri değiştirme suçlarını işlediğinin kabul olunduğu olayda; tüm dosya kapsamından sanığın atılı suçu işlediği anlaşıldığından mahkemenin kabul ve uygulamasında bir isabetsizlik görülmemiştir. **Yargıtay 15. Ceza Dairesi, 27.02.2018 tarihli ve 2016/4959 E., 2018/1372 K. sayılı kararı** https://www.lexpera.com.tr/ (E.T: 18.12.2018)
Sanığın, olay tarihinde arkadaşı adına kayıtlı ...Vınn hattından internete girmek suretiyle katılan ...'in email ve buna bağlı oluşturduğu facebook hesabının şifresini kırmak suretiyle katılanın izni ve bilgisi olmaksızın erişim sağladığı ve katılanın erişimini şifresini değiştirerek engellediği, ardından da arkadaş listesinde bulunan şikayetçi ...'dan internet bankacılığı ile para göndermesini istediği, şikayetçi ....'nin şüphelenip katılan ...'ı araması ile hesabının ele geçirildiğini öğrendiği ve parayı göndermediği, bu suretle sanığın bilişim sistemine hukuka aykırı olarak girmek suretiyle verilerin yok edilmesi veya değiştirilmesi ve teşebbüs aşamasında kalan bilişim sistemlerinin araç olarak kullanılması suretiyle dolandırıcılık suçlarını işlediğinin iddia olunduğu olayda; teşebbüs aşamasında kalan bilişim sistemlerinin araç olarak kullanılması suretiyle dolandırıcılık suçunu işlediği anlaşıldığından mahkemenin kabulünde bir isabetsizlik görülmemiştir.

Bilişim sistemlerini etkileyerek, sistemin normal olarak yapması gerekenden farklı sonuçlar üretmesini sağlayan, manipülasyon niteliğindeki hareketler neticesinde haksız çıkar sağlanıyorsa burada 244/4'üncü maddede yer alan bilişim sistemi aracılığıyla haksız çıkar sağlama suçu oluşacaktır. Gerçekleştirilen hile sonucunda aldatılan kişinin tasarrufta bulunmasının dolandırıcılık suçunu oluşturması gibi, bilişim sistemlerinin hataya düşürülerek işlem yapmasının sağlanması da alan bilişim sistemi aracılığıyla haksız çıkar sağlama suçunu oluşturacaktır[720]. Yargıtay da vermiş olduğu kararlarda insana yönelik hilenin bulunduğu durumlarda dolandırıcılık suçunun gerçekleştirildiğini, sadece bilişim sisteminin kullanılması suretiyle çıkar sağlandığı durumlarda ise bilişim sistemi aracılığıyla haksız çıkar sağlama suçunun oluştuğunu kabul etmektedir[721].

Bilişim sistemine girme ve engellenme suçundan verilen beraat hükmüne yönelik o yer Cumhuriyet Savcısının temyiz talebinin incelenmesinde; Sanığın katılan ...'in hesaplarının şifresini ele geçirip, ardından şifreleri değiştimesi şeklindeki eylemi ile şikayetçi ...'dan para istemesi eyleminin iki ayrı suçu oluşturması karşısında; TCK'nın 44. maddesinin uygulanma imkanının bulunmadığı, ayrıca iddia makamının talep ettiği kanun maddesinin sanık için kazanılmış hak oluşturmayacağı da gözönüne alındığında, tebilğnamedeki TCK'nın 243/1 maddesi gereğince bozma isteyen düşünceye iştirik edilmemiş olup, sanığın katılan ...'in e posta adresinin ve facebook hesabının şifresini kırması, ardından da şifreyi değiştirmesi şeklindeki eyleminden dolayı TCK'nın 244/2 maddesinde düzenlenen bilişim sistemindeki verileri bozma yoketme, erişilmez kılma, sisteme veri yerleştirme suçundan da mahkumiyet kararı verilmesi gerekirken yazılı şekilde hüküm kurulması bozmayı gerektirmiştir. **Yargıtay 15. Ceza Dairesi, 17.04.2018 tarihli ve 2017/31912 E., 2018/2652 K. sayılı kararı** https://www.lexpera.com.tr/ (E.T: 18.12.2018)

"Bilişim sistemlerinin aynı anda birçok kişiye ulaşmasındaki çabukluk ve sağladığı kolaylığa dayanarak "www.sahibinden.com" adlı internet sitesinde emsallerine göre fiyatını da ucuz göstererek araç satışı için ilan veren sanığın, bu ilanı görüp kendisini telefonla arayan şikayetçiden kapora adı altında 250 Lira alması şeklinde gerçekleşen olayda; sanığın bilişim sistemini araç olarak kullanmak suretiyle suçu işlediği anlaşılmakla, eylemin TCK'nun 158. maddesinin 1. fıkrasının (f) bendinde düzenlenmiş olan nitelikli dolandırıcılık suçunu oluşturduğu kabul edilmelidir." **Yargıtay Ceza Genel Kurulu, 11.06.2013 tarihli ve 2013/15-239 E., 2013/289 K. sayılı kararı** https://www.lexpera.com.tr/ (E.T: 18.12.2018)

720 Yargıtay, sanığın, katılan şirkete ait ....Mağazasında bilgisayar sorumlusu olarak çalıştığı, şubelerde yapılan satışların yine şubelerde bulunan bilgisayar vasıtasıyla, şirket merkezindeki server üzerinde bulunan veritabanına işlendiği ve bu işlem sonunda merkezdeki programdan şubelerdeki günlük satış ve stok miktarının takip edildiği, yapılan kayıtların merkezde görevli "...." isimli kullanıcı olan sanık tarafından bilişim sisteminin işleyişi değiştirilerek sisteme gerçeğe aykırı veri yerleştirmek suretiyle haksız çıkar sağlandığı, haksız yararın doğrudan katılana yönelik hileli davranışlarla gerçekleşmemesi karşısında eylemin dolandırıcılık olarak nitelendirilemeyeceği gibi, katılan tarafından sanığın zilyetliğine devredilmiş bir mal bulunmaması karşısında eylemin güveni kötüye kullanma suçunu da oluşturmayacağı belirlenmiş olmakla sanığa yüklenen eylemin TCK'nın 244/4. maddesinde düzenlenen bilişim sistemini aracı kılarak yarar sağlama suçunu oluşturduğu gözetilmeden, suç vasfında hataya düşülerek yazılı şekilde hüküm kurulmasını bozma sebebi olduğu yönünde karar vermiştir**. (Yargıtay 23. Ceza Dairesi, 14.12.2015 tarihli ve 2015/4528 E., 2015/8082 K. sayılı kararı)** www.lexpera.com (E.T:10.07.2019)

721 **Akbulut,** Bilişim Alanında Suçlar, s.256; **Çetin Yılmaz,** Türk Ceza Hukukunda Dolandırıcılık Suçu, Yayımlanmamış Yüksek Lisans Tezi, Çankaya Üniversitesi SBE, Ankara 2018, s.60 https://tez.yok.gov.tr/UlusalTezMerkezi/ (E.T: 25.11.2018). Yargıtay bu konuda vermiş olduğu kararlarda, "*Gerçek bir kişiyle karşı karşıya gelmeden, yüz yüze veya telefon, bilgisayar, bilgi geçer gibi bir başka vasıta kullanılarak görüşmeden, konuşmadan, hileli davranışlarla gerçek kişiler dolandırılmadan sadece bilişim sistemi kullanılarak doğrudan doğruya çıkar sağlanması halinde 'bilişim sistemine girerek haksız çıkar sağlama suçu'*

Bu suçun 245'inci maddede yer alan banka veya kredi kartlarının kötüye kullanılması suçu ile içtimaının da değerlendirilmesi gerekmektedir. 245'inci madde kapsamında yer alan banka ve kredi kartları dışında manyetik bantlı ya da chipli kartların kullanımı neticesinde haksız yarar elde etme durumuna ilişkin bir belirleme yapmamıştır.

Yargıtay, vermiş olduğu bir kararda, kredisi bitmiş manyetik telefon kartları üzerinde yapmış olduğu değişikliklerle, sistemin verileri farklı algılamasını sağladığı veya başka bir deyişle sisteme farklı veri yüklediği olayda 244'üncü maddenin dördüncü fıkrasının oluştuğunu kabul etmiştir[722]. Yine online bankacılık işlemlerinde, kişi sisteme şifre aracılığıyla girdiğinden, kişinin müşteri numarası öğrenme, sistemin güvenlik duvarının aşılması gibi yollarla sisteme girip sistemdeki verileri değiştirerek haksız yarar sağlama eylemi 244'üncü maddenin dördüncü fıkrasında yer alan suçu oluşturmaktadır.

TCK'nın 245/A maddesinde, 244'üncü maddede yer alan suçların işlenmesi için bir cihazın, bilgisayar programının, şifrenin veya sair güvenlik kodunun 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 kişinin cezalandırılacağı öngörülmüştür. Bu durumda fail bu eylemleri gerçekleştirdikten sonra, 244/4'üncü maddede yer alan suçu da işlemişse bu durumda gerçek içtima hükümleri uygulanacak ve fail her iki suçtan dolayı da cezalandırılacaktır[723].

E. KUSURLULUK

Daha önce de ifade etmiş olduğumuz gibi, kusurluluk, kişinin işlediği fiil dolayısıyla kınanabilmesini, haksızlık teşkil eden eylemin kişiye yüklenebilmesini ifade etmektedir[724]. Bilişimi aracılığıyla kendisinin ya da başkasının yararına haksız çıkar sağlama suçu

---

gerçekleşecektir." şeklinde hüküm kurmuştur. (Yargıtay 11. Ceza Dairesi, 12.10.2009 tarihli ve 2008/11060 E., 2009/11936 K. sayılı kararı) https://www.lexpera.com.tr/ (E.T: 18.12.2018)

722 Yargıtay Ceza Genel Kurulu, 19.06.2007 tarihli ve 2007/6-136 E., 2007/150 K. sayılı kararı www.lexpera.com (E.T:10.07.2019)

723 **Akbulut,** Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme, s.47.

724 **Artuk/Gökcen/Alşahin/Çakır**, Genel Hükümler, s.569.

bakımından da somut olaya göre kusurluluğu kaldıran veya azaltan haller söz konusu olabilir[725]. Örneğin, sisteme veri kaydetmekle sorumlu kişi cebir veya tehdit ile yanlış veri girmeye zorlanarak başkasının yararına haksız çıkar sağlanabilir. Bu ve benzeri kusurluluğu azaltan veya ortadan kaldıran durumlarda kişiye verilecek ceza bu durumlar göz önünde bulundurularak belirlenecektir.

F. SORUŞTURMA USULÜ, GÖREVLİ VE YETKİLİ MAHKEME, YAPTIRIM, ZAMAN AŞIMI

TCK m.244'ün dördüncü fıkrasında bu suçun cezası olarak iki yıldan altı yıla kadar hapis cezası ve beş bin güne kadar adli para cezası öngörülmüştür.

Adli para cezası, TCK m. 52/1'de "*Adlî para cezası, beş günden az ve kanunda aksine hüküm bulunmayan hallerde yediyüzotuz günden fazla olmamak üzere belirlenen tam gün sayısının, bir gün karşılığı olarak takdir edilen miktar ile çarpılması suretiyle hesaplanan meblağın hükümlü tarafından Devlet Hazinesine ödenmesinden ibarettir.*" şeklinde düzenlenmiştir. Yine maddenin devamında bir gün karşılığının en az yirmi ve en fazla yüz Türk Lirası şeklinde takdir edilebileceği belirtilmiştir. Bu miktar, kişinin ekonomik ve diğer şahsi halleri dikkate alınarak belirlenecektir. Gün sayısı ise TCK m. 61'de yer alan ölçütlere göre belirlenecektir. Madde metninde öngörülen ceza seçimlik olmadığından adli para cezasının ve hürriyeti bağlayıcı cezanın beraber tayin edilmesi gerekmektedir[726]. Yine şartlarının bulunması halinde ceza tayininde TCK'nın 62'nci maddesi gereğince takdiri indirim yapılması mümkündür

---

725 Kusurluluğu azaltan veya ortadan kaldıran hallere ilişkin yaptığımız açıklamalar için bkz. s.105.

726 "Kabule göre de; TCK'nın 244/4. maddesinde hapis cezası ile birlikte adli para cezasının da düzenlendiği ve birlikte hükmedilmesi gerektiği gözetilmeden sadece hapis cezasına hükmedilmesi bozmayı gerektirmiştir." **Yargıtay 2. Ceza Dairesi, 30.05.2017 tarihli ve 2014/37954 E., 2017/6242 K. sayılı kararı** https://www.lexpera.com.tr/ (E.T:18.12.2018)

TCK m. 246 gereğince lehine yarar sağlanan, bir tüzel kişi ise güvenlik tedbirleri uygulanabilecektir. Tüzel kişiler hakkında uygulanabilecek güvenlik tedbirleri ise TCK m.60'a göre faaliyet izninin iptali ve müsaderedir.

TCK m.66'ya göre 244. maddenin dördüncü fıkrasında düzenlenen bilişim sistemi aracılığıyla çıkar sağlama suçunun cezasının üst sınırı 6 yıl hapis cezası olarak belirlendiğinden 15 yıllık dava zamanaşımına tabi olacaktır.

Bilişim sistemleri aracılığıyla çıkar sağlama suçu, resen soruşturulan ve kovuşturulan bir suç olup şikâyete bağlı değildir.

5235 sayılı Adli Yargı İlk Derece Mahkemeleri ile Bölge Adliye Mahkemelerinin Kuruluş, Görev ve Yetkileri Hakkında Kanun'un 10, 11 ile 12. maddelerine göre bu suç için görevli mahkeme Asliye Ceza Mahkemeleridir

SONUÇ

Tarihin bütün dönemlerinde, daha fazla ve nitelikli bilgiye sahip olan ve elde ettiği bu bilgiyi doğru bir şekilde kullanan toplumlar, her alanda diğer toplumların önünde, güç ve zenginliğin sahibi olmuşlardır.

20'nci yüzyılın ortalarından beri bu güç ve zenginliğe, sağlık, eğitim vb. tüm siyasi, ekonomik ve sosyal alanlarda teknolojik gelişmeleri takip eden ve bu gelişmelere öncülük eden toplumlar sahip olmuştur. 21'inci yüzyılda toplumlar, teknolojiyi hayatın her alanında kullanmaya başlamış ve bilgi toplumuna dönüşüm süreci başlatmışlardır. Ülkemizde de 1990'lı yılların ikinci yarısından sonra bilgi toplumuna geçişe yönelik strateji planları yapılmaya başlanmış, bilişim sistemleri ve internet kullanımı yaygınlaştırılmaya çalışılmıştır. Yine bu kapsamda "e-Dönüşüm Türkiye" projesi oluşturulmuş ve kamusal hizmetlerin elektronik ortama taşınmasına yönelik çalışmalar başlatılmıştır. "E-Devlet", "UYAP", "TAKBİS", "MERSİS" gibi programlarla, bilgi toplumuna yönelik, yeni bir kurumsal yapı oluşturulmaya çalışılmıştır. Bu süreçte her türlü kişisel ve kurumsal bilgiler bilişim sistemlerinde saklanmaya başlanmış ve sisteme girilen her bir bilgi veri niteliği kazanmıştır.

Bütün bu gelişmeler sosyal, ekonomik ve siyasi alanlarda hızla gelişimlere sebep olurken aynı zamanda her türlü kişisel ve kurumsal bilginin bilişim sistemlerinde tutulması, sistemlerle etkileşim halinde olan kişilerin bunları bilinçli bir şekilde kullanamaması, bu alanda suç işlemenin kolay olması, işlenen suçun etkisinin fazla olması, faillerin anonim profillere sahip olması ve bunların tespitindeki zorluklar, bu sistemlerin kötü niyetli kullanımına sebep olmuş ve yeni suç tipleri ortaya çıkmıştır. Bu şekilde ortaya çıkan yeni suç tipleri ve bunların sürekli değişen işleniş yöntemleri, suçun sınırlar aşan niteliği, suçluların teknik bilgileri, ulusal ve uluslararası alanda bilişim suçlarına ilişkin olarak kurumlar arası adli iş birliğinde aksaklıkların yaşanması, klasik soruşturma yöntemlerinin bu alanda işlenen suçlar için yetersiz kalması, bilişim suçları ile mücadele yöntemleri için

gerekli yatırımların yapılmaması gibi nedenlerle bu suçlarla mücadelede zorluk yaşanmaktadır.

Bireylerin, toplumun ve devletin sistem üzerinde kaydedilen verilerinin ve verilerin gizliliğinin korunması, bunların girildiği sistemlerin güvenliği için saldırılara karşı dayanıklı güvenlik duvarları bulunan bilişim sistemlerinin oluşturulması ve hem bireysel hem de kurumsal bazda bilişim sistemlerinin güvenli kullanımı konusunda bilinçlendirme çalışmaları yapılması gerekmektedir.

Teknolojideki hızlı değişimler ve gelişimler ile bu alanda işlenen suçların sınır tanımaz niteliği, kanuni düzenlemelerin de kısa sürede yetersiz kalmasına neden olmaktadır. Bu sebeple, bilişim hukuku alanında uluslararası iş birliğine dayanan, etkin bir ceza politikasının oluşturulması gerekmektedir. Her ne kadar Sanal Ortamda İşlenen Suçlar Sözleşmesi'nde, uluslararası adli yardımlaşma ilkeleri benimsenmiş olsa da bu sözleşmenin bağlayıcılığının olmaması sebebiyle uygulamada sorunlar çıkmaktadır. Bunun yanı sıra mevcut düzenlemede yer alan cezaların caydırıcılığının da artırılması gerekmektedir. TCK'nın 244'üncü maddesinde yer alan suçlara ilişkin yaptırımlar, suçların düzenlenmesi ile amaçlanan yararlara hizmet etmekten uzaktır. Bilişim sistemindeki verileri bozma, yok etme, değiştirme, erişilmez kılma, sisteme veri yerleştirme ve var olan verileri başka bir yere gönderme suçuna ilişkin yaptırımın alt sınırının altı ay hapis cezasından başlaması ve uygulamada cezaların genellikle alt sınıra yakın bir şekilde verilmesi, bu derece önemli bir suçun cezasız kalmasına neden olabilecek niteliktedir.

Hakim, savcı ve kolluk görevlilerinin bilişim suçlarına ilişkin araştırma ve soruşturma yöntemlerine hakim olmaması, bu alanda uzman olmamaları, soruşturma ve kovuşturmanın sağlıksız bir şekilde tamamlanmasına ve bazen gerçek suçlunun cezasız kalmasına ve bazı hak ihlallerine neden olabilmektedir. Bunun çözümü, bu alanda görev yapan hakim, savcı ve kolluk görevlilerinin bilişim alanında hukuki ve teknik konularda uzmanlaşmasını sağlamak, bilgilerini sürekli güncel tutmak ve bilişim suçlarına özgü ihtisas mahkemeleri oluşturmaktır.

TCK'nın 244'üncü maddesinde yer alan sistemi engelleme, bozma, verileri yok etme veya değiştirme suçlarının yapısı itibariyle delil tespitinin, soruşturmanın ve yargılamanın hızlı bir şekilde tamamlanması gerekmektedir. Bu da klasik soruşturma yöntemlerinin dışına çıkılması ve hem soruşturma hem de kovuşturmaya ilişkin kanuni bir düzenleme yapılması ile gerçekleşecektir.

TCK'nın 244'üncü maddesinde düzenlenen suçlarla ilgili bir diğer önemli sorun da diğer suçlarla özellikle hırsızlık ve dolandırıcılık suçlarının nitelikli halleriyle içtimaı halinde uygulanacak maddenin belirlenmesi konusudur. Maddelerin ve madde gerekçelerinin açık bir şekilde olmaması ve çelişkiler barındırması, uygulanacak maddenin belirlenmesini zorlaştırmaktadır. Bu çelişkilerin giderilmesi ve maddelerin yeniden düzenlenmesi gerekmektedir. TCK'nın 244'üncü maddesinin dördüncü fıkrasında eylemin başka bir suç oluşturmaması halinde bu hükmün uygulanabileceği düzenlenmişken, madde gerekçesinde fiilin, daha ağır cezayı gerektiren başka bir suç oluşturmaması halinde uygulanabileceği düzenlenmiştir. Bu fıkranın da içtima kuralları gereğince, gerekçede yer alan şekilde yeniden düzenlenmesi gerekmektedir.

Bu önlemler, teknolojinin ve bilişim sistemlerinin daha verimli ve daha güvenli bir şekilde kullanılmasına katkı sağlayacak ve bu alanda işlenen suçlarla mücadeleyi güçlendirecektir.

KAYNAKÇA

ADALI Eşref, "İnternet Suçları", Bilişim ve İnternet Teknolojilerinin Ceza Hukuku Açısından Doğurduğu Yeni Sorunlar Konferansı Konuşma Metni, Bursa, İçişleri Bakanlığı Yayını, 2001.

ALACA Bahaddin, "Ülkemizde Bilişim Suçları ve İnternetin Suça Etkisi (Antropolojik ve Hukuki Boyutları ile)", Ankara Üniversitesi SBE, Yayımlanmamış Yüksek Lisans Tezi, Ankara, 2008.

ALİUSTA Cahit/BENZER Recep, "Avrupa Siber Suçlar Sözleşmesi ve Türkiye'nin Dahil Olma Süreci", Uluslararası Bilgi Güvenliği Mühendisliği Dergisi, C:4, S:2, 2018.

ALP Barış Emre, "5237 Sayılı Türk Ceza Kanunu'nda Bilişim Sistemini Engelleme, Bozma, Verileri Yok Etme veya Değiştirme Suçu", Yayımlanmamış Yüksek Lisans Tezi, Çankaya Üniversitesi SBE, Ankara, 2018.

ALTUNOK Ebru/VURAL A. Fatih, "Bilişim Suçları" (Çevrimiçi Yayın)
AKARSLAN Hüseyin, "Bilişim Suçları"**,** 1. Baskı, Seçkin Yayıncılık, Ankara, 2015.

AKBULUT Berrrin, "Ceza Hukuku Genel Hükümler"**,** 4. Baskı, Adalet Yayınevi, Ankara, 2017.

AKBULUT Berrrin, "Bilişim Alanında Suçlar", 2. Bası, Adalet Yayınevi, Ankara, 2017.

AKBULUT Berrrin, "Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme", Selçuk Üniversitesi Hukuk Fakültesi Dergisi, C:24, S:2, 2016.

AKBULUT Berrrin Bozdoğan, "Bilişim Suçları", Selçuk Üniversitesi Hukuk Fakültesi Dergisi Milenyum Armağanı, Konya, C.8, S:1-2, 2000.

AKBULUT Berrrin Bozdoğan, "Bilişim Suçları", Kemal Oğuzman'a Armağan, İstanbul, Galatasaray Üniversitesi Yayınları, 2004,

AKGÜL Mustafa, "İnternet Yasakları ve Hukuk", Türkiye Barolar Birliği Dergisi, Yıl:21, Sayı:78, Eylül-Ekim 2008.

AKPEK Nusret Onur, Siber Suçlar Sözleşmesinin Getirdikleri ve İç Hukuk Açısından Konuya Yaklaşım, Yayımlanmamış Yüksek Lisans Tezi, İstanbul Bilgi Üniversitesi SBE, İstanbul, 2015.

ALİUSTA Cahit – BENZER Recep, "Avrupa Siber Suçlar Sözleşmesi ve Türkiye'nin Dahil Olma Süreci", Uluslararası Bilgi Güvenliği Mühendisliği Dergisi, C:4, S:2, 2018.

ALTUNOK Ebru / VURAL Fatih, Bilişim Suçları, Denetişim Dergisi, S:8, 2011.

APAYDIN Cengiz, "Bilişim Suçları ve Bilişim Ceza Hukuku", 1. Basım, İstanbul, Acar Matbaacılık, 2017.

APAYDIN Cengiz, "Başkalarına Ait Banka Hesaplarıyla İlişkilendirerek Sahte Banka veya Kredi Kartını Üretmek, Satmak, Devretmek, Satın almak veya Kabul Etmek", Terazi Hukuk Dergisi, C:12, S:127, 2017

APİŞ Özge, "Bilişim Sistemine Girme Suçu Bakımından Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama Kopyalama Elkoyma Koruma Tedbiri", Yasama Dergisi, C:12, S:37, 2018.

ARTUK Mehmet Emin/GÖKCEN Ahmet/ALŞAHİN M. Emin / ÇAKIR Kerim, "Ceza Hukuku Genel Hükümler", 13. Baskı, Ankara 2019.

ARTUK Mehmet Emin/GÖKCEN Ahmet/YENİDÜNYA Ahmet Caner, "Türk Ceza Kanunu Şerhi", 5. Cilt, Ankara, Turhan Kitapevi, 2009.

ARTUK Mehmet Emin/GÖKCEN Ahmet/YENİDÜNYA Ahmet Caner, "Ceza Hukuku Özel Hükümler", 11.Basım, Ankara, Turhan Kitapevi, 2011

AVŞAR B.Zakir/ ÖNGÖREN Gürsel, "Bilişim Hukuku", İstanbul, Türkiye Bankalar Birliği Yayınları, Yayın No:270, 2010.

AYDIN Emin Doğan, "Bilişim Suçları ve Hukukuna Giriş", 1. Baskı, Ankara, Doruk Yayınları, 1992.

AYDIN Emin Doğan, "Bilişim Sistemlerinde, Güvenlik, Güvenirlik, Mahremiyet ve Bilişim Suçları", Marmara İletişim Dergisi, 1992.

AYDIN Devrim, "Türk Ceza Hukukunda İştirak, (Yayımlanmamış Doktora Tezi)", Ankara Üniversitesi SBE, Ankara, 2008 .

BAĞCI Hasan, Sosyal Mühendislik ve Denetim, Denetişim Dergisi, S:1, 2009. (Çevrimiçi Yayın)

BAŞ Eylem, "Banka ve Kredi Kartlarının Kötüye Kullanılması", (Yayınlanmamış Yüksek Lisans Tezi) Ankara Üniversitesi SBE, Ankara, 2011.

BAŞBÜYÜK İsa, "Hırsızlık ve Dolandırıcılık Suçlarının Bilişim Sistemlerinin Araç Olarak Kullanılması Suretiyle İşlenmesi", Ceza Hukuku Dergisi, Aralık 2010, Sayı:4.

BATI Kutay, Bulut Bilişim ve Etkileri, Yayımlanmamış Yüksek Lisans Tezi, Dokuz Eylül Üniversitesi SBE, İzmir, 2015.

BATIR Uğur, "E- Devlet Uygulamalarından Adalet Bakanlığı Ulusal Yargı Ağı Bilişim Sistemi Portalı (UYAP)'ın Etkinliğini Belirlemeye Yönelik Ankara Barosu Avukatları Üzerine Bir Alan Araştırması", Yayımlanmamış Yüksek Lisans Tezi, Gazi Üniversitesi Eğitim Bilimleri Enstitüsü, Ankara, 2013.

BECENİ Yasin, "Türk Hukuk'undaki Bilişim Suçlarının Tasnif Şekilleri", Ankara Barosu Hukuk Kurultayı 2006, Bilişim ve Hukuk Yargılama Hukuku, Cilt:4, Ankara, Ustaoğlu, Basım Yayın Ltd.Ştd., 2006.

BİÇKİN İnci, "Siber Suç Sözleşmesi ve 5237 s. Türk Ceza Kanununda Bilişim Suçları", Yargıtay Dergisi, Cilt:32, Ocak-Nisan 2006, Sayı:1-2.

BİLEK Burak Tunç, "Bilişim Suçları ve Üniversite Lisans Öğrencilerinin Bilişim Suçlarına Yönelik Görüşleri", Yayımlanmamış Yüksek Lisans Tez**i,** Gazi Üniversitesi SBE, Ankara, 2012.

BUDAK Mesut, "Banka ve Kredi Kartlarının Kötüye Kullanılması Suçu", Yayınlanmamış Yüksek Lisans Tezi, Polis Akademisi Başkanlığı Güvenlik Bilimleri Enstitüsü, 2009.

CAN Esra Gül, Dolandırıcılık Suçu, Yayımlanmamış Yüksek Lisans Tezi, Çankaya Üniversitesi SBE, Ankara, 2014

CENTEL Nur / ZAFER Hamide / ÇAKMUT Özlem, "Türk Ceza Hukukuna Giriş", 10. Baskı, Ankara 2017, s .170.

ÇAKICI Mert, "Türk Ceza Kanunu m.243 ve m.244'te Düzenlenen Bilişim Suçları", Ceza Hukuku Dergisi, C: 9, S: 24, 2014.

ÇARKACIOĞLU Abdurrahman, Kripto-Para Bitcoin, Sermaye Piyasası Kurulu Araştırma Dairesi, Ankara 2016. (Çevrimiçi Yayın)

ÇEKİÇ Burak, "İnternet Aracılığıyla İşlenen Suçlar", Yayınlanmamış Yüksek Lisans Tezi, Marmara Üniversitesi SBE, İstanbul, 2006.

ÇİÇEK İlker, Ülkemizde Adli Bilişim Laboratuarı Kurulumu ve Bilişim Suçlarıyla Mücadeleye Katkıları, Yayımlanmamış Yüksek Lisans Tezi, Haliç Üniversitesi FBE, İstanbul, 2008.

DEĞİRMENCİ Olgun, "2004 Türk Ceza Kanunu'nun Bilişim Suçları Bakımından Değerlendirilmesi", Türkiye Barolar Birliği Dergisi, Yıl:18, sayı58, Mayıs-Haziran 2005.

DEĞİRMENCİ Olgun, "Bilişim Suçları**"**, Yayınlanmamış Yüksek Lisans Tezi, Marmara Üniversitesi SBE, İstanbul, 2002.

DEĞİRMENCİ Olgun, "Bilişim Suçları Alanında Yapılan Çalışmalar ve Bu Suçların Mukayeseli Hukukta Düzenlenişi", Legal Hukuk Dergisi, S:11, 2003.

DEMİRBAŞ Timur, "Ceza Hukuku Genel Hükümler", 12. Baskı, Seçkin Yayınevi, Ankara, 2017.

DEMİRCAN Tunç, "Yeni ve Eski TCK Bağlamında Bilişim Alanında Suçlar", Legal Yayıncılık, İstanbul, 2016.

DEMİROĞLU Abdullah Taner, "Stratejik İstihbaratın Önemi: Bilişim Suçları Uygulaması", Yayımlanmamış Yüksek Lisans Tezi, Polis Akademisi Güvenlik Bilimleri Enstitüsü, Ankara, 2015.

DİLEK Halil İbrahim, "Bilişim Suçları ve Türk Hukuk Sistemindeki Yeri", Dicle Üniversitesi SBE, Yayımlanmamış Yüksek Lisans Tezi, Diyarbakır, 2006.

DİJLE Hikmet, "Türkiye'de Eğitimli İnsanların Bilişim Suçlarına Yaklaşımı", Yayınlanmamış Yüksek Lisans Tezi, Gazi Üniversitesi Fen Bilimleri Enstitüsü, Ankara, 2006.

DOĞAN Koray, "Bilişim Suçları ve Yeni Türk Ceza Kanunu", Hukuk ve Adalet Eleştirel Hukuk Dergisi, Y:2 S:6-7, 2005.

DÖNMEZER Sulhi, "Kişilere ve Mala Karşı Cürümler", Tıpkı 17. Baskı, İstanbul, Beta Yayıncılık, 2004.

DÖNMEZER Sulhi/ERMAN Sahir, "Nazari ve Tatbiki Ceza Hukuku, Genel Kısım", C.2, 11. Baskı, İstanbul, Beta Yayınevi, 1997.

DURDU Ali, "Türk Silahlı Kuvvetleri Personelinin Bilişim Suçlarına Yönelik Yaklaşımı (Gaziantep İli Örneği)", Yayımlanmamış Yüksek Lisans Tezi, Gaziantep Üniversitesi SBE, Gaziantep, 2015.

DURSUN Eser, "Sosyal Medya Aracılığıyla İşlenen Suçlar (Geniş Anlamda Bilişim Suçları)", Ceza Hukuku Dergisi, C:9, S:24, 2014.

DÜLGER Murat Volkan, "Bilişim Suçları ve İnternet İletişim Hukuku", 7. Baskı, Ankara, Seçkin Yayınevi, 2018.

EFE Ahmet / OMAK Isamettin, Security Considerations Regarding Terms And Conditions of Cloud Service Providers, İleri Teknoloji Bilimleri Dergisi, C:8, S:1, 2019.

EKER Ö. Umut, "Türk Ceza Hukuku'nda Bilişim Suçları Eski TCK Bağlamında Hukukumuzda Yer Alan İlk Düzenlemeler ve 5237 s. Yeni Türk Ceza Kanunu'nun İlgili Hükümlerinin Yorumu", Türkiye Barolar Birliği, Yıl:19, Sayı: 62, Ocak-Şubat 2006.

EKİM Ahmet, "Bilişim Suçlarında Sayısal Delillerin Toplanması, Muhafaza Edilmesi, İncelenmesi ve Raporlanması", Yayımlanmamış Yüksek Lisans Tezi, Marmara Üniversitesi SBE, İstanbul, 2013.

EMEKÇİ Adem / KUĞU Emin / TEMİZTÜRK Murtaza, Adli Bilişim Ezberlerini Bozan Bir Düzlem: Bulut Bilişim, Uluslararası Bilgi Güvenliği Mühendisliği Dergisi, C:2, S:1, 2016.

ERALP Özgür, "Hukukçular İçin Bilişim Terimleri Sözlüğü", Ankara, Avbil Yayınları, 2007.

ERDAĞ Ali İhsan, "Bilişim Alanında Suçlar (Türk ve Alman Ceza Hukukunda)" Gazi Üniversitesi Hukuk Fakültesi Dergisi C.14, Y. 2010 S.2.

ERDEM Merve/ÖZOCAK Gürkan, "Avrupa Konseyi Siber Suç Sözleşmesi ve Türk Hukukuna Etkileri" (Çevrimiçi Yayın).

ERDOĞAN Yavuz, "Türk Ceza Kanunu'nda Bilişim Suçları (Avrupa Konseyi Siber Suç Sözleşmesi ve Yargıtay Kararları İle)", Legal Yayınları, 2012.

ERDOĞAN Yavuz, "Türk Ceza Kanunu'nda Banka ve Kredi Kartlarının Kötüye Kullanılması Suçu", Legal Hukuk Dergisi, C:9, S:107, 2011.

ERDOĞAN Yavuz, "Bilişim Sistemine Girme ve Kalma Suçu", Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi, C:12 Özel S., 2010.

EREM Faruk, "Bilgisayar Suçları ve Türk Ceza Kanunu" (Çevrimiçi Yayın).

ERGÜÇ Seher, "Türk Bankacılık Sisteminde İnternet Bankacılığı İle Yapılan Dolandırıcılıklar ve Bilişim Suçları Hukuku", Yayımlanmamış Yüksek Lisans Tezi, Kadir Has Üniversitesi SBE, İstanbul, 2008.

ERGÜN İsmail, "Siber Suçların Cezalandırılması ve Türkiye'de Durum", Ankara, Adalet Yayınevi, 2008.

ERMAN Ragıp Barış, "Yanılmanın Ceza Sorumluluğuna Etkisi", Yayımlanmamış Doktora Tezi, İstanbul Üniversitesi SBE, İstanbul, 2006.

ERMEYDAN Damla, "Türk Ceza Kanunu'nda Bilişim Suçları", Yayımlanmamış Yüksek Lisans Tezi, Çağ Üniversitesi SBE, Mersin, 2018.

ERSOY Yüksel, "Genel Hukuki Koruma Çerçevesinde Bilişim Suçları", Prof.Dr Yılmaz GÜNAL'a Armağan, Ankara Üniversitesi Siyasal Bilgiler Fakültesi Yayını, Cilt:49, No:3-4, 1994.

ESEN Sinan, "Malvarlığına Karşı Suçlar, Belgelerde Sahtecilik ve Bilişim Alanındaki Suçlar", Ankara, Adalet Yayınevi, 2007.

FERT İsmail, "İnternet Kafeler Üzerinden Gerçekleştirilen Bilişim Suçları", Adli Psikiyatri Dergisi, C:2, S:1, 2005.

GEDİKLİ Cüneyt/GÜVEN Gökhan/TORUN Talip, "Bilgisayar Teknolojileri ve İnternet", Ankara, Detay Yayıncılık, 2004.

GÖKCEN Ahmet, "Belgede Sahtecilik Suçları (m.204-212)", 4. Baskı, Ankara, Adalet Yayınevi, 2016.

GÖKCEN Ahmet / ERDİN Selim / ŞENERDOĞAN Büşra, Hırsızlık Suçu (m.141), Malvarlığına Karşı Suçlar (m.141-169), Adalet Yayınevi, Ankara 2018.

GÖKCEN Ahmet / BALCI Murat, Dolandırıcılık Suçu (m.157-159), Malvarlığına Karşı Suçlar (m.141-169), Adalet Yayınevi Ankara 2018.

GÖKTÜRK Neslihan, "Türk Hukuku'nda Suçların İçtiması", Ceza Hukuku ve Kriminoloji Dergisi, C.2, S:1-2, 2014,

GÖNEN Serkan/ULUS Halil İbrahim/YILMAZ Ercan Nurcan, "Bilişim Alanında İşlenen Suçlar Üzerine Bir İnceleme", Bilişim Teknolojileri Dergisi, C:9, S:3, 2016.

GÖZÜŞİRİN Mesih, "5237 Sayılı Türk Ceza Kanununda Bilişim Suçları ve Bilişim Suçları ile Mücadeleye İlişkin Model Önerisi", Kara Harp Okulu Savunma Bilimleri Enstitüsü, Ankara, 2011.

GÜL Ahmet, "Doğrudan / Dolaylı Bilişim Suçları", 1. Baskı, Seçkin Yayınevi, Ankara, 2016.

GÜLER Dilek, "Bilişim Sistemine Girme Suçu", KTO Karatay Üniversitesi Hukuk Fakültesi Dergisi, C:3, S:2, 2018.

GÜLTEKİN Nil Melek, Kişisel Verilerin Ceza Hukuku Yönünden Korunması, Yayımlanmamış Yüksek Lisans Tezi, Galatasaray Üniversitesi SBE, İstanbul, 2012.

GÜLTEKİN Nurbay, "Bilgisayara Giriş Basic Programlama", 1. Baskı, Karadeniz Teknik Üniversitesi Yayınları, Trabzon, 1989.

GÜNDÜZ M. Zekeriya, "Bilişim Suçlarına Yönelik IP Tabanlı Delil Tespiti", Yayımlanmamış Yüksek Lisans Tezi, Fırat Üniversitesi FBE, Elazığ, 2013.

GÜNEŞ Alper, "Bilişim Suçları ve İdarenin Hukuki Sorumluluğu", Yayımlanmamış Yüksek Lisans Tezi, Selçuk Üniversitesi SBE, Konya, 2015.

GÜNGÖR Necmi Murat, "Yeni Türk Ceza Kanunu Kapsamında Bilişim Suçları ve Emniyet Genel Müdürlüğü Uygulamaları", Yayımlanmamış Yüksek Lisans Tezi, İstanbul Üniversitesi SBE, İstanbul, 2007.

GÜMÜŞ Çetin, "Bilişim Suçlarıyla Mücadelede Polisin Eğitimi", Yayımlanmamış Doktora Tezi, Fırat Üniversitesi SBE, Elazığ, 2008.

GÜROCAK İsmail, "Bilişim Sistemine Girme Suçu (TCK m.243)" (Çevrimiçi Yayın)

GÜRSOY Emin, Bilişim Yoluyla Dolandırıcılık ve Korunma Yöntemleri, Yayımlanmamış Yüksek Lisans Tezi, Afyon Kocatepe Üniversitesi Fen Bilimleri Enstitüsü, Afyon 2015

HAFIZOĞULLARI Zeki/ÖZEN Muharrem, "Türk Ceza Hukuku Genel Hükümler", US-A Yayıncılık, Ankara, 2017.

HAFIZOĞULLARI Zeki/ÖZEN Muharrem, "Türk Ceza Hukuku Özel Hükümler Topluma Karşı Suçlar" US-A Yayıncılık, Ankara, 2012, s. 48.

HENKOĞLU Türkay / KÜLCÜ Özgür, Bilgi Erişim Platformu Olarak Bulut Bilişim: Riskler ve Hukuksal Koşullar Üzerine Bir İnceleme, Bilgi Dünyası Dergisi, Y:14, S:1, 2013

İÇEL Kayıhan, "Görünüşte Birleşme (İçtima) İlkeleri ve Yeni Türk Ceza Kanunu", İstanbul Ticaret Üniversitesi Sosyal Bilimler Dergisi, Y.7, S. 14, Güz 2008.

İÇEL Kayıhan, "Ceza Hukuku Genel Hükümler" Beta Basım Yayın, 5. Baskı, 2017.

İLBAŞ Çığır, "Bilişim Suçlarının Sosyo-Kültürel Seviyelere Göre Algı Analizi", Yayımlanmamış Yüksek Lisans Tezi, Başkent Üniversitesi FBE, Ankara, 2009.

KADAYIFÇILAR Müzeyyen, "Bilgisayara Giriş", Bil-Öm A.Ş. Yayıncılık, Ankara, 1988.

KARA Veli, "Bilgisayara Giriş", Karadeniz Teknik Üniversitesi Yayınları, 1. Baskı, Trabzon, 1989.

KARAGÜLMEZ Ali, "Bilişim Suçları ve Soruşturma – Kovuşturma Evreleri", 5. Baskı, Seçkin Yayınevi, Ankara, 2014.

KARAKEHYA Hakan, **"**Türk Ceza Kanununda Bilişim Sistemine Girme Suçu**"** TBB Dergisi, S:81, 2009.

KESKİN İbrahim, Bilişim Suçları, Adalet Dergisi, Ankara Sayı:29, 2007.

KETİZMEN Muammer, "Türk Ceza Hukukunda Bilişim Suçları", 1. Baskı, Adalet Yayınevi, Ankara,2008.

KILIÇ Hakan, Kamuda Bulut Bilişim Kullanımına Yönelik Risk Analiz ve Yönetimi, Yayımlanmamış Uzmanlık Tezi, T.C. Çevre ve Şehircilik Bakanlığı, Ankara, 2017.

KIZILTAN Mehmet Burak, "5237 Sayılı Türk Ceza Kanunu'nda Bilişim Sistemine Girme, Sistemi Engelleme ve Bozma Suçları", Yayınlanmamış Yüksek Lisans Tezi, İstanbul Üniversitesi SBE, İstanbul, 2007.

KOCA Mahmut, YTCK'da Hukuka Uygunluk Nedenleri, Ceza Hukuku Dergisi, Y:1, S:1, 2006.

KOCA Mahmut, Verileri Yok Etme veya Değiştirme Suçu, T.C. Yargıtay Başkanlığı, Bilişim Hukuku Konferansı (09-10 Ekim 2008), Ankara.

KOCA Mahmut / ÜZÜLMEZ İlhan, "Türk Ceza Kanunu Özel Hükümler", Ankara, Seçkin Yayınevi, 5. Baskı 2018.

KOCA Mahmut / ÜZÜLMEZ İlhan, "Türk Ceza Hukuku Genel Hükümler", 10. Baskı, Seçkin Yayıncılık, Ankara, 2017.

KOÇAK Hüseyin/DANDİN Ali Nazmi, "Toplumsal ve Yönetsel Alanda Bilişim Teknolojilerinin Kriminal Etkileri" Afyon Kocatepe Üniversitesi Sosyal Bilimler Dergisi, C:19, S:1, 2017.

KORUYAN Kutan / BİNGÖL F. Itır, Bulut Bilişim Hizmet Sağlayıcılarının Veriyi Koruyamama Durumuyla İlgili Türk, Avrupa Birliği ve Amerikan Hukukundaki Düzenlemeler, Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, C:17, S:3 Y:2015.

KORKMAZ İbrahim, "Cihaz, Program, Şifre ve Güvenlik Kodlarının Bilişim Suçlarının İşlenmesi Amacıyla İmal ve Ticareti Suçu", Terazi Hukuk Dergisi, C:13, S:142, 2018.

KÖKSAL Aydın, "Bilişim Toplumu", Türkiye Bilişim Ansiklopedisi, (Baş Editörler: Tuncer Ören, Tuncer Üney, Rifat Çölkesen), Papatya Yayıncılık, 2006.

KÖKSAL Aydın, "Adı Bilgisayar Olsun", Cumhuriyet Kitapları, Bilişim Yazıları, Ankara, 2010.

KÖKSAL Aydın, "Bilişim Terimleri Sözlüğü", Türk Dil Kurumu Yayınları, Ankara Üniversitesi Basımevi, Ankara, 1991.

KURGAN Bilişim Güvenliği Araştırmaları Ve Geliştirme Merkezi, "Siber Mücadeleye Giriş", Kutlu Yayınevi, İstanbul, 2018.

KURT Levent, "Açıklamalı İçtihatlı Tüm Yönleriyle Bilişim Suçları", Seçkin Yayınevi, Ankara, 2005.

KURTARAN Özlem Meltem, ÇUBUKÇU Faruk, "Ansiklopedik Bilgi İşlem Terimleri Sözlüğü", Türkmen Kitabevi, İstanbul, 1991.

MAHMUTOĞLU Fatih Selami, "Türk Ceza Kanununda Yer Alan Bilişim Alanındaki Suçlar ve Karşılaşılan Sorunların Yargı Kararları Işığında Değerlendirilmesi", İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, C:71 S:1, 2013.

MAHMUTOĞLU Fatih Selami, "Kusurluluk Prensibi Açısından Azmettirenin Ceza Sorumluluğu", İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, C:63, S:1-2, 2005.

MAHMUTOĞLU Fatih Selami, "Karşılaştırmalı Hukuk Bakımından İnternet Sujelerinin Ceza Sorumluluğu", İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, İnternet Özel Bölümü Cilt: 59, Sayı:1-2, İstanbul, 2001.

MALKOÇ İsmail, "Açıklamalı İçtihatlı Yeni Türk Ceza Kanunu", 4. Cilt, Yetkin Kitabevi, Ankara, 2013.

MEMİŞ Tekin, Hukuki Açıdan Kitlelere E-Posta Gönderilmesi, Atatürk Üniversitesi Erzincan Hukuk Fakültesi Dergisi, C:5, S:1-4, 2001.

MERAN Necati, "Yeni Türk Ceza Kanununda Sahtecilik – Malvarlığı – Bilişim Suçları ile Ekonomi ve Ticaret Alanında Suçlar", Seçkin Yayıncılık, Ankara, 2005.

MODOĞLU Gözde, Dijital Oyunların Ceza Hukuku ve 5651 Sayılı Kanun Kapsamında Erişim Engelleme Kararları Açısından Değerlendirilmesi, Yayımlanmamış Yüksek Lisans Tezi, İstanbul Bilgi Üniversitesi SBE, İstanbul, 2015.

NACAR Fatma Burcu, "Avrupa Birliği Ülkeleri ve Türkiye'de Bilişim Suçlarının Ceza Hukukundaki Uygulamaları", Yayımlanmamış Yüksek Lisans Tezi, Atılım Üniversitesi SBE, Ankara, 2010.

NİZAM Feridun, "Avrupa Birliği Bilişim Politikası ve Türkiye'nin Uyumu", Akademik Bilişim 2005 Konferansı Konuşma Metni (Çevrimiçi Yayın).

ORTA Mesut, "Bilişim Suçları ve Elektronik Delillerin Toplanması, Muhafazası, Değerlendirilmesi, Sunulması (Adli Bilişim)", Yetkin Yayınları, Ankara, 2015.

ÖNER Mehmet Zülfü, "Türk Ceza Hukukunda Uyuşturucu veya Uyarıcı Madde İmal ve Ticareti Suçları" Yayınlanmamış Doktora Tezi, Ankara Üniversitesi SBE, Ankara, 2010.

ÖNOK Murat, "Avrupa Konseyi Siber Suçlar Sözleşmesi Işığında Siber Suçlarla Mücadelede Uluslararası İşbirliği", (Çevrimiçi Yayın).

ÖZ Arzu, Bulut Bilişim Veri Güvenliği, Yayımlanmamış Yüksek Lisans Tezi, Gazi Üniversitesi Bilişim Enstitüsü, Ankara, 2013.

ÖZBAŞ Mert Yılmaz, Elektronik Para ve Sanal Para:, Bitcoin Geleceğin Para Birimi Olabilir Mi? İşletme Ekonomi ve Yönetim Araştırmaları Dergisi, S:1, 2019.

ÖZBEK Mücahid, "Avrupa Siber Suçlar Sözleşmesinin Türk Ceza Hukukuna Etkileri", (Çevrimiçi Yayın).

ÖZBEK Veli Özer, "Banka Veya Kredi Kartlarının Kötüye Kullanılması Suçu (TCK m.245)", Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi, Cilt: 9, Özel Sayı, İzmir, 2007.

ÖZBEK Veli Özer, "İnternet Kullanımında Ortaya Çıkabilecek Bazı Ceza Hukuku Sorunları" (Çevrimiçi Yayın).

ÖZBEK Veli Özer/DOĞAN Koray/BACAKSIZ Pınar/TEPE İlker, "Türk Ceza Hukuku Özel Hükümler", 11. Baskı, Ankara, Seçkin Yayıncılık, 2017.

ÖZEN Mustafa, "Suçların İçtiması (Zincirleme Suç – Fikri İçtima – Bileşik Suç)" Yayımlanmamış Doktora Tezi, Ankara Üniversitesi SBE, Ankara, 2008.

ÖZGENÇ İzzet, "Türk Ceza Kanunu Gazi Şerhi (Genel Hükümler)", Ankara Açık Ceza İnfaz Kurumu Matbaası, 3.Basım, 2006.

ÖZGENÇ İzzet , "Türk Ceza Kanunu Genel Hükümler", Ankara, Seçkin Yayıncılık, 14. Baskı, 2018.

ÖZKAN Halid, "Sorularla, Açıklamalı İçtihatlı, Bilişim Hukuku Mevzuatı", Adalet Yayınları, Ankara, 2014.

ÖZKUL Davut, "Bilişim Sistemi Kavramı ve Bilişim Sistemlerinin Denetimi", Sayıştay Dergisi, S:44-45, 2002.

PALLI Hayati, "Türk Hukukunda ve Mukayeseli Hukukta Bilişim Suçları", Yayımlanmamış Yüksek Lisans Tezi, Erciyes Üniversitesi SBE, Kayseri, 2008.

PARLAR Ali, "Türk Ceza Hukukunda Bilişim Suçları", 3. Baskı, Ankara, Bilge Yayınevi, 2015.

PEKER Bekir, "Bilişim Suçları ve Bilişim Güvenliğinin Ulusal ve Uluslararası Boyutu", Yayımlanmamış Yüksek Lisans Tezi, Selçuk Üniversitesi SBE, Konya, 2010.

ROTMAN Sarah, Bitcoin Versus Electronic Money, World Bank Document, 2014.

SARI Onur, "Uluslararası Hukuk ve Türk Ceza Hukuku Bağlamında Siber Güvenlik ve Bilişim Sistemine Yönelik Suçlar", Yayımlanmamış Yüksek Lisans Tezi, Harp Akademileri Stratejik Araştırmalar Enstitüsü, İstanbul, 2013.

SAY Kubilay, "Bilişim Suçlarında Elde Edilen Delillerin Olay Yerinden Toplanması ve Laboratuvarda İncelenmesi", Yayınlanmamış Yüksek Lisans Tezi, Ankara Üniversitesi Sağlık Bilimleri Enstitüsü, Disiplinlerarası Adli Tıp Anabilim Dalı Fizik İncelemeler Ve Kriminalistik Bilim Dalı, Ankara, 2006.

SERT Şeyma, Kişisel Verilerin 5237 Sayılı Türk Ceza Kanunu Kapsamında Korunması, Yayımlanmamış Yüksek Lisans Tezi, Atatürk Üniversitesi SBE, Erzurum, 2018.

SEYREK İbrahim Halil, Bulut Bilişim, İşletmeler için Fırsatlar ve Zorluklar, Gaziantep Üniversitesi Sosyal Bilimler Dergisi, Y:10 S:2.

SINAR Hasan, "İnternet ve Ceza Hukuku", Beta Yayınları, İstanbul, 2001.

SINAR Hasan, "İnternetin Ortaya Çıkardığı Hukuki Sorunlara Bir Ceza Hukuku Yaklaşımı", Milletlerarası Hukuk ve Özel Hukuk Bülteni, Sayı:1-2, 1997-1998.

SÖNMEZ Yağmur, "Günümüz İnternet Ortamında Bilişim Suçları ve Türkiye'deki İnternet Haber Sitelerine Yansımaları", Yayımlanmamış Yüksek Lisans Tezi, Marmara Üniversitesi SBE, İstanbul, 2018.

SÖNMEZ Ümit, "Bilişim Sistemleri Aracılığıyla Dolandırıcılık Suçu", Dicle Üniversitesi Adalet Meslek Yüksekokulu Dicle Adalet Dergisi, C:1, S:2, 2017.

SÖZER Bülent, "Elektronik Sözleşmeler", İstanbul, Beta Basım Yayın, 2002.

ŞENGÜL Gökhan / BOSTAN Atila, Bulut Bilişimde Bilgi Güvenliği Standardizasyon Çalışmaları, 6. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı, 2013. (Çevrimiçi Yayın)

TAMER İzzet, *"*Bilgisayara Giriş*"*, SFS Grup Yayınevi, Ankara 1. Baskı, 2012.

TAŞ İsmail Melih, "Bilgisayar Tabanlı Bilişim Suçlarının Adli Bilişim Çerçevesinde İncelenmesi ve Analizi", Yayımlanmamış Yüksek Lisans Tezi, Marmara Üniversitesi FBE, İstanbul, 2013.

TAŞ Kezban Atalıç, "Bilişim Suçları ve Adana İlinde 2006-2009 Yılları Arasında Meydana Gelen Bilişim Suçlarının Değerlendirilmesi", Yayımlanmamış Yüksek Lisans Tezi, Çukurova Üniversitesi SBE, Adana, 2010.

TAŞÇI Ufuk/CAN Ali, Türkiye'de Polisin Siber Suçlarla Mücadele Politikası, Fırat Üniversitesi Sosyal Bilimler Dergisi, C:25, S:2, Elazığ, 2015.

TAŞDEMİR Kubilay, "Bilişim, Banka ve Kredi Kartlarının Kötüye Kullanılması ve Dolandırıcılık Suçları", Cantekin Matbaacılık, Ankara, 2009.

TAŞKIN Şaban Cankat, "Bilişim Suçları", İstanbul, Beta Yayınevi, 2008.

TAŞKIN Şaban Cankat, "Bilişim Hukuku Uluslararası Anlaşmazlıklar" TBB Dergisi, S:85, 2009.

TEZCAN Durmuş/ERDEM Mustafa Ruhan/ ÖNOK Murat, "Teorik ve Pratik Ceza Özel Hukuku", 16.Baskı, Seçkin Yayınevi, Ankara, 2018.

TIEDEMANN Klaus "Bilgisayarla İşlenen Suçların Ceza Hukuku Yönünden İncelenmesi", İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, Cilt:41, 1975.

TOPALOĞLU Mustafa, "Bilişim Hukuku", Adana, Karahan Kitabevi, 2005.

TOPALOĞLU Murat / ÖZKİŞİ Harun / TEKKANAT Egemen, Bulut Bilişim, Seçkin Yayınları, Ankara, 2017.

TULUM İsmail, "Bilişim Suçları İle Mücadele", Yayınlanmamış Yüksek Lisans Tezi, Isparta Süleyman Demirel Üniversitesi SBE, Isparta, 2006.

TUFANOĞLU İshak, Banka veya Kredi Kartlarının Kötüye Kullanılması Suçu, Yayımlanmamış Yüksek Lisans Tezi, İstanbul Üniversitesi SBE, İstanbul, 2014

TUNCER Arzu, "Uyuşturucu veya Uyarıcı Madde Ticareti ve Kullanılmasına İlişkin Suçlar", Yayımlanmamış Doktora Tezi, İstanbul Kültür Üniversitesi SBE, 2011.

TURABİ Selami, "Kusurluluk ve Kusurluluğu Etkileyen Haller" TBB Dergisi, S:101, 2012.

TURAN Fatma, "Milli Eğitim Bakanlığı Bilişim Sisteminin Bir Alt Sistemi Olarak E-Okul Uygulamasına İlişkin İlköğretim Okullarındaki Yönetici, Öğretmen ve Veli Görüşleri", Yayımlanmamış Yüksek Lisans Tezi, Akdeniz Üniversitesi SBE, Antalya, 2010.

TURAN Metin/ KÜLCÜ Özgür, "Türkiye'de Bilişim Suçlarının Tanımlanması ve Yaşanan İhlallere Yönelik İçerik Analizi", Türk Kütüphaneciliği Dergisi, C:28, S:1, 2014.^

TÜYSÜZ Fırat, Dolandırıcılık Suçu, Yayımlanmamış Yüksek Lisans Tezi, Başkent Üniversitesi SBE, Ankara 2017.

Türkiye 2'nci Bilişim Şurası Sonuç Raporu, 10-11 Mayıs 2004, Ankara, 2004

UÇAR Hüdaverdi, "5237 Sayılı Türk Ceza Kanunu'nda Bilişim Suçları", Yayımlanmamış Yüksek Lisans Tezi, Çankaya Üniversitesi SBE, Ankara, 2014.

UÇKAN Özgür, "Bilgi Ekonomisi, Bilgi Toplumu, Mahremiyet ve Güvenlik" Ankara Barosu Uluslararası Hukuk Kurultayı, 03-07 Ocak Ankara, Ankara Barosu Yayınları, Ankara, Cilt:4 s.2, 2006.

ULUTÜRK Güner Hande, "Türk Ceza Hukukunda Akıl Hastalığı ve Kusur Yeteneğine Etkisi", Bahçeşehir Üniversitesi SBE, Yayımlanmamış Yüksek Lisans Tezi, İstanbul, 2009.

UZUNTOK Mesut, "Uyuşturucu Veya Uyarıcı Madde İmal Ve Ticareti Suçları", Yayınlanmamış Doktora Tezi, Marmara Üniversitesi SBE, İstanbul, 2008.

ÜNAL Ahmet, "Bilişim Suç Türlerinden Biri Olan Dağıtık Servis Dışı Bırakma Saldırılarının Önlenmesindeki Hukuki ve Teknik Zorluklar", Yayımlanmamış Yüksek Lisans Tezi, İstanbul Bilgi Üniversitesi SBE, İstanbul, 2014.

ÜNAL Cahide / ŞAHİN İsmail, İstanmeyen Elektronik Postaların (SPAM) Filtrelenmesi için Bir Uzman Sistem Tasarımı ve Gerçekleştirilmesi, Politeknik Dergisi, C:20, S:2, 2017.

ÜNVER Mustafa / MİRZAOĞLU Ayşe Gül, Yemleme (Phishing) Raporu, Bilgi Teknolojileri ve İletişim Kurumu Yayınları, 2011.

ÜNVER Yener, "Türk Ceza Kanunu'nun ve Ceza Kanunu Tasarısının İnternet Açısından Değerlendirilmesi", İstanbul Üniversitesi Hukuk Fakültesi Mecmuası İnternet Özel Bölümü, Cilt:59, Sayı:1-2, 2001.

YARDIMCIOĞLU Mahmut/ŞERBETÇİ Gamze, Bitcoin'in Yapısı ve Yasa Dışı Kullanımı, Al Farabi Sosyal Bilimler Dergisi, C:2, S:4, 2018.

YAŞAR Osman/GÖKÇAN Hasan Tahsin/ARTUÇ Mustafa, "Yorumlu, Uygulamalı Türk Ceza Kanunu", Cilt:5, Ankara, Adalet Yayınevi, 2010.

YAYCI Esra, "Bilişim Suçları" Yayınlanmamış Yüksek Lisans Tezi, Gazi Üniversitesi SBE, Ankara, 2007.

YAZICIOĞLU Recep Yılmaz, "Bilgisayar Suçları: Kriminolojik, Sosyolojik ve Hukuksal Boyutları İle", İstanbul , Alfa Yayınevi, 1997.

YAZICIOĞLU Recep Yılmaz, "Yeni Türk Ceza Kanunundaki Bilişim Suçlarının Genel Değerlendirilmesi", Yeditepe Üniversitesi Hukuk Fakültesi Dergisi, Cilt:2, Sayı:2, Yıl:2005.

YAZICIOĞLU Recep Yılmaz, "Hukukumuzda TCK'nın 243'üncü Madde Kapsamında Bilişim Sistemine Girme Eylemi" 9-10 Ekim 2008 Yargıtay Bilişim Hukuku Konferansı Yargıtay Başkanlığı Yayını, Ankara 2009, s. 81.

YENİSEY Feridun, "İnternet Suçlarının Yeni İşleniş Biçimleri", Uluslararası İnternet Hukuku (21-22.05.2001) Sempoyumu, İzmir, Dokuz Eylül Üniversitesi Yayınları, 2002.

YENİDÜNYA A. Caner, "Bilişim Sistemine Hukuka Aykırı Erişim Suçu", Legal Fikri ve Sınai Haklar Dergisi, C:1 S:4 Y:2005.

YENİDÜNYA Caner/DEĞİRMENCİ Olgun, "Mukayeseli Hukukta ve Türk Hukukunda Bilişim Suçları", İstanbul, Legal Yayınevi, 2003.

YETİM Servet, "Bilişim Suçları ve Etkin Mücadele Yöntemleri", Terazi Hukuk Dergisi, C:9, S:95, 2014.

YILDIZ Arif/ AKDENİZ M. Ali, "Vpn (Sanal Özel Ağlar)**"** (Çevrimiçi Yayın).

YILDIZ Mehmet Emre, "Banka ve Kredi Kartlarının Kötüye Kullanılması Suçu", Yayınlanmamış Yüksek Lisans Tezi, Dokuz Eylül Üniversitesi SBE, İzmir, 2011.

YILMAZ Çetin, Türk Ceza Hukukunda Dolandırıcılık Suçu, Yayımlanmamış Yüksek Lisans Tezi, Çankaya Üniversitesi SBE, Ankara 2018

YILMAZ Furkan, "Türkiye'deki Bilişim Suçlarının Sosyolojik Bir Analizi: Tehditler ve Çözüm Stratejileri", Yayımlanmamış Yüksek Lisans Tezi, Anadolu Üniversitesi SBE, Eskişehir, 2015.

YILMAZ Sacit, "5237 Sayılı TCK'nın 244.Maddesinde Düzenlenen Bilişim Alanındaki Suçlar", Türkiye Barolar Birliği Dergisi, 2011.

WAGNER Andrew, Digital vs. Virtual Currencies, Bitcoine Magazine, S:22 Ağustos 2014. (Çevrimiçi Yayın)

Web Siteleri

https://ab.org.tr/ab05/tammetin/89.doc

http://appsso.eurostat.ec.europa.eu/nui/show.do?dataset=isoc_bde15ei&lang=en

http://www.biakraporu.org/docs/rapor.kisim3.bolum01.pdf

http://bidb.itu.edu.tr/seyir-defteri/blog/2013/09/07/intranet-(i%C3%A7-a%C4%9F)-ve-extranet-(d%C4%B1%C5%9F-a%C4%9F)

http://www.bilgitoplumu.gov.tr/

https://bitcoinmagazine.com/articles/digital-vs-virtual-currencies-1408735507

https://www.ccn.com/cryptocurrency/

http://conventions.coe.int/Treaty/en/Reports/Html/185.htm

http://dergipark.gov.tr/maruid/issue/434/3229

http://www.elithukuk.com/yeni-bir-bilisim-sucu-zararli-yazilim-ve-yasak-cihaz/

https://www.goksusafiisik.av.tr/Articletter/2015_Summer/GSI_Articletter_2015_Summer_Article6.pdf

http://www.hasanbalik.com/projeler/bitirme/32.pdf

http://hgm.ubak.gov.tr/Content/UploadedFile/Ulusal%20Geni%C5%9Fbant%20Stratejisi%20ve%20Eylem%20Plan%C4%B1%202017-2020&&dfc2d335-235b-4293-a946-b371a6262244.pdf

http://hukuk.deu.edu.tr/dosyalar/dergiler/DergiMiz4-1/PDF/ozbek5.pdf

http://www.idc-online.com/technical_references/pdfs/data_communications/Internet_Intranet_and_Extranet.pdf

http://www.internetsociety.org/internet/what-internet/history-internet/brief-history-internet

http://www.internetworldstats.com/

https://www.iscturkey.org/assets/files/2016/03/2013-paper45.pdf

http://istanbul.dergipark.gov.tr/download/article-file/99545

http://www.ismailgurocak.av.tr/makale/

http://www.journals.istanbul.edu.tr/iuhfm/article/view/1023010611/1023009846

https://jurix.com.tr/

http://law.yeditepe.edu.tr/tr/yu-hukuk-fakultesi-dergisi

https://www.lexpera.com.tr

https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf (

http://www.onurunurlu.com/dosyalar/agsistemleriyonlendirme/yerelagsistemleri.pdf

https://openknowledge.worldbank.org/bitstream/handle/10986/18418/881640BRI0Box30WLEDGENOTES0Jan02014.pdf?sequence=1&isAllowed=y

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

http://www.ozocak.com/Dosyalar/27669f.pdf

http://www.politics.ankara.edu.tr/dergi/pdf/49/3/ersoyyuksel.pdf

http://portal.ubap.org.tr/App_Themes/Dergi/2009-81-498.pdf

https://www.selcuk.edu.tr/hukuk/birim/web/sayfa/ayrinti/2102/tr

http://some.sdu.edu.tr/assets/uploads/sites/408/files/ddos-el-kitabi-22092017.pdf

https://statik.tse.org.tr/upload//tr/dosya/icerikyonetimi/1202/17032015093613-3.pdf

http://www.spk.gov.tr/SiteApps/Yayin/YayinGoster/1130

http://tbbdergisi.barobirlik.org.tr/m1993-19932-968

http://tbbdergisi.barobirlik.org.tr/m2009-85-571

http://tbbdergisi.barobirlik.org.tr/m2011-92-669

https://www.tbb.org.tr/Content/Upload/Dokuman/801/BILISIM_HUKUKU.pdf

https://www.tbmm.gov.tr/sirasayi/donem26/yil01/ss117.pdf

http://tdk.gov.tr/

https://tez.yok.gov.tr/UlusalTezMerkezi/

https://ticaret.edu.tr/uploads/kutuphane/dergi/s14/035-049.pdf

http://www.tuik.gov.tr/PreHaberBultenleri.do?id=21779

http://www.tk.org.tr/index.php/tk/article/viewArticle/2394

http://www.usg.edu/galileo/skills/unit07/internet07_02.phtml

http://www.yayin.adalet.gov.tr/adaletdergisi/29.sayi/09_34_14.pdf

https://webdosya.csb.gov.tr/db/cbs/icerikler/tez-hakan-kilic-20180925132839.pdf