TÜRK HUKUKUNDA DOĞRUDAN BİLİŞİM SUÇLARI

Yüksek Lisans Tezi

Hasan Burak ÖNDİN

Eskişehir, 2017

TÜRK HUKUKUNDA DOĞRUDAN BİLİŞİM SUÇLARI

Hasan Burak ÖNDİN

YÜKSEK LİSANS TEZİ

Kamu Hukuku Anabilim Dalı

Danışman: Yrd. Doç. Dr. Nazmiye ÖZENBAŞ BOYDAĞ

Eskişehir

Anadolu Üniversitesi

Sosyal Bilimler Enstitüsü

Ağustos, 2017

JÜRİ VE ENSTİTÜ ONAYI

Hasan Burak ÖNDİN'in "Türk Hukukunda Doğrudan Bilişim Suçları" başlıklı tezi **21 Ağustos 2017** tarihinde, aşağıdaki jüri tarafından Lisansüstü Eğitim Öğretim ve Sınav Yönetmeliğinin ilgili maddeleri uyarınca toplanan **Kamu Hukuku** Anabilim Dalında, **yüksek lisans tezi** olarak değerlendirilerek kabul edilmiştir.

İmza

Üye (Tez Danışmanı) : **Yrd.Doç.Dr.Nazmiye ÖZENBAŞ BOYDAĞ**

Üye : **Doç.Dr.Mustafa AVCI**

Üye : **Yrd.Doç.Dr.Mahmut KAPLAN**

Prof.Dr.Kemal YILDIRIM
Anadolu Üniversitesi
Sosyal Bilimler Enstitüsü Müdürü

TEŞEKKÜR

Tez çalışmam boyunca benden desteğini esirgemeyen danışman hocam Yrd. Doç. Dr. Nazmiye ÖZENBAĞ BOYDAĞ'a, jüri üyesi diğer hocalarıma, kaynaklara ulaşabilmem için bana yardımcı olan değerli arkadaşlarıma ve çok kıymetli ailem başta olmak üzere tüm sevdiklerime teşekkür ederim.

Hasan Burak ÖNDİN

Eskişehir, 2017

21 / 08 /2017

ETİK İLKE VE KURALLARA UYGUNLUK BEYANNAMESİ

Bu tezin bana ait, özgün bir çalışma olduğunu; çalışmanın hazırlık, veri toplama, analiz ve bilgilerin sunumu olmak üzere tüm aşamalardan bilimsel etik ilke ve kurallara uygun davrandığımı; bu çalışma kapsamında elde edilemeyen tüm veri ve bilgiler için kaynak gösterdiğimi ve bu kaynaklara kaynakçada yer verdiğimi; bu çalışmanın Anadolu Üniversitesi tarafından kullanılan "bilimsel intihal tespit programı"yla tarandığını ve hiçbir şekilde "intihal içermediğini" beyan ederim. Herhangi bir zamanda, çalışmamla ilgili yaptığım bu beyana aykırı bir durumun saptanması durumunda, ortaya çıkacak tüm ahlaki ve hukuki sonuçlara razı olduğumu bildiririm.

Hasan Burak ÖNDİN

İÇİNDEKİLER

Sayfa

İKİNCİ BÖLÜM

KISALTMALAR DİZİNİ

a.g.k. : Adı Geçen Kaynak

ASSS : Avrupa Konseyi Siber Suçlar Sözleşmesi

AÜEHFD : Atatürk Üniversitesi Erzincan Hukuk Fakültesi Dergisi

AÜHFD : Ankara Üniversitesi Hukuk Fakültesi Dergisi

AÜSBFD : Ankara Üniversitesi Siyasal Bilgiler Fakültesi Dergisi

BKKKK **:** Banka Kartları ve Kredi Kartları Kanunu

Bkz. : Bakınız

CMK : Ceza Muhakemesi Kanunu

Çev. : Çeviren

DEÜHFD : Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi

Ed. : Editör

EİK : Elektronik İmza Kanunu

FSEK : Fikir ve Sanat Eserleri Kanunu

GÜHFD : Gazi Üniversitesi Hukuk Fakültesi Dergisi

http. : Hyper Text Transfer Protocol

İÜHFM : İstanbul Üniversitesi Hukuk Fakültesi Mecmuası

m. : Madde

s. : Sayfa

SÜHFD : Selçuk Üniversitesi Hukuk Fakültesi Dergisi

TBB : Türkiye Barolar Birliği

TBMM : Türkiye Büyük Millet Meclisi

TCK : 5237 Sayılı Türk Ceza Kanunu

TCKÖT : Türk Ceza Kanunu Ön Tasarısı

TRIPS : Treaty Related Aspects of Intellectual Property Rights

vb. : Ve Benzeri

WIPO : World Intellectual Organization

WTO : World Trade Organization

www. : World Wide Web

GİRİŞ

Bilişim sistemleri sürekli gelişmektedir. Geçmişte günlerce süren işlemler, günümüzde bilgisayarlar, akıllı telefonlar, tabletler ve diğer bilişim araçları sayesinde, birkaç dakika içerisinde halledilebilmektedir. Teknolojinin gelişmesiyle, bilişim sistemleri eğitimden ticarete, sanayiden bankacılık işlemlerine kadar hemen her alanda kullanılmaya başlanmıştır. Devlet kurumları da birçok kamu hizmetinin vatandaşa sunulmasında, bilişim sistemlerinden aktif olarak yararlanmaktadır. Bilişim sistemlerinin yaygın olarak kullanımıyla, bilginin dolaşımı hızlanmış, insanların iletişim alışkanlıkları değişmiş, sanayi ve tarımda üretim olanakları artmış, ekonomik ve ticari yaşamda faaliyetler daha kolay ve verimli hale gelmiştir. Bilişim sistemlerinin yaygın olarak kullanılmasıyla birlikte sınırlar kalkmış dünya adeta global bir köy olmuştur.

Tüm bu gelişmelere bağlı olarak bilişim suçları da son yıllarda artış göstermiştir. Bilişim araçlarının, suç işlemede sağladığı kolaylıktan faydalanan failler, yeni suç işleme yöntemleri geliştirmişlerdir. Bugün itibariyle bilişim sistemleri üzerinde gerçekleştirilebilecek bütün ihlal hareketlerinin bilindiğini söylemek mümkün değildir. Sürekli gelişen bir alanda böyle bir şey iddia etmek doğru da değildir. Çalışmamızda inceleyeceğimiz ihlal hareketleri, bugüne kadar sıklıkla karşılaşılan yöntemlerden ibarettir.

Türk Hukukunda, bilişim suçları 1991 yılında yapılan değişiklikle, 765 sayılı Türk Ceza Kanunu (TCK)'na eklenmiştir. Bu düzenlemeden önce, bilişim sistemlerine yönelik ihlallere, ceza kanunundaki genel normlar uygulanıyordu. Ancak, gelişen bilişim teknolojisiyle birlikte mevcut kanun hükümlerinin yetersiz kalması sonucu yeni düzenlemeler yapılması ihtiyacı doğmuştur. Yapılan düzenlemeyle, bilişim sistemlerinin kendisine zarar vermenin yanı sıra sistemde var olan verilerin, programların ve diğer unsurların bozulması, silinmesi ya da ele geçirilmesi gibi fiiller ve bilişim sistemlerindeki sahtekarlık fiilleri suç olarak tanımlanmıştır.

Zaman içerisinde kanundaki düzenlemeler, siber alanda yaşanan ilerlemenin hızına yetişememiştir. 2005 yılında 5237 sayılı Türk Ceza Kanunu (TCK)'nun yürürlüğe

girmesiyle birlikte yeni suç tipleri oluşturulmuştur. 5237 sayılı TCK ile yetkisiz erişim ilk kez münhasıran suç haline getirilmiş ayrıca banka ve kredi kartlarının kötüye kullanılması suç olarak tanımlanmıştır. Kanunda daha sonra yapılan değişikliklerle, bilişim sistemine girmeksizin veri nakillerinin teknik araçlarla izlenmesi, bilişim suçlarının işlenmesini sağlayacak cihaz ve programların üretimi, bulundurulması, nakledilmesi ve ticareti suç haline getirilmiştir.

Türk Ceza Kanunu'nun yanı sıra Fikir ve Sanat Eserleri Kanunu (FSEK)'nda, Elektronik İmza Kanunu (EİK)'nda da doğrudan bilişim suçlarına yer verilmiştir. Fikir ve Sanat Eserleri Kanunu'nda, bilgisayar programları, fikir ve sanat eseri olarak kabul edilerek, fikir ve sanat eserlerini ve sahiplerinin haklarını koruma amaçlı olan manevi, mali ve bağlantılı haklara tecavüz suçları ile koruyucu programları etkisiz kılma suçu, doğrudan bilişim suçlarından sayılır olmuştur. Elektronik İmza Kanunu'nda, bazı istisnalar dışında hüküm ve sonuçları itibariyle ıslak imzaya eşdeğer olan elektronik imzanın kötüye kullanılmasına yönelik suç tiplerine yer verilmiştir.

Çalışmanın birinci bölümünde, öncelikle bilişim ve bilişim sistemi kavramı üzerinde durulmuş, doktrinde yapılmış olan çeşitli tanımlamalar ayrıntılı olarak ele alınmıştır. Daha sonra, bilişim alanında en temel unsurlar olan bilgisayar, internet, program ve veri kavramları tanımlanmıştır. Ardından, bilişim suçlarının neler olduğu ve failleri bu suçları işlemeye iten etkenler üzerinde durulmuş, ilk bölümün son kısmında ise bugüne kadar çok sık karşılaşılmış bilişim suçu işlenme şekilleri incelenmiştir.

İkinci bölümde ise, bilişim suçlarının Türk Hukukundaki tarihsel süreci kronolojik olarak anlatılmıştır. Bilişim suçlarına dair esas ceza normlarını düzenleyen 5237 sayılı Türk Ceza Kanunu'ndaki doğrudan bilişim suçları, unsurları itibariyle ayrıntılı olarak ele alınmıştır. Ayrıca, yine doğrudan bilişim suçlarına yönelik düzenlemeler içeren Fikir ve Sanat Eserleri Kanunu'ndaki, manevi, mali ve bağlantılı haklara tecavüz suçları ile koruyucu programlara ilişkin suçlar, Elektronik İmza Kanunu'ndaki, imza oluşturma verilerini izinsiz kullanma ve elektronik sertifikalarda sahtekarlık suçları incelenmiştir. Mevzuattaki dolaylı bilişim suçları olarak kabul edilen düzenlemeler çalışma kapsamı dışında bırakılmıştır.

BİRİNCİ BÖLÜM

1. BİLİŞİM SUÇLARINA DAİR TEMEL KAVRAMLAR

1.1. Bilişim ve Bilişim Sistemi Kavramları

Bilişim sözcüğünün kökeni, Fransızca "informatıque" sözcüğüne dayanmaktadır. Aynı kavram İngilizcede "informatics" olarak ifade edilmektedir. Bu ifade, Türkçeye de "bilişim" sözcüğü olarak geçmiştir. Bilişim sözcüğü, bilgi ve iletişim sözcüklerinin bir araya getirilmesiyle oluşmuştur.[1] Bilişim çok farklı şekillerde tanımlanmaktadır. Sözlük anlamı olarak bakıldığında bilişim; insanoğlunun, teknik, ekonomik ve toplumsal alanlardaki iletişiminde kullandığı ve bilimin dayanağı olan bilginin özellikle elektronik makineler aracılığıyla düzenli ve akla uygun bir biçimde işlenmesi olarak tanımlanmıştır.[2] Bir bilim dalı olarak ise bilişim; bilginin, özellikle elektronik makineler aracılığıyla, düzenli ve ussal biçimde işlenmesi bilimidir.[3]

Bilişim sözcüğünün tanımı konusunda doktrinde bir mutabakat yoktur. Bu alanda çok çeşitli tanımlamalar yapılmıştır. Bu tanımlamalara örnek verecek olursak; Dülger'e göre, "bilişim; insanların, teknik, ekonomik, siyasal ve toplumsal alanlardaki iletişiminde kullandığı bilginin özellikle bilgisayarlar aracılığıyla düzenli ve akılcı biçimde işlenmesi, her türden düşünsel sürecin yapay olarak yeniden üretilmesi, bilginin bilgisayarlarda depolanması ve kullanıcıların erişimine açık bulundurulması bilimidir".[4] Yenidünya/Değirmenci' ye göre, "bilişim; teknik, ekonomik, sosyal, hukuk ve benzeri alanlardaki verinin saklanması, saklanan bu verinin otomatik olarak işlenmesi, organize edilmesi, değerlendirilmesi ve aktarılması ile ilgili bir bilim dalıdır".[5] Parlar'a göre ise, "bir sistem olarak bilişim sistemi; verileri toplayıp yerleştirdikten sonra bunları otomatik işleme tabi tutma olanağını veren sistemlerden oluşan alandır".[6] Eralp'e göre ise, "bilişim; teknolojinin ve belgeleme tekniğinin gelişmesiyle insanların, sosyal, siyasal, hukuki, askeri, ekonomik, kültürel, teknik vb. birçok alana dair sahip oldukları

[1]M. Özen ve İ. Baştürk (2011). *Bilişim - İnternet ve Ceza Hukuku*. Ankara: Adalet Yayınevi, s. 11.
[2] http://www.tdk.gov.tr/index.php?option=com_gts&kelime=B%C4%B0L%C4%B0%C5%9E%C4%B0M (Erişim Tarihi: 05.04.2016)
[3]http://kelimeler.net/BİLİŞİM-kelimesinin-anlami-nedir (Erişim Tarihi: 15.05.2017)
[4]M.V. Dülger (2004). *Bilişim Suçları*. Ankara: Seçkin Yayınevi, s. 47.
[5]A.C. Yenidünya ve O.Değirmenci (2003). *Mukayeseli Hukukta ve Türk Hukukunda Bilişim Suçları*. İstanbul: Legal Yayıncılık, s. 27.
[6]A. Parlar (2011). *Türk Ceza Hukukunda Bilişim Suçları*. Ankara: Bilge Yayınevi, s. 16.

verilerin saklanması, işlenmesi, organize edilmesi, değerlendirilmesi ve bu verilerin işitsel ve görsel olarak aktarılmasını konu edinen akademik ve mesleki bir disiplindir".[7] Esen'e göre ise, "bilişim; bilgisayarlardan yararlanılarak bilgilerin depolanması, işlenerek başkalarının istifadesine sunulur hale getirilmesi ve iletilmesi faaliyetidir".[8]

Bilişim sistemi, donanım (hardware) ve yazılım (software) olmak üzere iki bileşenden oluşmaktadır. Donanım (hardware), verileri depolamayı, işlemeyi, kullanmayı ve nakletmeyi sağlarken; yazılım (software), bunların bu şekilde çalışmasını sağlamaktadır.[9] Bir başka deyişle; donanım, yazılım sisteminin talimatlarına göre belli zamanlarda devreye girerek fonksiyonlarını yerine getiren bilgisayarın klavye, kamera, yazıcı vb. gibi her türlü fiziksel parçasıdır. Yazılım ise donanımın nasıl çalışacağını belirleyen sanal bir uygulamadır.[10] Bilişim sistemi, bilgisayardan beklenen tüm amaçları gerçekleştirmeye elverişli donanım ve yazılım elemanlarının bütününü ifade eder.[11]

Bilişim alanı, siber alan ya da siber uzay olarak da bilinmektedir. Özellikle yabancı literatürde bu isimlerle ifade edilmektedir. Siber uzay kavramı, ilk kez ünlü bilim kurgu yazarı William Gibson tarafından Neuromancer isimli romanda kullanılan terimdir.[12] Avrupa'da bu alandaki en etkin düzenleme olan Avrupa Konseyi Siber Suçlar Sözleşmesi (ASSS)'nde[13] de bu terim kullanılmaktadır. Siber alan (siber uzay) kavramı, internet ile bilgisayar ve diğer bilgi teknolojileri temelli diğer geniş alan ağlarını ifade etmektedir.[14]

Tüm bu değerlendirmelerden anlaşılacağı üzere; bilişim faaliyetinin gerçekleştirildiği sisteme bilişim sistemi, tüm bu yapının genel adına da bilişim alanı denilmesi isabetli olacaktır. Burada, genel bir tanım vermek gerekirse, bilişim; modern

---

[7] http://www.ozgureralp.av.tr/web/makaleler/bilisim-suclari-turk-ceza-kanunu-madde-243-bilisim-sistemine-girme-2/ (Erişim Tarihi: 10.04.2016)

[8] S. Esen (2007). *Anlatımlı ve İçtihatlı Malvarlığına Karşı Suçlar Belgelerde Sahtecilik ve Bilişim Alanında Suçlar*. Ankara: Adalet Yayınevi, s. 624.

[9] B.Z. Avşar ve G. Öngören (2010). *Bilişim Hukuku*. İstanbul: Türkiye Bankalar Birliği, s. 45.

[10] N. Topaloğlu (2014). Bilgisayar Mimarisi. H. Çakır ve M.S. Kılıç (Ed.), *Adli Bilişim ve Elektronik Deliller*. içinde (25-93). Ankara: Seçkin Yayınevi, s. 25.

[11] Avşar ve Öngören, 2010, a.g.k., 45.

[12] E.D. Aydın (1999). *Bilişim ve Telekomünikasyon Terimler Sözlüğü*. İstanbul: Telsim Yayınları, s. 184.

[13] ASSS, bilişim suçları alanında maddi açıdan ve alan açıdan en geniş kapsama ve öneme sahip olan düzenlemedir. Bu sözleşme, Avrupa Konseyi bakanları tarafından 2001 yılında imzalanıp 2004 yılında yürürlüğe girmiştir. bkz. U. Sieber (2014). *İnternetteki Suçlar ve Suçun İnternette Takibi*. Y. Ünver (Ed.), Ankara: Seçkin Yayınevi, s. 64.; Özen ve Baştürk, 2011, a.g.k., 307.

[14] https://www.itu.int/osg/spu/visions/papers/securitypaper.pdf (Erişim Tarihi 03.07.2016)

dünyada, bilimden sanayiye, ekonomiden siyasete kadar çok farklı alanlarda insanlığın sahip olduğu her türlü verinin toplanmasını ve bunların otomatik olarak işlenmesini, saklanmasını, aktarılmasını ve analiz edilmesini sağlayan sisteme verilen isimdir. Böyle bir tanım yaptıktan sonra kanun koyucunun bilişim sistemi kavramını ne şekilde düzenlediği incelenmelidir. Çünkü, bu tür suçlarla mücadele edebilmenin ilk şartı, mevzuatın bilişim alanına dair kavramları net olarak açıklaması ve bu suç türünün unsurlarını da en azından genel anlamda belirtmesidir. Ayrıca, hızla gelişme gösteren teknoloji ve bilişim alanında koruyucu önlemlerin alınabilmesi ve bu alandaki ihlallerin karşılıksız kalmaması için mevzuatında sürekli yenilenmesi ve dinamik olması gerekir. Bu açıdan mevzuattaki bilişim alanına dair tanımlamaları gözden geçirmek gerekmektedir.[15]

Hukuk sistemimizde 1989 yılında hazırlanan Türk Ceza Kanunu Ön Tasarısı (TCKÖT) bilişim suçları alanında yapılan ilk çalışmadır. Bu tasarının 342. maddesinin gerekçesinde bilişim alanı; "bilgileri toplayıp depo ettikten sonra bunları otomatik işleme tabi tutma sistemlerinden oluşan alan" denilerek tanımlanmıştır.[16] 1991 yılında da mevzuatımızda ilk kez bilişim suçları (3756 Sayılı 765 Sayılı TCK'nın Bazı Maddelerinin Değiştirilmesine Dair Kanun'la 765 sayılı TCK'nın on birinci babında Bilişim Alanında Suçlar başlığı altında 525a, 525b, 525c, 525d maddeleri) düzenlenmiştir. 765 sayılı TCK'nın bilişim suçları alanına yönelik düzenlemesinin gerekçesinde, bilişim alanı ile ifade edilmek istenenin, "bilgilerin otomatik olarak işleme tabi tutuldukları sisteme ilişkin alan" olduğu ortaya konulmuştur.[17] 5237 Sayılı TCK'nın 243. maddesinin gerekçesinde de bilişim sistemi tanımı yapılmıştır. Gerekçeye göre, "Bilişim sisteminden maksat verileri toplayıp yerleştirdikten sonra bunları otomatik işlemlere tabi tutma olanağını veren manyetik sistemlerdir." Görüldüğü gibi, yıllar içerisinde mevzuatımızda bilişim alanının tanımında büyük bir değişiklik olmamıştır.

Bilişim üzerine yapılan tanımlamalarda birtakım farklılıkların olmasının başlıca sebepleri, bu alanın çok yeni ve henüz gelişimini sürdürüyor olması, teknoloji ile bilişim araçlarının da tahminlerin çok ötesinde bir süratle değişim/dönüşüm yaşaması ve

[15]A. Karagülmez (2009). *Bilişim Suçları ve Soruşturma - Kovuşturma Evreleri.* (2. Baskı). Ankara: Seçkin Yayınevi, s. 126-129.; ayrıca bkz. Sieber, 2014, a.g.k., 215-216.
[16]Yenidünya ve Değirmenci, 2003, a.g.k., 28.
[17]H. Karakehya (2009). Türk Ceza Kanunu'nda Bilişim Sistemine Girme Suçu. *TBB Dergisi*, (81), s. 8

nihayet bireysel ilişkileri de derinden etkilemesidir. Bu alandaki gelişmeler sosyal, siyasal, ekonomik ve hukuki alanda büyük değişimlere sebep olmaktadır. Geçmişte pek rastlanmayan bilişim teknolojileri günümüz dünyasında neredeyse her yerde karşımıza çıkmaktadır. Akıllı telefonlar, sosyal paylaşım siteleri, internetten alışveriş vb. burada verilebilecek sadece birkaç örnektir.[18] Bunun yanı sıra, bilişim alanında yüksek bilgi, işlem hızı, bilgilerin kitlesel olarak saklanabilmesi, dağıtılmış bilgilerin işlenebilmesi ve bir araya getirilebilmesi olanağıyla birlikte sistemin esnekliği, evrenselliği, formalizasyonu da bilişim alanındaki tanım sorununun ve bu alandaki suçların çeşitliliğinin esas sebeplerindendir.[19] Dünya tarihinde hiç görülmemiş bir hızla gelişen teknoloji alanında bugün son derece önemli kabul edilen bir teknolojik ürün, bir yıl sonra çok eski ve sıradan bir hal alabilir. Bu alandaki düzenlemeler ne kadar kapsamlı olursa olsun, anılan sebeplerden ötürü ileride yetersiz kalacağından kanun koyucular kanunları, bilişim teknolojilerinde gerçekleşecek yeniliklere açık hale getirebilmek amacıyla, bu suçlara dair düzenlemelerde genellemeler, betimlemeler yapma seviyesinde kalmakla yetinmiş ayrıntılı düzenlemeler yapmamıştır.[20]

1.2. Bilgisayar

Gündelik hayatın neredeyse her alanında karşılaştığımız bilgisayarlar, ilk olarak 1800'lü yılların başında kullanılmaya başlanmıştır. Fakat, 1800'lü yılların başında ortaya çıkan bu bilgisayarlar şu an kullanılanlara göre oldukça basit ve kullanım amaçları açısından da farklıdır. Günümüzdeki bilgisayarların mucidinin, 1941 yılında programları ve verileri depolama işlevine sahip, Z3 isimli elektronik ikili sayı sistemini kullanan bilgisayarı yapan Alman bir mühendis olan Konrad Zuse olduğu söylenebilir. Daha sonraki süreçte ise sahibine, önceden bir kişi tarafından yapılması mümkün olmayan işlemleri kolaylıkla yapabilen güçlü bir makineyi yönetme imkanı sunan kişisel bilgisayarlar ortaya çıkmıştır. Bu sayede büyük, pahalı ve merkezileşmiş bilgisayarların yerini küçük, ucuz ve her evde kendi başına çalışabilen bilgisayarlar almıştır. Ayrıca kişisel bilgisayarların yaygınlaşmasıyla birlikte global bir bilgisayar ağı

[18]Ayrıntılı bilgi için bkz. U. Sieber (2013). Bilgisayar Suçluluğu. Y. Ünver (Ed.), *İnternet Hukuku*. (Çev: Y. Ünver), içinde (s. 13-57). Ankara: Seçkin Yayınevi, s. 19.
[19]E.D. Aydın (1992). *Bilişim Suçları ve Hukukuna Giriş*. Ankara: Doruk Yayınevi, s. 15-16.
[20]Ö.U. Eker (2006). "Türk Ceza Hukuku'nda Bilişim Suçları" Eski TCK Bağlamında Hukukumuzda Yer Alan İlk Düzenlemeler ve 5237 Sayılı Yeni Türk Ceza Kanunu'nun İlgili Hükümlerinin Yorumu. *TBB Dergisi,* (62), s. 103.; Y. Ersoy (1994). Genel Hukuki Koruma Çerçevesinde Bilişim Suçları. *AÜSBFD*, 49 (3-4), s. 153.; F. Erem (1991). Bilgisayar Suçları ve Türk Ceza Kanunu. *Yargıtay Dergisi*, 17 (4), s. 439.

oluşmuştur. Çağımızda ise bu bilgisayar ağı gelişimini sürdürmektedir. Bilgisayar ağının gelişmesi de yeni suç işleme yöntemlerini ortaya çıkarmıştır.[21]

Bilişim alanıyla ilgili günlük kullanımda ve uygulamada sıklıkla karşılaşıldığı üzere, bilgisayar ile bilişim sistemi kavramları birbirinin yerine kullanılmaktadır. Fakat, Bilişim terimi, bilgisayara göre daha geniş bir kavramdır.[22] Bilgisayar, bilgi toplayan ve bunları işleme tabi tutup sonuç gösteren bir sistemi, bir makineyi ifade eder.[23] Bilgisayar, kendisine yüklenen programlar aracılığıyla verileri depolama, işleme tabi tutma, başka bir yere nakletme, bu verilerden bazı sonuçlar çıkarma, aritmetik ve mantık işlemleri yaparak çalışabilme özelliğine sahiptir.[24] Kısaca bilgisayar, bir veya birden fazla görevi yerine getirmek için oluşturulmuş parçalar bütünüdür.[25] Bilişim, bilgisayarın yanı sıra, bilgisayar destekli cihazları ve diğer elektronik manyetik sistemleri kapsadığı gibi; sadece veri işlemi ve depolanmasını değil, ayrıca veri iletişimini de kapsamaktadır.[26] Buna göre, bilgisayar, bilişim sistemi için bir tür araçtır. Bilişim; bilgisayardan da faydalanarak bilgiyi saklayan, ileten ve bunları kullanmak amacıyla işleme tabi tutan sistemi konu alan akademik disiplindir.[27]

1.3. İnternet

İnternet international ve network sözcüklerinin birleşimiyle oluşmuştur ve "uluslararası ağ" anlamına gelmektedir.[28] İnternet, insanların dünya üzerinde bilgi paylaşımını sağlayan ve sürekli büyümekte olan bir iletişim yapısıdır.[29] İnternet sistemine bağlı binlerce ağ ve bu ağlara bağlı da milyonlarca bilgisayar bulunmaktadır.

---

[21]E. Casey. (2011). *Digital Evidence and Computer Crime Forensic Science, Computers and Internet*. Cambridge, Massachusetts: Academic Press, s. 437-439.; Bilgisayarın tarihçesi ile ilgili ayrıntılı bilgi için bkz. O. Değirmenci (2014). *Ceza Muhakemesinde Sayısal (Dijital) Delil*. Ankara: Seçkin Yayınevi, s. 41-44.; M. Topaloğlu (2005). *Bilişim Hukuku*. Adana: Karahan Kitabevi, s. 1-3.

[22]Ayrıntılı bilgi için bkz. V.Ö. Özbek, K. Doğan, P. Bacaksız ve İ. Tepe (2016). *Türk Ceza Hukuku Özel Hükümler*. (10. Baskı) Ankara: Seçkin Yayınevi, s. 966-967.; M. Koca ve İ. Üzülmez (2016). *Türk Ceza Hukuku Özel Hükümler*. (3. Baskı). Ankara: Adalet Yayınevi, s. 810-811.; K. Doğan (2005). Bilişim Suçları ve Yeni Türk Ceza Kanunu. *Hukuk ve Adalet Eleştirel Hukuk Dergisi*. (6-7), s. 293.

[23]İ. Biçkin (2006). Siber Suç Sözleşmesi ve 5237 Sayılı Türk Ceza Kanunu'nda Bilişim Suçları. *Yargıtay Dergisi*, 32 (1-2), s. 153.; Ersoy, 1994, a.g.k., 150.; H. Oğuz (2010). *İnternet Ortamında Kişilik Haklarının İhlali ve Korunması*. Ankara: Adalet Yayınevi, s., 25.

[24]Değirmenci, 2014, a.g.k., 34-35; Özen ve Baştürk, 2011, a.g.k., 10-11.

[25]Topaloğlu, 2014, a.g.k., 25.

[26]Eker, 2006, a.g.k., 104.; Bilişim sistemi teriminin en temel yansıması bilgisayarlardır. Bilgisayarı, diğer otomatik işlem yapan araçlardan ayırt eden özellik bilgileri otomatik olarak işleme tabi tutmasının yanında genel kapsamlı olarak verileri işleyebilme ve kullanabilmesidir. Bkz. Karakehya, 2009, a.g.k. 8.

[27]R.Y. Yazıcıoğlu (1997). *Bilgisayar Suçları Kriminolojik, Sosyolojik ve Hukuki Boyutları İle*. İstanbul: Alfa Yayınevi, s. 130.

[28]Oğuz, 2010, a.g.k., 26; Özen ve Baştürk'e göre, internet İnterconnected Networks (kendi aralarında bağlantılı ağlar) ifadesinin kısaltılmış biçimidir. bkz. Özen ve Baştürk, 2011, a.g.k., 13.

[29]Oğuz, 2010, a.g.k., 26

Böylece, internet temel fonksiyonu olan çift yönlü bilgi aktarımını sağlamaktadır. Uluslararası ağa bağlı iki bilgisayar arasında çift yönlü olarak mesaj, dosya, program, resim vb. aktarımı gerçekleştirilmektedir.[30]

Dünya üzerinde internet, ilk kez askeri nedenlerle Amerika'da ortaya çıkmıştır. Amerikan savunma bakanlığı bilgisayar ve askeri araştırma projelerini geliştirmek maksadıyla ARPANET (Advanced Research Project Agency Network) adında bir ağ kurmuş, bu ağ daha sonra Amerika'daki üniversiteler ile araştırma kuruluşlarının dahil olmasıyla büyümüştür. 1983'te ARPANET kullanıcıları iletim kontrol/internet protokolü adında yeni bir protokole geçiş yapmışlardır. 1990 yılında ise ARPANET tamamıyla kullanımdan kaldırılmıştır. ilerleyen yıllarda yerel düzeyde kullanıma imkan sağlayan ARPANET ağının yerini her geçen gün büyüyen ve tüm dünyada kullanılabilen internet ağı almıştır.[31] Türkiye'de ise ilk internet bağlantısı 1993 tarihinde ODTÜ (Ortadoğu Teknik Üniversitesi)'de gerçekleştirilmiştir.[32]

İnternet günümüzde film izlemek, müzik dinlemek, e-posta göndermek, otobüs, uçak, tren, sinema, tiyatro bileti almak, fatura yatırmak, alışveriş yapmak, gazete, dergi, kitap, haber okumak gibi burada sadece birkaç tanesini sayabileceğimiz birçok amaç için kullanılmaktadır.

1.4. Program

Program, yazılımın bir parçası sayılabilir ve programcı tarafından programlama dilinde yazılmış mantıklı ve anlamlı komutlar bütünü şeklinde tanımlanabilir. Program ya bir problemi çözmekte ya da verilerin işlenmesini sağlamaktadır.[33] Bilgisayar programları, Fikir ve Sanat Eserleri Kanunu'nun 1/B-g maddesinde "bir bilgisayar sistemini özel bir işlem veya görev yapmasını sağlayacak bir şekilde düzene konulmuş bilgisayar emir dizgesini ve bu emir dizgesinin oluşum ve gelişimini sağlayan hazırlık çalışması" şeklinde tanımlanmıştır. Bilgisayar programları, bilgisayarın somut unsuru olan donanımın yanında cihazın işlevini gerçekleştirmesini sağlayan soyut bir bileşeni sayılabilir.[34] Aslında, bilgisayar programlarının, bilgisayarın soyut unsurunu oluşturan

[30]H. Sınar (2001). *İnternet ve Ceza Hukuku*. İstanbul: Beta Yayınevi, s. 33.
[31]İnternetin tarihçesi ile ilgili ayrıntılı bilgi için bkz. Sınar, 2001, a.g.k., 22-23.;
http://bidb.itu.edu.tr/seyirdefteri/blog/2013/09/07/internet'in-tarih%C3%A7esi (Erişim Tarihi: 26.01.2017)
[32]Sınar, 2001, a.g.k., 111.
[33]Topaloğlu, 2014, a.g.k., 25.
[34]R.Y. Yazıcıoğlu, (2009). *Fikri Mülkiyet Hukukundan Kaynaklanan Suçlar*. İstanbul: XII Levha Yayıncılık, s. 82.

ve onun işlevini yapmasını sağlayan yazılımlar olduğu söylenebilir. Bu programlar bir programlama dili kullanılarak yazılmaktadır. Bilgisayarların yanı sıra işlevini yerine getirebilmek için neredeyse tüm elektronik cihazlar program barındırır. Bilgisayar programları yazılırken, bu programların istenilen fonksiyonu yerine getirebilmesini temin edebilecek çok çeşitli programlama dilleri kullanılabilmektedir.[35]

1.5. Veri

Veri kavramı, bir araştırmada, tartışmada, akıl yürütmede sonuca ulaşabilmek için gereken ilk bilgi olarak tanımlanabilir. 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun'un 2/1-k maddesinde veri, "bilgisayar tarafından üzerinde işlem yapılabilen her türlü değer" olarak tanımlanmıştır. Veri, bilişim sistemlerinin üzerinde işlem yapabilme, yapılan bu işlemlere bağlı olarak sonuçlar üretebilme, saklayabilme ve diğer bilişim sistemlerine iletebilme imkanı sağlar. Bilgisayarlar da sahip olduğu her bilgiyi sayı ya da harfler şeklinde kodlanmış veriler aracılığıyla işleme tabi tutabilir ve bu bilgileri yazılım diliyle kullanıcılarına aktarır. Bilgisayarın varlık sebebi zaten üzerine yüklenmiş olan verilerdir.[36]

Burada özellikle belirtilmelidir ki veri, sadece bilgisayar alanında değil, istatistikte, telekomünikasyonda, işletme yönetiminde de kullanılan bir kavramdır. Veri kavramı, bilgisayar verisinin yanı sıra kişisel veri[37] ya da elektronik verileri[38] de kapsamaktadır. Ancak, biz bu çalışma kapsamında veri kavramıyla bilgisayar verilerini kastetmekteyiz.

ASSS'nin 1. maddesinde bilgisayar verisi, "bilgisayar sisteminin bir işlevi yerine getirmesini mümkün kılan bir programı da kapsayan, olguların, bilgilerin veya kavramların bir bilgisayar sisteminde işlenmeye uygun haldeki her türlü temsili" olarak tanımlanmıştır. Veri özetle, bilişim sistemleri üzerinde işlenen başta bilgi olmak üzere her türlü soyut unsurdur.[39]

---

[35] http://www.emreeren.com/2005/10/bilgisayar-program-nedir.html (Erişim Tarihi: 03.07.2016).; Bilgisayar programları ile ilgili ayrıntılı bilgi için bkz. Topaloğlu, 2005, a.g.k., s.4-14.

[36] M.V. Dülger (2013). *Bilişim Suçları ve İnternet İletişim Hukuku.* (3. Baskı). Ankara: Seçkin Yayınevi, s. 71-72.

[37] 6698 sayılı Kişisel Verilerin Korunması Hakkındaki Kanun'un 3. maddesine göre kişisel veri: kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgidir.

[38] 5070 sayılı Elektronik İmza Kanunu'nun 3. maddesine göre elektronik veri: elektronik, optik veya benzeri yollarla üretilen, taşınan veya saklanan kayıtlardır.

[39] Değirmenci, 2014, a.g.k., 50.; H. Erol (2010). *Türk Ceza Kanunu Gerekçeli ve Açıklamalı*. Ankara: Yayın Matbaacılık ve Ticaret İşletmesi, s. 3748.

1.6. Bilişim Suçu

1.6.1. Bilişim suçunun tanımı

Bilişim ve bilişim sistemi kavramlarının net ve herkesin üzerinde uzlaşabileceği bir tanımının olmaması durumu bilişim suçları için de geçerlidir. İlk olarak, ABD'de ortaya çıkan ve bilgisayarın yaygınlaşmasıyla birlikte tüm dünyada meydana gelen bu tarz hukuka aykırı eylemleri nitelemek için, doktrinde bilişim suçu ifadesinin yanı sıra, bilgisayar suçu, siber suç, internet suçu, sanal suç, ileri teknoloji suçu, yüksek teknoloji suçu, bilişim sistemi aracılığıyla işlenen suç elektronik suç, dijital suç gibi ifadeler kullanılmaktadır.[40]

Bilişim suçu ifadesi, diğer isimlendirmelere göre daha geniş ve kapsayıcıdır. Nitekim doktrin ve uygulamada da genel itibariyle bu ifade kullanılmaktadır. Buna karşın bilişim suçunun tanımı konusunda farklı görüşler olduğu için doktrinde bu hususta genel bir kabul olduğunu söylemek mümkün değildir. Örneğin, Eker'e göre, "bilişim suçları; bilişim araçlarına/sistemlerine karşı veya bilişim araçları/sistemleri vasıtasıyla işlenen verilerle, veri işlem ile veri aktarımıyla ilgili olan suç şekilleridir".[41] Karagülmez'e göre, "bilişim suçları; bilişim sistemine yönelik veya bilişim sisteminin kullanıldığı suç olarak tanımlanabilir".[42] Dülger'e göre, "bilişim suçu; verilere karşı ve/veya veri işlemle bağlantısı olan sistemlere karşı, bilişim sistemleri aracılığıyla işlenen suçlardır".[43] Katyal'a göre, "bilişim suçu; bir saldırı gerçekleştirmeyi kolaylaştırmak amacıyla bilgisayarın kullanıldığı suçlardır. Bu tarz suçlar, bilgisayar programlarına ve dosyalarına yetkisiz erişmek, bu dosya ve programları yine yetkisi olmaksızın bozmak ya da değiştirmek ve elektronik kimliği çalmak gibi üç farklı yolla işlenebilir".[44] Uluslararası alanda bilişim suçlarının ilk resmi tanımını, Avrupa Ekonomik Topluluğu Uzmanlar Komisyonu yapmıştır. 1983'te Paris'te toplanan komisyon bilişim suçunu, "bilgileri otomatik işleme tabi tutan veya verilerin nakline yarayan bir sistemde gayri kanuni gayri ahlaki veya yetki dışı gerçekleştirilen her türlü

[40]H. Akarslan (2012). *Bilişim Suçları*. Ankara: Seçkin Yayınevi, s. 33.; Yenidünya ve Değirmenci, 2003, a.g.k., 111.; Yazıcıoğlu, 1997, a.g.k. 125.; Biçkin, 2006, a.g.k., 147.
[41]Eker, 2006, a.g.k., 105.
[42]Karagülmez, 2009, a.g.k., 38.
[43]Dülger, 2004, a.g.k., 67.
[44]N.K. Katyal (2001). Criminal Law in Cyberspace. *University Of Pennsylvania Law Review*, (149). s. 1013.

davranış" olarak tanımlamıştır.[45]

Bilişim suçları, genel itibariyle beyaz yaka suçları olarak ifade edilmektedir. Beyaz yaka suçları, şiddet içermeyen ve genelde suçlunun mesleğinden ötürü sahip olduğu birtakım yetkilerini kötüye kullanması sonucu ortaya çıkan suç kategorisidir.[46] Bilişim suçluları da mesleklerinden ya da özel ilgilerinden dolayı bilişim teknolojileri alanında genel olarak uzman kişilerdir. Bunun yanı sıra, bilişim suçları, genel itibariyle ekonomik amaçlarla işlenmektedir ve suçlular çoğunlukla organize çalışmaktadırlar. Nitekim, 765 sayılı TCK'da bu suç tipi mala karşı cürümler bölümünde düzenlenmiştir.[47]

Bilişim araçlarından en yaygınının bilgisayar olması bilişim suçlarına bilgisayar suçu denilmesinin esas sebebidir.[48] Oldukça geniş kapsamlı olan bilgisayar suçluluğu, bilgisayar sistemlerine olan güvene, bu sistemlerin bütünlüğüne ve tasarruf edilebilirliğine karşı yapılan saldırı anlamına gelmektedir.[49] Bilişim suçunun bilgisayar suçu olarak ifade ediliyor olmasının bir başka sebebi de bu suçların Amerika'da ortaya çıkması sonucu Amerikan doktrininde yaygın olarak kullanılan computer crime (bilgisayar suçu) ifadesinin başka ülkelerdeki hukukçular tarafından da benimsenmesidir.[50]

Bilişim suçu, bilgisayarın yanı sıra elektronik araçlardan olan cep telefonları, üzerindeki web paneli sayesinde ağa bağlanabilen elektronik ev aletleri, bankamatikler, radyo dalgalarını algılayabilen cihazlar vb. araçlarla da işlenebileceğinden bilgisayar suçu kavramı yetersiz kalmaktadır. Bu tür eylemlere bilişim suçu demek daha isabetlidir.[51]

---

[45]O. Yaşar, H.T. Gökcan ve M. Artuç (2010). *Yorumlu - Uygulamalı Türk Ceza Kanunu Cilt V Madde 205-256*. Ankara: Adalet Yayınevi, s. 6735.
[46]Eker, 2006, a.g.k., 105.
[47]H. Akarslan (2015). *Bilişim Suçları*. Ankara: Seçkin Yayınevi, s. 36.
[48]Ersoy, 1994, a.g.k., 151.
[49]Sieber, 2013, a.g.k., 16.
[50]M.E. Artuk, A.Gökçen ve A.C. Yenidünya (2009). *TCK Şerhi Özel Hükümler Madde 235-345 5. Cilt*. Ankara: Turhan Kitabevi, s. 4628.; M.E. Artuk, A. Gökçen ve A.C. Yenidünya (2015). *Ceza Hukuku Özel Hükümler*. (15. Baskı). Ankara: Adalet Yayınevi, s. 674
[51]Yenidünya ve Değirmenci, 2003, a.g.k., 31.; Biçkin, 2006, a.g.k. 146.; Benzer bir görüş için bkz. Ünver, Y. (2001). Türk Ceza Kanunu'nun ve Ceza Kanunu Tasarısının İnternet Açısından Değerlendirilmesi. *İÜHFM*, 59(1-2), s. 78-79.

1.6.2. Bilişim suçlarının tasnifi

Bilişim suçunun tasnifi yapılırken, genellikle doğrudan bilişim sistemine yönelen eylemler ve bilişim sistemi araç olarak kullanılarak işlenen diğer suçlar olarak ikili bir ayrım yapılmaktadır.

Bilişim suçlarına dair yapılan üçlü bir tasnife göre; "bilişim suçu, bilgisayarın bir suçta amaç olarak kullanılmasıyla ve failin odak noktasının bilgisayar olmasıyla ya da bilgisayarın bir suçun esas konusu olması suretiyle suçun kaynağı veya nedeni olmasıyla veyahut bilgisayarın bir suçun aracı olmasıyla işlenebilir".[52] Başka bir tasnife göre; "bilişim suçu, bilişim sistemlerine karşı suçlar, bilişim sistemleri ile işlenen suçlar, bilişim araçlarına karşı suçlar olmak üzere üç şekilde karşımıza çıkmaktadır."[53] Bir diğer tasnife göre ise "bilişim suçları, bilgisayar sistemi içinde işlenenler ve bilgisayara karşı işlenenler veya bilgisayar programlarının güvenliğini koruyacak suçlar ve teknik aracın kendisini korumak amacını güden suçlar olarak karşımıza çıkmaktadır."[54]

Bilişim suçunu ikili tasnife tabi tutanlar da vardır. Örneğin Akarslan'a göre; "bilişim suçu, bilişim teknolojilerinin amaç ve araç olarak kullanılmasına göre bilişim yoluyla işlenen suçlar ve bilişim suçları şeklinde ifade edilebilir".[55] Aydın'a göre; "bilişim suçları, bilişim sistemine karşı işlenen suçlar, bilişim sistemleri ile işlenen suçlar şeklinde iki ayrı düzeydedir".[56] Bakıcı ve Tarhan'a göre; "bilişim suçu, doğrudan bilişim suçu (gerçek bilişim suçu) ve dolayısıyla bilişim suçu (bilişim bağlantılı suç) şeklinde ifade edilmiş ve doğrudan bilişim suçunun TCK 243 ila 245. maddeler arasında düzenlendiği dolayısıyla bilişim suçu ise klasik suçların[57] bilişim sistemi marifetiyle işlenmesi anlamına geldiği belirtilmiştir."[58] Siber suçlar ifadesini kullanan Sınar'a göre ise "bilişim sistemindeki suçlar, internet aracılığıyla gerçekleştirilen suçlar ve internete

[52]Karagülmez, 2009, a.g.k., 51.
[53]Ersoy, 1994, a.g.k., 160-161.; Ayrıca benzer görüş için bkz. Mahmutoğlu, 856.
[54]S. Dönmezer (1995). *Kişilere ve Mala Karşı Cürümler*. (14. Bası). İstanbul: Beta Yayınevi, s. 505.
[55]Akarslan, 2015, a.g.k., 40.
[56]Aydın, 1992, a.g.k., 27.; Aydın'a göre, izinsiz olarak bilgisayara dayalı kişisel dosyanın açılması veya tutulması, bilgi hırsızlığına karşı koruma ile ilgili kanunların ihlal edilmesi, kişisel bilgiler verilmesi, bilgi tecavüzü gibi durumlar da bilişim suçu olarak kabul edilmelidir.
[57]Klasik suçlardan kasıt, geçmişten günümüze kadar hukuki dayanaklarıyla birlikte cezai yaptırımları olan adam öldürme, yaralama, hırsızlık, kundaklama, gasp, tehdit gibi suçlardır. Bkz. Akarslan, 2015, a.g.k. 36.
[58]Yargıtay Ceza Genel Kurulu'nun 17.11.2009 tarih ve 2009/11-193 Esas ve 2009/268 Karar sayılı kararında bahsedilen Sedat Bakıcı ile Saniye Tarhan'a ait muhalefet şerhi. Yine bu kararda bilişim sistemlerinden yararlanılarak TCK'nın 112, 113., 125., 132., 133., 134., 135., 136., 138., 142/2-e, 158/1-f, 213., 214., 215., 216., 217., 218., 226 ve 228. maddelerindeki suçların işlenebileceği belirtilmiştir.

özgü suçlar olarak ikiye ayrılmaktadır."[59]

ASSS'de bilişim suçu, bilgisayar sistemlerinin gizliliğine karşı suçlar bilgisayarla ilişkili suçlar, içerikle ilişkili suçlar ve fikri mülkiyet hakkının ihlaline ilişkin suçlar şeklinde tasnif edilmiştir.[60] ASSS'de yapılan tasnifte, bilişim sisteminin araç olarak kullanılması suretiyle klasik suçların işlenmesi yerine bilgisayarla ilişkili suç ifadesi kullanılmıştır. TCK sistematiği de incelendiğinde, bilişim alanında suçların ayrı bir başlık altında düzenlendiği görülmektedir ve kanunda bilişim sisteminin araç olarak kullanılması suretiyle diğer klasik suç tiplerinin gerçekleştirilmesi sadece klasik suçu nitelikli unsur yapan bir durum olarak düzenlenmiştir. Böylece, örneğin TCK'da düzenlenen hırsızlık suçunun, bilişim suretiyle işlenmesi ile yine aynı maddede düzenlenen haksız yere elde bulundurulan veya taklit anahtar kullanmak suretiyle işlenmesi arasında bu açıdan bir farklılık görülmemektedir. Kanunun bu düzenlemesini eleştiren yazarlar da vardır.[61]

Kanımızca, bilişim suçları ikili tasnife tabi tutmak daha isabetlidir. Buna göre, bilişim sistemlerine yönelik ihlal hareketleri doğrudan bilişim suçu olarak, bilişim sistemleri araç olarak kullanılarak klasik suçların işlenmesi ise dolaylı bilişim suçu olarak kabul edilmelidir.

1.6.3. Bilişim suçlarının işlenme sebepleri

Bilişim suçları, klasik suçlara göre işlenme sebepleri açısından farklılık gösterir. Bilişim suçlarını klasik suçlardan ayıran özelliği olan bilişim sisteminin olanaklarının fazlalığı ve hayal sınırlarının ötesinde bir alan olması, bilişim suçu faillerine geniş bir hareket alanı sunmaktadır. Ayrıca, bu failler suçun yargı organlarınca takibinin ve yapılacak soruşturmalarda aleyhlerinde yeterli delil bulunmasının zorluğunu bildikleri için çok daha rahat davranmaktadırlar.[62]

Bilişim suçları, klasik suç tiplerine göre suçun maddi unsurunu oluşturan fiiller bakımından farklılık arz etmektedir. Klasik suç tiplerindeki hileli hareket etmek

[59]Sınar, 2001, a.g.k., 78, 119-120.
[60]Akarslan, 2015, a.g.k., 38.
[61]O. Değirmenci (2005). 2004 Türk Ceza Kanunu'nun Bilişim Suçları Bakımından Değerlendirilmesi. *TBB Dergisi*, (58), s. 201, 208.
[62]Karagülmez, 2009, a.g.k., 44-45.; F.S. Akıncı (2001). Avrupa Konseyi Siber Suç Sözleşmesinde Yer Alan Maddi Ceza Hukukuna İlişkin Düzenlemeler ve Özellikle İnternette Çocuk Pornografisi. *İÜHFM.* 59 (1-2), s. 11-12.; M.T. Yücel (1992). Bilişim Suçları, *Ankara Barosu Dergisi*, (4), s. 505-507.

(dolandırıcılık TCK m.157), mevcut bir belgeyi değiştirmek (resmi ya da özel belgede sahtecilik TCK m.204, TCK m.207), taşınır malı bulunduğu yerden zilyedin rızası olmaksızın almak (hırsızlık TCK m.141) gibi fiillerin yerine bilişim suçlarında genellikle failin bilgisayar klavyesini kullanmak dışında dış dünyaya yansıyan bir fiili bulunmamaktadır. Fakat, bu basit sayılabilecek fiilden ötürü klasik suçlar sonucu oluşacak zararın çok daha fazlası meydana getirilebilmektedir.[63]

Bilişim suçu faillerini suç işlemeye iten sebep olarak, intikam duygusu, meydan okuma, kendini kanıtlama, hırs vb. faktörler gösterilebilir.[64] Bunun yanı sıra, bilişim suçu örneğin, öğrencinin okuduğu okuldaki programa girerek kendi notunu değiştirmesi şeklinde de işlenebilir[65] ya da California'da bir hastanede yatan hastanın, hastanenin bilgisayar sistemine girerek reçetesini sırf eğlence olsun diye değiştirmesi şeklinde de olabilir. [66] Görüldüğü gibi, bilişim suçu, sadece maddi yarar sağlamak için işlenmemektedir.

Bilişim suçu failleri, klasik suç faillerine göre daha nitelikli bireylerdir. Bu kişiler, bilgisayar teknolojilerini ve bilgi işlemi patronlarından ya da amirlerinden çok daha iyi bilirler ve yüksek düzeyde entelektüel davranışlar sergileyebilme yeteneğine sahiptirler. Bilişim suçu faillerinin böyle nitelikli bireyler olması bu suçlarla mücadeleyi de güçleştirmektedir.[67]

1.6.4. Bilişim suçlarının işlenme şekilleri

1.6.4.1. Genel olarak

Bilişim alanı, zaman içerisinde genişleyen ve yeni özellikler kazanan bir alan olduğundan dolayı bilişim suçlarının nasıl ve ne şekilde işlendiği klasik suçların aksine tam olarak bilinememektedir ve anlatılan suç işleme şekilleri bugüne kadar gerçekleşmiş eylemlerin sınıflandırılmasından ibarettir. Failler, her geçen gün yeni bir taktik geliştirmektedirler. Zaten böylesine dinamik bir alanda kesin olarak değerlendirme yapmak, bu tarz suçlarla mücadelede baştan dezavantajlı duruma düşmek anlamına gelir.[68]

[63]Dülger, 2004, a.g.k., 69.; Yücel, 1992, a.g.k., 506-507.
[64]Karagülmez, 2009, a.g.k., 44-45.
[65]Ersoy, 1994, a.g.k., 158.
[66]H. Dursun (1998). Bilgisayar İle İlgili Suçlar, *Yargıtay Dergisi*, 24 (3), s. 336.
[67]Aydın, 1992, a.g.k., 131.
[68]Yazıcıoğlu, 1997, a.g.k., 151-152

Bilişim sisteminin savunma düzeyinin düşük olması da suç işleme yöntemlerini çoğaltmaktadır. Failler "d" harfiyle ifade edilebilecek ve neredeyse her gün medyaya örnekleri yansıyan destroy, damage, deny, delay, deceive, disrupt, distort, degrade, disable, divulge, disconnect ve disguise şeklinde birçok olumsuz eylemi bilişim alanında gerçekleştirebilirler.[69] [70]

Bilişim suçlarının işlenme şekillerine yönelik bugüne kadar uygulamada çok çeşitli yöntemlerle karşılaşılmıştır.[71] Bilişim teknolojilerinin her geçen gün süratle gelişmesi sonucu yeni suç işleme yöntemleri ortaya çıkmaktadır. Dolayısıyla, bilişim suçu işleme şekillerinin tümünün biliniyor olduğunu söylemek yanlış bir değerlendirme olacaktır. Bunun yerine bugün için en sık görülen yöntemleri anlatmak daha uygundur. Bu sık karşılaşılan yöntemler, truva atı (trojan horse), salam tekniği, hacking, ağ solucanları (network worms), tavşanlar (rabbits), bukalemunlar (chameleons), mantık bombaları (logic bombs), virüsler, istem dışı alınan elektronik postalar (spam), bilgi aldatmacasıdır.[72]

Günümüzde failler, bilişim suçlarını genellikle amaçlarına uygun olarak oluşturdukları programlar aracılığıyla işlemektedir. Uygulamada bu zararlı programlara vandal ware (yıkıcı yazılımlar) adı verilmektedir. Failler, bu zararlı programlar aracılığıyla bilişim sistemine istedikleri gibi girebilirler ve sistemdeki veriler üzerinde değişiklik yapabilirler.[73]

1.6.4.2. Truva atı

Truva atı, ismini, aynı yöntem ve planla çalıştığından dolayı, herkesçe bilinen

[69]https://www.itu.int/osg/spu/visions/papers/securitypaper.pdf (Erişim Tarihi: 03.07.2016)
[70]Kelimelerin Türkçeleri sırasıyla şöyledir: yok etmek, zarar vermek, mahrum etmek, ertelemek, kandırmak, bozmak, biçimini bozmak, kalitesini azaltmak, geçersiz kılmak, açığa vurmak, bağlantıyı koparmak, kendisini gizlemek.
[71]Akarslan'a göre bu yöntemler şunlardır; zararlı yazılımlar, bilgisayar virüsleri, bilgisayar solucanları, truva atları, casus yazılımlar ya da reklam yazılımları, kök kullanıcı takımı (rootkit), mantık bombaları (yazılım bombaları-zaman bombaları), bukalemunlar-tavşanlar, gizli arka kapılar (back doors), yemleme-oltalama yöntemi (phishing), tarama (scanning), şifre kırıcılar, sos saldırıları ve köle bilgisayarlar, gizlice dinleme-ağı koklama (sniffing), sahte-istenmeyen elektronik postalar, sahte kişilik oluşturma ve kişilik taklidi yoluyla dolandırıcılık, hile-aldatma (spoofing), sosyal mühendislik, bilişim korsanları ve sistem kırıcılar, telefon kırıcı (phreaker), özenti (lamer), betik kerataları (script kiddie), çaylak (newbie), eylemci bilişim korsanı (hactivist). Bkz. Akarslan, 2015, a.g.k., 87-108.; Aydın ise bu yöntemleri şu şekilde saymıştır: bilgi aldatmacası, truva atı, salam tekniği, süper darbe, kapan kapakları, lojik bombaları, senkronize saldırı, leşçilik, veri sızdırma, yankesicilik, taklit, tel salma, simülasyon, modelleme. Bkz. Aydın, 1992, a.g.k., 128.
[72]Dülger, 2004, a.g.k., 69-77.
[73]B.B. Akbulut (2000). Bilişim Suçları. *SÜHFD*, 7 (1-2), s. 551.

tarihi Truva atından [74] almaktadır. [75] Truva atı (Trojan), kelime anlamı olarak bilgisayar yazılımı bağlamında zararlı program barındıran veya yükleyen programdır. En tanınan Truva atları ise Sub7, Poison Ivy, Bifrost, Pandora RAT (Türk yapımı), Prorat (Türk yapımı), JRat'tır. Truva atları, diğer kötücül yazılımlar ve bilgisayar solucanı ve virüsleri gibi kendi başlarına işlem yapamazlar. Bu yöntemin kullanıldığı alanlar oldukça geniştir, yetkisiz olarak bilişim sistemine girmek, verileri hukuka aykırı olarak elde etmek, hukuka aykırı yarar sağlamak, kişilere ve verilere zarar vermek gibi birçok eylem bu yöntem sayesinde gerçekleştirilebilir.[76] Truva atı, genel olarak yazılım programına yerleştirilmektedir. Fakat 1980'lerin başında İsveç'te yapıldığı gibi donanıma da yerleştirilebilmektedir.[77]

Truva atı yöntemine örnek olarak, Thompson adındaki bir bilgisayar programcısının eylemi gösterilebilir. Thompson, bir Kuveyt bankasında bilgisayar programcısı olarak çalışmakta iken, bankanın bilgisayar sistemine, uzun zamandır işlem görmeyen hesapları tespit ettikten sonra bu hesaplardan kendisinin yine aynı bankada açtığı hesaba havale yapması talimatını vermiştir. Ayrıca, bu programa verdiği talimat uyarınca program Thompson'un, Kuveyt'te görevi bitip İngiltere'ye döndükten sonra devreye girecek ve işlemler gerçekleştikten sonra da program kendi kendisini yok edecektir. Bu planın ilk kısmı, yani hesaplar arası havale başarıyla gerçekleştirilmiş ve Thompson 45000 Sterlini hesabına geçirtmiştir. Fakat bu işlemler bittikten sonra program kendisini silmemiş ve Thompson bu olaydan ötürü dolandırıcılık suçundan mahkum olmuştur.[78]

1.6.4.3. Salam tekniği

Çoğunlukla bankacılık sisteminde kullanılmakta olan bu yöntem bilginin manipüle edilmesi temeline dayanır. Bu yöntemle banka hesaplarının virgülden sonraki bir ya da iki hanesindeki önemsenmeyen meblağlar (küsuratlar) failin belirlediği başka bir hesaba aktarılarak orada biriktirilmektedir. Tek bir hesap açısından bakıldığında, çok küçük meblağ gibi gözükse bile günümüzde bankacılık sisteminin büyüklüğü ve

[74]Tarihi truva olayı, Truva Savaşı'nda kullanılan tahta atın hediye olarak Truvalılara gönderilmesi ve tahta atın kalenin içine girdikten sonra atın içine gizlenen düşman askerlerinin kaleyi ele geçirmesidir. Bkz. Avşar ve Öngören, 2010, a.g.k., 49.
[75]Akarslan, 2015, a.g.k., 91.
[76]Dülger, 2004, a.g.k., 70.
[77]Katyal, 2001, a.g.k., 1026.
[78]Ersoy, 1994, a.g.k., 172.; Bir başka örnek için bkz. Yazıcıoğlu, 1997, a.g.k., 151.

bankalarda milyonlarca müşteri mevduat hesabı olduğu göz önünde tutulursa bu fiiller sonucu elde edilecek meblağların inanılmaz boyutlara ulaşacağı bir gerçektir.[79]

1.6.4.4. Hacking

Hacking, bir bilgisayar sistemine bilgi veya program elde etmek ya da sisteme zarar vermek amacıyla yetkisiz erişim sağlamaktır.[80] Başkasına ait bilgisayar sistemine haksız şekilde giren hackerler, sisteme teknik etkide bulunmakta ve verileri ele geçirmeye çalışmaktadırlar.[81] Hacker kelimesi, yeni bir program ortaya çıkarılması ya da var olan programda değişiklik yapılması anlamında kullanılan hacking kelimesinden türetilmiştir. Hackerlara bilgisayar korsanı ya da bilişim korsanı da denmektedir.[82]

Hackerlar, kültür ve bilgi düzeyi yüksek, programcılık deneyimine sahip ayrıca konusunda iyi eğitim almış kişilerdir.[83] Bu kişiler, nitelikli ve donanımlı oldukları için yaptıkları eylemi çoğu zaman suç işlemek kastıyla gerçekleştirmemektedirler. Örneğin, bazı hackerlar, aşırı merak, kendini tatmin etme, kendi başına bir şeyleri başarma, kendine güven gibi olumlu güdülerle sosyal güvenlik veya okul bilgi sistemlerindeki verileri değiştirmek tarzında eylemlerde bulunmaktadır. Bu kişiler, amatör hackerlar olarak bilinen ve zararsız sayılan kişilerdir. Fakat bunun yanı sıra, intikam alma, güce sahip olma, açgözlülük, şehvet, macera, yasak meyveyi tatma arzusu ya da maddi menfaat temin etme gibi geleneksel suç işleme nedenleriyle hareket eden hackerlar da vardır. Bunlar, örgütlü hackerlardır ve en tehlikeli grup olarak nitelendirilirler ve diğer hackerlara göre çok daha yeteneklidirler. Bu grup devlete karşı politik eylemlere de girişmektedir.[84] 2004 yılında TBMM üyelerinin maillerinin hack edildiğini iddia eden mail gönderilmesi, Redhack grubunun Osmanlıspor ile Ankara Şehirlerarası Terminal İşletmesi'nin internet sitelerini hack etmesi, 50 milyon kişinin kimlik bilgilerinin hack edilmesi olayları hacking faaliyetlerine örnek olarak verilebilir.[85]

---

[79] http://novellaqalive2.mhhe.com/sites/dl/free/0073195553/462568/Chapter14.pdf (Erişim Tarihi: 16.05.2017).; Yazıcıoğlu, 1997, a.g.k. 155.; Aydın, 1992, a.g.k., 47.
[80]Ünver, 2001, a.g.k., 107.
[81]Sieber, 2014, a.g.k., 30.
[82]Karagülmez, 2009, a.g.k., 68-69.
[83]Akarslan, 2015, a.g.k., 104.
[84]http://teknolojibilimmerkezi.tr.gg/dokuman-tr.htm (Erişim Tarihi: 18.05.2016).; Yazıcıoğlu,1997, a.g.k. 155.; Aydın, 1992, a.g.k., 47.; http://novellaqalive2.mhhe.com/sites/dl/free/0073195553/462568/Chapter14.pdf (Erişim Tarihi: 16.05.2017)
[85]http://arsiv.ntv.com.tr/news/263321.asp#BODY (Erişim Tarihi: 01.06.2016).; http://www.mynet.com/haber/guncel/redhack-asti-ve-osmanlisporun-sitelerini-hackledi-1631129-1 (Erişim Tarihi: 01.06.2016).; http://www.milliyet.com.tr/50-milyon-kimlik-bilgisi-calindi--teknoloji-2221019/) (Erişim Tarihi: 01.06.2016)

Bilişim sisteminin çok yaygın olarak kullanılması ve her geçen gün de kullanım alanlarının artması dolayısıyla bilişim sistemini kullanan kurum ve kuruluşlar yeni birtakım önlemler almaya mecbur kalmaktadır. Bu önlemlerden bir tanesi de bilişim sisteminin güvenlik açığı olup olmadığının test edilmesi yani bir yoklama yapılması gerekliliğidir. Aslında, bu kontrol işlemini yapması gereken bilişim uzmanıdır. Fakat, bilişim uzmanının, bir hacker kadar bilişim sisteminin açığını bilebilmesi uzak ihtimaldir. Çünkü, bilişim uzmanı gerçek bir suçlunun psikolojisiyle hareket etmemektedir. Bundan dolayı da kurum ve kuruluşların hackerlarla çalışması bir zorunluluktur. Hackerlar, daha önceden suç işlemek için kullandıkları bilgi ve tecrübelerini bir anlamda artık suçları önlemek için kullanmaktadırlar. İşte bu amaç için çalışan hackerlara, ethical hacker denmektedir.[86]

Ethical hacker önleminin etkili olabilmesi bazı şartlara bağlıdır. İlk olarak ethical hacker, başarılı olmak için bazı özellikleri haiz olmalıdır. Bu kişiler, güçlü donanım ve bilgiye sahip olmalı, çok sabırlı ve inisiyatif sahibi olmalı, gelişmeleri takip edip kendisini yenilemelidir. Ayrıca kurum ve kuruluşlar tarafından da bu hackera tamamen güvenilmesi gerekmektedir.[87]

1.6.4.5. Ağ solucanları (network worms)

Ağ solucanları, virüs ve truva atı yöntemine benzetilmekle birlikte, onlardan çok daha karmaşık bir yazılım türüdür. E-posta ile gönderilen ekler, çeşitli web siteleri ve ağ üzerindeki dosyaları kullanarak yayılırlar. Solucanlar, bir bilişim sistemini ele geçirdiklerinde kullanıcının başka bir hareketine ihtiyaç duymaksızın kullanıcının veri kaynaklarını kullanarak kendi kaynak dosyalarını diğer kullanıcılara da ulaştırmak suretiyle kısa sürede çok fazla sayıda çoğalabilirler, zaten kendilerine solucan isminin verilmesinin sebebi de bu kısa süredeki çoğalma yetenekleridir. Solucanlar bunları yaparken kullanıcıların bant genişliklerini ve ağ kaynaklarını kullandıklarından ötürü, bilişim sistemi içindeki ağların kilitlenmesine ve web kaynaklarına erişimin kısıtlanmasına sebep olmaktadırlar.[88]

İnternette rastlanan ağ solucanlarına örnek olarak, tebrikler 250 sms kazandınız

[86]Karagülmez, 2009, a.g.k., 72-73.
[87]Karagülmez, 2009, a.g.k., 77-78.
[88] http://bidb.itu.edu.tr/seyirdefteri/blog/2013/09/07/vir%C3%BCs-solucan-ve-truva-at%C4%B1 (Erişim Tarihi: 03.06.2016).; Oğuz, 2010, a.g.k, 112-113.

telefonunuza indirmek için tıklayınız, tebrikler Amerika kapınızda, bugün şanslı gününüzdesiniz bizden para ödülü kazandınız tarzında yazılar, e-postalardaki ağ solucanlarına örnek olarak ise, Fidel Castro öldü, ilk defa nükleer terör saldırısı gerçekleşti, üçüncü dünya savaşı çıktı tarzında iletiler verilebilir.

1.6.4.6. Tavşanlar (rabbits)

Tavşanlar, bilgisayar virüslerinin bir türüdür. Bunlar, bilgisayar sistemine girdikten sonra sürekli ve hızlı bir şekilde çoğalırlar. Tavşanlar, yerleştikleri alanda sürekli koloniler kurarak sistemin alanını tüketirler. Amaç, özellikle çok kullanıcısı olan sistemlerde, iletişim ağ ortamlarındaki ana sistem bilgi işleme gücünü kaybedinceye kadar sistemi kurutmaktır. Böylece, sistemin bilgi işleme gücünü zayıflatırlar ve gereksiz komutlar vermek suretiyle sistemi zarara uğratırlar. Tavşanları diğer bilgisayar virüslerinden farklı kılan ise virüsler gibi asalak olmamalarıdır ve kendi kendilerine yetebilmeleridir.[89]

1.6.4.7. Bukalemunlar (chameleons)

Bukalemun adlı yazılımlar, Truva atı yöntemiyle benzerlik gösterir. Bilgisayar sistemini aldatmak suretiyle sisteme giriş yapan bukalemunlar, normal çalışan zararsız bir yazılım gibi hareket eder fakat ilerleyen süreçte gerçek kimliğini ortaya çıkarır ve zarar verici eylemlerini gerçekleştirir. Kendisini saklamaktaki hüneri dolayısıyla bu adı almıştır.[90] Bukalemun yazılımları, çok kullanıcılı sistemlerde kullanıcıların adlarını ve şifrelerini öğrenmek için giriş iletilerini taklit edebilecek şekilde programlanırlar. Bukalemunlar, kullanıcıların adlarını ve şifrelerini öğrendikten sonra bunları gizli bir dosyaya kaydeder ve sistemin bir süreliğine kapatıldığına dair bilgi verir. Bu sırada bukalemun programı yazmış olan kişi özel şifresiyle kullanıcıların adlarını ve şifrelerini içeren gizli dosyayı ele geçirir. Böylece, kişi gerekli bilgileri elde ettikten sonra sisteme zarar verici eylemlerini gerçekleştirir.[91]

1.6.4.8. Mantık bombaları (logic bombs)

Mantık bombaları aslında Truva atı yönteminin bir türüdür. Mantık bombaları, bir bilgisayar sisteminde zararlı bir eylem gerçekleştirmek amacıyla uygun durumlarda

[89]L. Kurt (2005). *Açıklamalı - İçtihatlı Tüm* Yönleriyle *Bilişim Suçları ve Türk Ceza Kanunundaki Uygulaması*. Ankara: Seçkin Yayınevi, s. 75.; Aydın 1992, a.g.k., 52.
[90]Dülger, 2004, a.g.k., 74.
[91]H. Oğuz (2010). *İnternet Ortamında Kişilik Haklarının İhlali ve Korunması*. Ankara: Adalet Yayınevi, s. 111.

veya sürekli olarak faaliyette olan bir yazılımdır ve bu yazılımın tespiti zordur. Mantık bombaları, bilgisayara ya mantık dışı ya da yapılan işlemin aksi yönde bilgiler göndermektedir. Böylece, bilgisayarın işleyişini bozabilmekte, sistemde birtakım değişiklikler yapabilmekte, hatta sistemi tamamıyla çalışamaz duruma da getirebilmektedirler.[92]

Uygun durumlarda faaliyete geçen mantık bombalarına örnek olarak, zaman bombaları örnek verilebilir. Zaman bombaları gerçek dünyadaki saatli bombalara benzemektedir. Bunlar, bilgisayar sistemine bulaştıkları anda değil zamanı geldiğinde faaliyete geçerler.[93]

Mantık bombası eylemlerine örnek olarak, bir Amerikan şirketinde EDP görevlisi olarak çalışan personelin işten çıkarılması sebebiyle şirketin manyetik arşivlerini silmesi (bu şekilde fail kendi kimlik bilgilerinin yanı sıra bütün çalışanların kimlik bilgilerini de sabote etmiştir), yine Amerika'da Los Angeles Su ve Enerji Dairesi'nde Pazartesi sabahı rutin işlerini yapmak üzere bilgisayarlarını açan EDP görevlilerinin bilgisayarlarının kilitlenmesi ve tüm çabalara rağmen açılamaması gösterilebilir. Bu olayda, bilgisayarların eski haline gelebilmesi için 20 uzman bir hafta boyunca çalışmıştır.[94] Ayrıca, mantık bombaları, para hırsızlığı, gizlice askeri bilgileri çalma, sabotaj vb. amaçlar için de kullanılabilir.[95]

1.6.4.9. Virüsler

Virüsler, kendilerini kopyalayarak çoğalabilme özelliğine sahip olan ve böylece bilgisayardaki diğer programlara bulaşarak sistemi etkileyebilen programlardır. Üremiş ya da kopyalanmış olan virüs, kendisine kaynaklık eden ana programdan da bağımsız hareket eder. Kendi kendine çoğalabilmesi ve kendisini oluşturan programdan da bağımsız hareket edebilmesi virüsleri, ağ solucanları ve truva atlarından ayıran en önemli özellikleridir.[96] Virüsler bilişim sistemi içindeki programların arzu edilmeyen şekilde çalışmasına sebep olarak bilişim sistemine zarar vermektedir.[97]

---

[92] Yazıcıoğlu, 1997, a.g.k., 157.; http://novellaqalive2.mhhe.com/sites/dl/free/0073195553/462568/Chapter14.pdf (Erişim Tarihi: 16.05.2017)
[93] Akarslan, 2015, a.g.k., 94.
[94] Yazıcıoğlu, 1997, a.g.k., 158.
[95] Dursun, 1998, a.g.k., 335.
[96] Yazıcıoğlu, 1997, a.g.k., 162-164.
[97] Sieber, 2014, a.g.k., 33.; Oğuz, 2010, a.g.k., 112.

Virüs programlarının yazılma amaçları oldukça fazladır. Bu amaçlardan bazıları, araştırma projeleri geliştirmek, şaka yapmak, belirli şirketlerin ürünlerine saldırmak, politik mesajları yaymak veya kimlik hırsızlığı yapmak, casus yazılım ve saklı virüs ile haraç kesme gibi yöntemlerle finansal kazanç sağlamaktır. Virüs programlarının yazılış amacının bu derece geniş olması onların sayısını çoğaltmakta ve her bilgisayar kullanıcısının bu virüs programlarıyla karşılaşma ihtimalini de artırmaktadır.

1.6.4.10. İstem dışı alınan elektronik postalar (spam)

Spam kelimesi, ilk kez Hormel Foods Corporation adındaki Amerikan firmasının İkinci Dünya Savaşı sırasında Amerikan askerlerine dağıttığı baharatlı domuz eti ile jambon olarak Türkçeye çevrilen Spiced Pork and Ham (spam) kelimelerinin harflerinden oluşan bir kısaltma olarak kullanılmıştır. Bu kelimenin İngilizce "Sending Personally Annoying Mail" ifadesinin baş harflerinin biraraya getirilmesiyle oluştuğu da söylenilmektedir.[98] Daha sonra spam kelimesi, bilişim alanında istenmeyen elektronik postalar için kullanılan bir tabir olmuştur.

Spam, bilgisayar teknolojisinin yaygınlaşması ve çok kısa sürede milyonlarca e-posta adresine erişimin kolaylaşması ile e-posta kullanıcılarının hayatlarına izin almaksızın girmeye başlamıştır.[99] Bu şekilde failler sadece masumane reklam maillerini değil özellikle küçük çocuklar için tehlike oluşturacak pornografik içerikli mailleri de yollamaktadırlar.[100] Bunun dışında, e-postalara müdahalenin en çok rastlanan biçimi olan Spam mailleri e-posta kullanıcılarının spam filtresi yoksa e-posta trafiğinin kilitlenmesi suretiyle e-posta hesabının çökmesine de sebep olabilir.[101]

1.6.4.11. Bilgi aldatmacası

Bilgi aldatmacası, bilişim suçu işleme şekilleri arasında en sık başvurulan yollardan biridir. Bilgi aldatmacası, verilerin bilgisayara yanlış girilmesi ya da bazı verilerin kasten bırakılması suretiyle oluşur. Bu şekilde fail, bilgisayarda istediği gibi değişiklik yapabilme olanağını elde etmektedir. Bu fiili bilgisayarla çalışma şansına

[98]M. F. Yıldırım ve T. Memiş (2005). Elektronik Posta Kutusu Kullanımı ile İlgili Karşılaşılan Hukuki Sorunlar ve Çözüm Önerileri. *AÜEHFD*, 9 (3-4), s. 346.
[99]Spam mailleri, e-posta kullanıcılarının hayatlarına izin almaksızın girerek kişilerin yalnız kalma hakkını ihlal etmekte, ayrıca ticari hayatı da olumsuz etkilemektedir. Bu konuda ayrıntılı bilgi için bkz. Yıldırım ve Memiş, 2005, a.g.k., 346-349.
[100]http://bilisim-kulubu.com/makale/makale.php?e=T%FCrk+Hukuku%27nda+Spam%27%FDn+Hukuki+Niteli%F0i&mid=5381 (Erişim Tarihi: 03.06.2016)
[101]Oğuz, 2010, a.g.k., 87-88.

sahip, veri yaratan, kaydeden, nakleden ve kontrol yapan her hangi biri gerçekleştirilebilir. Bu tür hareketler, basit ve güvenli olmalarının yanında hareketin tespitinin zor olması açısından da faile geniş bir hareket sahası sunmaktadır. Bilgisayardaki dokümanlarda sahtecilik yapmak veya bunları taklit etmek, disk ve disketlerle manyetik bantlarda değişiklikler yapmak bilgi aldatmacasına örnek olarak verilebilecek eylemlerdir.[102]

[102]Yazıcıoğlu, 1997, a.g.k., 152.

İKİNCİ BÖLÜM

2. DOĞRUDAN BİLİŞİM SUÇLARI

2.1. Genel Olarak Bilişim Suçlarının Düzenlenme Yöntemleri

Bilişim sistemlerinin son yıllarda gösterdiği gelişmeye bağlı olarak bilişim alanında da çeşitli suçlar ortaya çıkmaya başlamış ve hukuk dünyasında bu suçlara yönelik yeni düzenlemeler yapma ihtiyacı doğmuştur. Önceleri, bilişim sistemlerine karşı yapılan ihlallerin klasik suç tiplerinden farklı olup olmadığı düşünülmeye başlanmıştır. Bu süreçte, bilişim suçlarıyla mücadele etmekte klasik suç tiplerine yönelik olan ceza hukuku normlarının yeterli olacağını savunanlar olmakla birlikte, bilişim alanında yeni ceza hukuku normlarının gerekli olduğunu savunanlar da olmuştur.[103] Fakat, zaman içerisinde klasik ceza hukuku normları bilişim alanındaki suçlarla mücadelede yetersiz kaldığından dolayı ceza kanunlarında bilişim alanında suçlar ve bilişim sistemleri aracılığıyla işlenen suçlar şeklinde yeni suç tipleri düzenlenmiştir.[104]

Bilişim alanında, yeni düzenlemeler yapılması gerektiği genel kabul görünce, bu kez de yapılacak düzenlemelerin genel ceza kanunlarında mı yoksa ayrı olarak hazırlanacak özel ceza kanunlarında mı yapılacağı tartışılmıştır. Anglo Amerikan Hukuk Sistemine tabi ülkeler tercihlerini bilişim suçlarını ayrı bir özel ceza kanununda düzenlemek yönünde kullanmıştır.[105] Bu ülkelere örnek olarak, Avustralya (2000 tarihli Mahremiyet Yasası), Şili (1993 tarihli Otomatik Bilgi İşlem Suçları Yasası), Hindistan (2000 tarihli Bilgi Teknolojileri Yasası), İsrail (1995 tarihli Bilgisayar Yasası), Malezya (1997 tarihli Bilgisayar Suçları Yasası), İngiltere (1990 tarihli Bilgisayarın Amaca Aykırı Kullanımı Yasası) verilebilir.[106]

Mevcut yasalarda değişiklik yapmak suretiyle bilişim suçlarının düzenlenmesi yönteminde de iki farklı alternatif ortaya çıkmaktadır. Bu alternatifler, bilişim suçlarının ayrı bir başlık altında düzenlenmesi ya da klasik suç tiplerinin bilişim suretiyle

[103]Eker, a.g.k., 107-108.; Dülger, 2013, a.g.k., 205.
[104]Dülger, 2013, a.g.k., 207.
[105]Eker, a.g.k., 109.; Dülger, 2013, a.g.k., 207.
[106]Değirmenci, 2005, a.g.k., 200

işlenmesinin suçun nitelikli hali sayılmasıdır. ETCK, birinci alternatife örnek olarak verilebilir. Bunların yanı sıra, bu iki alternatif bir arada da bulunabilir. Yani kanunda, hem bilişim alanında suçlar başlığı altında münhasıran düzenlemeler yapılmakla birlikte, çeşitli klasik suç tiplerine yönelik maddelerde bilişim sistemleri kullanılmak suretiyle anılan suçun işlenmesi nitelikli hal olarak düzenlenebilir. 5237 sayılı TCK buna örnektir. Türkiye, bu alanda Kıta Avrupası ülkelerinin izlediği sistemi benimsemiştir.[107]

2.2. Türk Hukukunda Bilişim Suçlarının Tarihsel Gelişimi

2.2.1. Türk Ceza Kanunu'ndaki gelişmeler

Türkiye'de bilişim alanındaki suçlara pek sık rastlanmayan dönemlerde, bilişim alanındaki ihlallere İtalya'da da olduğu gibi ceza kanununun genel hükümleri uygulanıyordu. Somut olaya göre fiil, sahtecilik, hırsızlık, dolandırıcılık gibi klasik suçlardan biri olarak düşünülüyordu. Fakat, daha sonraları bilişim suçunun konusu olan veri, bilgisayar vb. unsurlar klasik ceza hukukundaki gibi taşınır eşya sayılamayacağından ve bu unsurların mülkiyetinin de fiziki olarak el değiştirmesi mümkün olmadığından ceza kanununun kıyas yasağı, genişletici yorum yasağı ve kanunilik ilkeleri de nazara alınarak yeni düzenlemeler yapılması yoluna gidilmiştir.[108]

Türk Hukukunda bilişim suçları 1989 TCK Ön Tasarısı'yla tartışılmaya başlanmıştır. Tasarının ikinci kitabının ikinci kısmının 9. bölümünde 342. ila 346. maddeleri arasında, bilgileri otomatik işleme tabi tutmuş bir sistemden hukuka aykırı olarak veri ele geçirmek, bu verileri başkasına zarar vermek maksadıyla kullanmak, nakletmek, çoğaltmak, bu sisteme zarar vermek, hukuk alanında delil olarak kullanmak üzere sahte belge oluşturmak maksadıyla sistemdeki verilerde değişiklik yapmak suç olarak tanımlanmıştır. 346. maddede tüzel kişilerinde bu suçlardan sorumlu olduğu belirtilmiştir. Bunun yanı sıra, suçun teşebbüs aşamasında kalması durumunda da fiilin tamamlanmış suç olarak kabul edileceği düzenlenmiştir.[109]

Bilişim suçları, mevzuata ilk kez 765 sayılı TCK'nın bazı maddelerinin değiştirilmesine ilişkin 06.06.1991 tarihli ve 3756 sayılı Kanun'la girmiştir. Kanun, bazı

[107]Dülger, 2013, a.g.k., 210-211.; Kurt, 2005, a.g.k., 116.
[108]Kurt, 2005, a.g.k., 115.
[109]Kurt, 2005, a.g.k., 117, 295.

eksiklikleri olmakla beraber ASSS'deki suç tiplerinin büyük bir kısmını karşılamaktadır.[110] Bu Kanunda düzenlenen bilişim suçları, Fransız Ceza Kanunu Projesi'nde, Enformatik'e Karşı Suçlar başlığı altında yer alan maddelerden esinlenilerek hazırlanmıştır.[111] Bu suçlar, 765 Sayılı TCK'nın on birinci babında bilişim alanında suçlar bölümünde 525a ila 525d arasındaki 4 maddeyi içermektedir. 765 Sayılı Kanun'da, bilgileri otomatik işleme tabi tutmuş bir sistemle ilgili, ele geçirme (m.525/a-1), tasarruf etme (m.525/a-2), tahrip (m.525/b-1), yarar sağlama (m.525/b-2), delil tahrifi (m.525/c) fiillerinin suç oluşturduğu belirtilmiştir. Buradan da anlaşılacağı gibi, her fıkra ayrı bir suç oluşturduğundan dolayı 765 Sayılı TCK'da 5 farklı bilişim suçu öngörüldüğü söylenebilir.[112] 525/d maddesinde ise kanunun bu kısmında düzenlenmiş olan suçları işleyenlere, asli cezaların yanı sıra verilecek olan fer'i cezalar düzenlenmiştir. 525a, 525b, 525c maddeleri 1989 tarihli TCKÖT'deki düzenlemenin aynen tekrarı iken suçlardan dolayı fer'i cezaları gösteren 525d maddesi tasarının sadece 345/1. bendindeki cezayı içermektedir.[113]

1997 tarihli TCKÖT'de 347 ila 352 maddeleri arasında bilişim suçları düzenlenmiştir. Bu tasarıda bir ilk olarak bilgileri otomatik işleme tabi tutan sistem ifadesi yerine, bundan sonraki tasarılarında benimsediği şekilde bilişim sistemi ifadesi kullanılmıştır. Yine bir başka ilk olarak, tasarının 347. maddesiyle birlikte bilişim sisteminin bütününe veya bir kısmına hukuka aykırı olarak girmek de suç olarak düzenlenmiştir.[114]

Tasarının 352. maddesiyle bilişim suçlarının örgüt faaliyeti içerisinde işlenmesiyle ilgili daha önceki tasarılarda olmayan bir düzenleme getirilmiştir. Madde metninde, bilişim suçlarını işlemek için oluşturulan ve varlığı bir veya birden çok maddi nitelikte hazırlıklardan anlaşılan bir teşekkül kuran veya buna katılan kimselere işlemek istedikleri suçlardan en ağırının cezası verileceği hükme bağlanmıştır. Burada kastedilen örgüt ikiden fazla kişinin bir araya gelmesiyle oluşacaktır.[115]

---

[110]Kurt, 2005, a.g.k., 116.; Kanun'da yer verilen bilişim suçlarının eksik ve hatalı tarafları için bkz. Yücel, 1992, a.g.k., 510-511.
[111]Erem, 1991, a.g.k., 441.
[112]B.B. Akbulut (2000). Bilişim Suçları. *SÜHFD*, 7 (1-2), s. 554-555.; Sınar, 2001, a.g.k., 125-126.
[113]Dönmezer, 1995, a.g.k., 503.
[114]Kurt, 2005, a.g.k., 117-118.
[115]Kurt, 2005, a.g.k., 128.

2000 tarihli TCKÖT'de bilişim suçları, tasarının ikinci kısmının dokuzuncu bölümünde 346-352. maddeleri arasında düzenlenmiştir. Bu tasarının getirdiği yenilik ise, ilk kez banka ve kredi kartlarının kötüye kullanılmasını suç olarak düzenleyen 349. maddesidir.[116]

2003 tarihli TCKÖT'de bilişim suçları tasarının ikinci kitabının ikinci kısmının dokuzuncu bölümünde yine 346-352. maddeler arasında düzenlenmiştir. 2003 tasarısı 2000 tasarısının gerekçe de dahil olmak üzere neredeyse aynısıdır. Fakat bu tasarı, Adalet Komisyonu'nda bazı değişikliklere uğramıştır. 2003 TCKÖT'ün Adalet Komisyonu'nca kabul edilen son halinde bilişim suçları 245-248. maddeleri arasında düzenlenmiştir. [117] Komisyon tarafından kabul edilen tasarıda hukuk alanında kullanılmak üzere sahte belge oluşturmak için bilişim sistemlerine veri yerleştirmek ya da mevcut verilerde değişiklik yapmak olarak ifade edilen sahtecilik kenar başlıklı maddeye yer verilmemiştir. Ayrıca, yine komisyonca kabul edilen tasarıda önceki tasarılarda mevcut olan fer'i cezalara[118] yer verilmemiştir. 2003 TCKÖT'ün suç işlemek için örgütlenme kenar başlıklı 351. maddesi de Adalet Komisyonu'nun kabul ettiği metinde bulunmamaktadır. Yine, tasarının komisyonca kabul edilen halinde, önceki tasarılarda olduğu gibi bilişim suçlarından dolayı tüzel kişilerin de sorumlu olacağını belirtmek yerine tüzel kişiler hakkında güvenlik tedbirleri uygulanması düzenlenmiştir.

Son olarak, bilişim suçları mevcut ceza kanunumuz olan 26.09.2004 tarihli ve 5237 Sayılı TCK'nın özel hükümleri düzenleyen 2. kitabının Topluma Karşı Suçlar başlıklı 3. kısmının Bilişim Alanında Suçlar başlıklı onuncu bölümünde 243-246. maddeleri arasında düzenlenmiştir. 5237 sayılı TCK ile bilişim sistemine hukuka aykırı olarak girme fiili ilk kez münhasıran suç olarak düzenlenmiştir. Önceki tasarılarda yer alan fakat bir türlü yasalaşmayan bu suç kanunun 243. maddesiyle birlikte mevzuata girmiştir.[119] Sistematik olarak 5237 sayılı TCK da aynı 765 sayılı TCK gibi bilişim alanındaki suçları, suçların hukuki konularına göre düzenlenmesi şeklindeki Alman ve

[116]Kurt, 2005, a.g.k., 129-130.
[117]Kurt, 2005, a.g.k., 133-136.
[118]1989 TCKÖT m.345, 1997 TCKÖT m.350, 2000 TCKÖT m.349, 2003 TCKÖT m.349'da düzenlenmiş olan fer'i cezalar: kamu hizmetinden veya meslek veya sanat veya ticaretten yasaklanma, suçta kullanılan kurumların kapatılması, suçta kullanılan araçların mülkiyetinin devlete geçmesi veya müsaderedir.
[119]Kurt, 2005, a.g.k., 136.

İtalyan Ceza Kanunları yerine Fransız Ceza Kanunu'nda olduğu gibi tek bir başlık altında bir arada düzenlemiştir.[120]

2.2.2. Diğer kanunlardaki gelişmeler

Bilişim suçlarıyla daha etkin mücadele edebilmek için kanun koyucu, doğrudan bilişim suçlarına ilişkin hem yeni kanunlar yapmış hem de var olan çeşitli kanunlarda değişiklikler yapmıştır. Bunlardan ilki, 15.01.2004 tarih 5070 Sayılı Elektronik İmza Kanunu'dur. Bu kanunla birlikte Türk Hukukunda elektronik imza geçerlilik kazanmış ve uygulamada da sıkça kullanılır olmuştur. Kanunun, denetim ve ceza hükümleri başlıklı üçüncü kısmının 15-19. maddeleri arasında bilişim suçlarına yönelik düzenlemeler yapılmıştır. 16. maddeyle sahte elektronik imza yapılması ve kullanılması, 17. maddeyle sahte elektronik sertifika yapılması ve kullanılması suç olarak düzenlenmiştir.[121]

Doğrudan bilişim suçlarına yönelik düzenleme yapılan ikinci kanun olan 5.12.1951 tarihli ve 5849 Sayılı Fikir ve Sanat Eserleri Kanunu'nda 23.01.2008 tarihli 5728 sayılı yasayla yapılan değişiklikle anılan kanunun hukuk ve ceza davaları başlıklı beşinci bölümünde bilgisayar yazılım ve programları da diğer fikir ve sanat eserleri gibi koruma altına alınmış, 71. maddede bunlara yönelik ihlal hareketleri suç olarak düzenlenmiştir.[122]

2.3. Türk Hukukunda Bilişim Suçlarına Dair Hukuki Düzenlemeler

2.3.1. 5237 sayılı Türk Ceza Kanunu'nda yer alan bilişim suçları

2.3.1.1. Genel olarak

5237 sayılı TCK'nın hazırlanıp yürürlüğe sokulmasının iki önemli sebebi vardır. Bunlardan birincisi, 1 Temmuz 1926'da yürürlüğe giren 765 sayılı TCK'nın güncel sorunların sürekli değişmesi karşısında yetersiz kalmasıdır. İkincisi ise, yabancı bir kanunun (1899 İtalyan Ceza Kanunu) bazı değişikliklerle yürürlüğe sokulmuş olmasından duyulan rahatsızlık ve artık kendi kanunumuza sahip olmamız gerektiği özlemidir.[123] İşte bu sebeplerden dolayı, 765 sayılı TCK'da çeşitli zamanlarda

[120]Ketizmen, M. (2008). *Türk Ceza Hukukunda Bilişim Suçları*. Ankara: Adalet Yayınevi, s. 60.
[121]Dülger, 2013, a.g.k., 214.
[122]Dülger, 2013, a.g.k., 214.
[123]N. Toroslu ve Y. Ersoy (2004). Kanunlaşmaması Gereken Bir Tasarı. T. Ergül (Ed.), *Türk Ceza Kanunu Reformu İkinci Kitap Makaleler, Görüşler, Raporlar* içinde (s. 1-20). Ankara: Türkiye Barolar Birliği Yayınları, s. 1.

değişiklikler yapılmış ya da yeni ceza kanunu tasarıları hazırlanmıştır. İlk olarak, 1940 tarihinde hazırlanan bu kanun tasarılarının sonuncusu ise 12.05.2004 tarihinde Adalet Komisyonu Başkanlığı'na sunulmuş olan Türk Ceza Kanunu Tasarısı'dır.[124]

Bu tasarı, 26 Eylül 2004 tarihinde TBMM'de kabul edilmiş ve Resmi Gazete'nin 12 Ekim 2004 tarihli 25611. sayısında yayımlanmıştır. Bu kanunun 344. maddesinde, kanunun yürürlüğe giriş tarihi ise bazı hükümleri hariç (m. 181, 182, 184) olmak üzere 1 Nisan 2005 olarak belirtilmiştir. Kanunun yürürlüğe girmesiyle birlikte de 765 sayılı TCK yürürlükten kalkmıştır.

Yürürlüğe giren 5237 sayılı TCK'da bilişim suçları, kanunun Özel Hükümler başlıklı ikinci kitabının, Topluma Karşı Suçlar başlıklı üçüncü kısmının, Bilişim Alanında Suçlar başlıklı onuncu bölümünde 243 ila 246 maddeleri arasında düzenlenmiştir. Kanunun, 243. maddesinde, bilişim sistemine girme, 244. maddesinde sisteme veya verilere zarar verme, 245. maddesinde banka veya kredi kartlarının kötüye kullanımı, 245/A maddesinde bilişim suçu işlenmesinde kullanılacak cihaz vb. aygıtların imal edilmesi, alımı, satımı, saklanması suç olarak öngörülmüş, 246. maddesinde ise tüzel kişilere uygulanacak güvenlik tedbirleri düzenlenmiştir.

2.3.1.2. 765 sayılı TCK ile 5237 sayılı TCK'da yer alan bilişim suçları arasındaki farklılıklar

765 sayılı TCK ile 5237 sayılı TCK'daki bilişim suçları düzenlemeleri arasında, düzenlenme yöntemi ve suç tipleri açısından bazı farklılıklar vardır. Göze çarpan ilk farklılık, bilişim sistemlerinin kullanılması suretiyle işlenen suçların da yeni kanunla birlikte mevzuata girmesidir. Bilindiği gibi, eski kanunda sadece sistemin kendisine karşı işlenen fiiller suç oluşturmaktaydı. Bunun yanı sıra, suç tipleri açısından bakıldığında da yeni kanunun eski kanunda yer alan bazı suç tiplerine yer vermediği görülmektedir. Ayrıca, eski kanunda yer alıp da yeni kanunda düzenlenmeyen suç tipleri de vardır. Bazı suçlar ise yeni kanunda aynen korunmuştur. Çalışmanın bu kısmında her iki kanun arasındaki farklılıkların neler olduğunu kısaca inceleyeceğiz.

[124]M.E. Artuk ve A.R. Çınar (2004). Yeni Bir Ceza Kanunu Arayışları ve Adalet Alt Komisyonu Tasarısı Üzerine Düşünceler. T. Ergül (Ed.), *Türk Ceza Kanunu Reformu İkinci Kitap Makaleler, Görüşler, Raporlar* içinde (s. 37-84). Ankara: Türkiye Barolar Birliği Yayınları, s. 37 vd.

765 sayılı TCK bilişim alanında suçlar başlığı altında 4 madde halinde bilişim suçlarını düzenlemekteydi. Bu 4 maddede kanun sadece bilişim sistemlerine karşı işlenecek suçlara yer veriyordu. 5237 sayılı TCK, eski kanunun bu sisteminden ayrılarak bilişim sistemlerine karşı suçların yanı sıra bilişim sistemlerinin kullanılması yoluyla işlenen suçları da düzenleyerek karma bir sistem kabul etmiştir.[125]

Terminolojik açıdan bakıldığında, 765 sayılı TCK'da geçen bilgileri otomatik işleme tabi tutan sistem ifadesi yerine yeni TCK'da bilişim sistemi ifadesi kullanılmıştır. Bu tercih doktrinde isabetli görülmüştür.[126]

Yeni TCK ile mevzuata ilk kez giren suç tiplerinden birisi 243. maddede düzenlenen bilişim sistemine girme fiilidir. 765 sayılı TCK'da suçun oluşması için, sisteme sadece hukuka aykırı olarak girmek fiili yetmiyor, bunun yanı sıra sisteme hukuka aykırı girildikten sonra verilerde değişiklik yapmak, verileri ele geçirmek gibi fiillerin de gerçekleştirilmiş olması gerekiyordu. Bu durum, eski yasa döneminde çok eleştiriliyor ve yetkisiz erişimin münhasır bir suç olarak düzenlenmesi öneriliyordu.[127] Kanun koyucu eleştirileri dikkate alarak, TCK'da artık bilişim sistemine hukuka aykırı girmek fiilini de münhasıran suç saymıştır. Ayrıca, hukuka uygun olarak girilmiş olsa bile, eğer hukuka uygunluk sebebi ortadan kalktıktan sonra sistemde kalmaya devam ediliyorsa bu durumda da 243. maddedeki suç oluşacaktır.

5237 sayılı TCK ile mevzuata ilk kez giren suç tiplerinden bir diğeri de 243. maddenin 4. fıkrasında yer verilen bilişim sistemine girmeksizin bilişim sistemlerindeki veri nakillerini teknik araçlarla izleme suçudur.

Başka bir farklılık ise 765 sayılı TCK'nın 525/c maddesindeki suç tipiyle ilgilidir. 765 sayılı TCK'nın 525/c maddesi hukuk alanında kullanılmak amacıyla, sistem üzerindeki veri veya diğer unsurlar üzerinde yapılacak değişiklikler yoluyla sahte belge oluşturmak fiilini cezalandırmaktaydı. Kanun koyucu yeni TCK'da bu hükme yer vermemiştir. Ancak TCK'daki hukuka aykırı veri yerleştirme veya değiştirme suçu, 765 sayılı TCK'daki 525/c maddesini de kapsayacak bir hüküm olarak düzenlenmiştir.[128]

765 sayılı TCK'nın 525/a-2 maddesinde düzenlenmiş olan suç tipine yeni TCK'da

[125]Eker, 2006, a.g.k., 120.
[126]Eker, 2006, a.g.k., 120.; Dülger, 2013, a.g.k., 317.; Artuk, Gökçen ve Yenidünya, 2009, a.g.k., 4627.
[127]Ünver, 2001, a.g.k., 91.
[128]Biçkin, 2006, a.g.k., 157-158.

doktrin ve uygulamadaki eleştiriler dikkate alınarak yer verilmemiştir.[129]

TCK'nın yasak cihaz ve programlar başlıklı 245/A maddesinde yer verilen suç tipi 765 sayılı TCK'da yer almamaktaydı. TCK'nın ilk halinde mevcut olmayan bu hüküm daha sonra kanuna eklenmiştir. Yine kanuna sonradan eklenmiş olan bir diğer suç tipi olan 243/4. maddedeki bilişim sistemine girmeksizin veri nakillerini teknik araçlarla hukuka aykırı izleme suçu da 765 sayılı TCK'da düzenlenmemişti.

765 sayılı TCK'nın 525/d maddesi bilişim alanında suçlar başlığı altındaki 525/a ve 525/b maddelerindeki suçları işleyenler için fer'i cezalar öngörmekteydi. Fakat, yeni TCK'da fer'i cezalara yer verilmemiştir.

5237 sayılı TCK'da, eski yasadan farklı olarak 246. maddede bu suçların işlenmesi sonucu yararına haksız menfaat sağlanan tüzel kişiler için güvenlik tedbirleri öngörülmüştür. 765 sayılı TCK'nın bilişim alanında suçlar bölümünde böyle bir düzenleme bulunmamaktaydı.

2.3.1.3. Hukuka aykırı olarak bilişim sistemine girme veya sistemde kalmaya devam etme suçu (m. 243/1)

2.3.1.3.1. Genel olarak

Maddenin birinci fıkrası şu şekildedir: "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."

5237 sayılı TCK'nın tasarı metninin Adalet Komisyonu'ndaki halinde bu fıkra aynen yukarıda belirtildiği gibiydi. Fakat, TBMM Genel Kurulu'nda verilen bir önerge ile hukuka aykırı olarak girme veya orada kalmaya devam etme ifadesindeki "veya" sözcüğünün yerine "ve" sözcüğü getirildi. Böylece, suçun oluşumu için sadece hukuka aykırı olarak bilişim sistemine girmek yetmemekte, ayrıca sistemde kalmaya devam etmiş olmak şartı da gerekmekteydi. Bu fıkranın gerekçesinde ise aynı değişiklik yapılmadığından dolayı madde metni ile gerekçe arasında çelişki olmaktaydı.[130][131]

Doktrinde, bilişim sistemine yetkisiz erişimin cezalandırılmasının ayrıca sistemde

[129]Dülger, 2013, a.g.k., 317.
[130]Artuk, Gökçen ve Yenidünya, 2009, a.g.k., 4625-4626.
[131]TCK'nın 243. maddesinin gerekçesi: "...maddenin birinci fıkrasında bir bilişim sisteminin bütününe veya bir kısmına hukuka aykırı olarak girmek veya orada kalmaya devam etmek fiili...".

kalmaya devam etmek şartına bağlı olması eleştirilmekteydi.[132] Kanun koyucu doktrinde ve uygulamada bu madde ile ilgili yapılan eleştirileri de dikkate alarak, bu fıkrada geçen "ve" ibaresini 24/3/2016 tarihli ve 6698 Sayılı Kişisel Verilerin Korunması Hakkındaki Kanun'un 30'uncu maddesiyle "veya" olarak değiştirdi. Kanunun son haliyle birlikte artık bilişim sistemine hukuka aykırı erişim fiili, sistemde kalmaya devam etme gibi bir fiil olmasa bile tek başına suç oluşturacaktır. Yapılan bu değişiklik ASSS'deki yükümlülüklere de uygundur. Çünkü, sözleşmede, sözleşmenin metninde illegal access (hukuka aykırı erişim) olarak belirtilen fiilin sistemde kalmaya devam etme şartı aranmaksızın taraf devletlerce suç olarak düzenlenmesi istenmektedir.[133] Bu değişiklikle madde metni ile gerekçesi arasındaki çelişki de ortadan kaldırılmıştır. Böylece, ASSS'nin 2. maddesindeki kanunsuz erişim başlıklı yükümlülük yerine getirilmiş olmaktadır.[134]

Bilişim sistemlerinde işlenen diğer ihlaller esas alındığında, bilişim sistemine erişim, diğer suçların işlenebilmesi için bir araç niteliği taşımaktadır. Hukuka aykırı olarak bilişim sistemlerine erişimin bu maddede münhasıran suç olarak düzenlenmiş olması, failin sistemdeki verilere yönelik başka fiiller gerçekleştirip gerçekleştirmediğine bakılmaksızın cezalandırılabilmesi imkanı vermektedir. Yani fail, bilişim sistemine ya da sistemde bulunan verilere zarar vermemiş dahi olsa hukuka aykırı erişim sağladığından dolayı cezalandırılacaktır. Dolayısıyla, kanun koyucunun bilişim sistemine yetkisiz erişimi münhasıran suç haline getirmiş olması bilişim suçlarıyla mücadele açısından yerinde bir düzenleme olmuştur. [135]

Maddenin ikinci fıkrasında ise bu suç tipi açısından suçun nitelikli haline yer verilmiştir. Bu fıkrada "yukarıdaki fıkrada tanımlanan fiillerin bedeli karşılığı yararlanılabilen sistemler hakkında işlenmesi halinde, verilecek ceza yarı oranına kadar indirilir" denilmek suretiyle birinci fıkradaki suç açısından cezayı hafifletici bir hal öngörülmüştür.

---

[132] Bu eleştiriler için bkz. Dülger, 2013, a.g.k., 319-320.; Ketizmen, 2008, a.g.k., 81-82.; Artuk, Gökçen ve Yenidünya, 2009, a.g.k., 4632-4633.; D. Tezcan , M.R. Erdem ve R.M. Önok (2017). *Teorik ve Pratik Ceza Özel Hukuku.* (14. baskı). Ankara: Seçkin Yayınevi, s. 980.; Koca ve Üzülmez, 2016, a.g.k., 806-807.; A. Karagülmez (2010). Olması Gereken Hukuk Açısından Türk Ceza Kanununda Bilişim Sistemine Haksız Erişim Suçu. *TAAD,* 1 (3), s. 239-240.

[133] Ketizmen, 2008, a.g.k., 100.

[134] Parlar, 2011, a.g.k., 15.

[135] Ketizmen, 2008, a.g.k., 79-80.; Değirmenci, 2005, a.g.k., 204.; Koca ve Üzülmez, 2016, a.g.k., 808.

Maddenin üçüncü fıkrasında ise yine birinci fıkradaki suç açısından nitelikli hal öngörülmüştür. Fakat, buradaki nitelikli halde, cezayı hafifletici değil, ağırlaştırıcı bir durum söz konusudur. Fıkrada netice sebebiyle ağırlaşan suç[136] tipine yer verilmiştir. Buna göre, bilişim sistemine yetkisiz erişim durumunda sistemde yer alan veriler zarar görürse faile birinci fıkradaki suça göre daha fazla ceza verilecektir.

2.3.1.3.2. Korunan hukuki yarar

Hukuki yarar, hukuk tarafından korunan menfaattir. Bu menfaati ihlal etmeye yönelenleri hukuk normu, ceza ile tehdit ederek olası ihlalleri önlemeye çalışmaktadır. Devlet, bazı menfaatleri, toplumsal yaşam için böyle bir zorunluluk olmasından dolayı, korunmaya değer bulmuş ve bunun için de hukuk normlarını oluşturmuştur.[137]

Bilişim sistemine hukuka aykırı olarak girme suçunda korunan hukuki yarar, karma bir nitelik taşımaktadır. Bilişim sistemine hukuka aykırı olarak girme suçu öncelikle özel hayatın gizliliğini, kamu güvenini, sırrın masuniyetini, haberleşme özgürlüğünü korumaktadır.[138] Bu suçla, temel olarak, bireyin sanal ya da diğer bir ifadeyle dijital ortamdaki özel alanı koruma altına alınmaktadır. Yani bilişim sistemine hukuka aykırı olarak erişim suçuyla korunan hukuki menfaatin öncelikle dijital dünyadaki özel alan olduğunu söyleyebiliriz.[139]

İkincil olarak ise bilişim sisteminin güvenliği korunmaktadır. Çünkü burada suç sayılan fiil bilişim sisteminin güvenliğini de tehlikeye atmakta, sistem sahibi ya da kullanıcısına zarar verebilmektedir. Ayrıca, bu tarz fiiller bilişim sistemlerine olan güven duygusunu da sarsmaktadır.[140]

Bilişim sistemine hukuka aykırı girme suçuyla korunan bir başka hukuki değer ise, sistemin sahibi ya da kullanıcılarının sistem üzerinde tasarruf edebilmelerine ilişkin

---

[136]TCK'nın, Netice sebebiyle ağırlaşmış suç başlıklı 23. maddesi şu şekildedir: Bir fiilin, kastedilenden daha ağır veya başka bir neticenin oluşumuna sebebiyet vermesi halinde, kişinin bundan dolayı sorumlu tutulabilmesi için bu netice bakımından en azından taksirle hareket etmesi gerekir.

[137]D. Soyaslan (2012). *Ceza Hukuku Genel Hükümler*. (5. Baskı). Ankara: Yetkin Yayınevi, s. 242-243.

[138]A.İ. Erdağ (2010). Bilişim Alanında Suçlar (Türk ve Alman Ceza Hukukunda). *GÜHFD*, 14 (2), s. 279-281.; Y. Erdoğan (2012). Bilişim Sistemine Girme ve Kalma Suçu. *Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi*, 10 (Özel Sayı), s. 1370.; M.E. Artuk, A. Gökçen ve A.C. Yenidünya (2015). *Ceza Hukuku Özel Hükümler*. (15. Baskı). Ankara: Adalet Yayınevi, s. 860.; Kurt, 2005, a.g.k., 148.; F.S. Mahmutoğlu (2013). Türk Ceza Kanunu'nda Yer Alan Bilişim Alanındaki Suçlar ve Karşılaşılan Sorunların Yargı Kararları Işığında Değerlendirilmesi. *İÜHFM*. 71 (1), s. 858-859.

[139]Karakehya, 2009, a.g.k., 12.

[140]Erdoğan, 2012, a.g.k., 1371.; Artuk, Gökçen ve Yenidünya, 2015, a.g.k., 860.; Özbek, Doğan, Bacaksız ve Tepe, 2016, a.g.k., 932-933.

yetkileridir. Buradaki tasarruf yetkisi bir bilişim sistemine kimlerin erişebileceğinin sistem sahibi ya da kullanıcıları tarafından belirlenebilmesi anlamına gelmektedir.[141]

Burada belirtmek gerekir ki, maddenin 3. fıkrasında nitelikli hal olarak öngörülen sistemin içerdiği verilerin yok olması ya da değişmesi durumunda yukarıda belirtmiş olduğumuz hukuki yararların yanı sıra, kanun koyucu mülkiyet hakkını da koruma altına almıştır.[142]

Bilişim sistemine yetkisiz erişim, genellikle daha sonra işlenecek bir suç için araç olma niteliği taşımaktadır. Sisteme giriş çoğu zaman başka suçların işlenebilmesi için deneme amaçlı da yapılabilmektedir. Bu nedenle, fiilin suç olarak düzenlenmesi diğer suçların engellenmesi bakımından da önem kazanmaktadır.[143]

2.3.1.3.3. Maddi unsur

2.3.1.3.3.1. Fiil

Genel olarak suçun maddi unsuru, fiil (hareket) ve neticedir. Fiil, insana atfedilebilen ve dış dünyada etki doğurabilen her şeydir ve 2 şekilde karşımıza çıkabilir. Bunlar, icrai (aktif) ya da ihmali (pasif) hareket şeklindedir.[144] Neticeden kasıt ise işlenen suç sebebiyle dış dünyada meydana gelecek bir değişikliktir. Bu değişiklik maddi, fizyolojik ya da psikolojik bir zarar veyahut zarar tehlikesidir. Bir suçun oluşumu için hareketten kaynaklı suç tiplerinde belirtilmiş olan bir netice meydana gelmelidir.[145] Buradan hareketle, çalışma kapsamında maddi unsur başlığı altında sırasıyla fiil (hareket), fail (fiili yapan) ve mağdur (fiilden etkilenen) ile neticeyi her suç

---

[141]Ketizmen, 2008, a.g.k., 82.; Akıncı, 2001, a.g.k., 14.
[142]Kurt, 2005, a.g.k., 148.
[143]Erdoğan, 2012, a.g.k., 1371.; Artuk, Gökçen ve Yenidünya, 2015, a.g.k., 860.; Karagülmez, 2010, a.g.k., 236.; Akıncı, 2001, a.g.k., 14-15.
[144]M.E. Artuk, A. Gökçen ve A.C. Yenidünya (2016). *Ceza Hukuku Genel Hükümler*. (10. Baskı). Ankara: Adalet Yayınevi., s. 213-216.; Soyaslan 2012, a.g.k., 236.; Doktrinde suçun unsurları farklı şekillerde tasnif edilmiştir. Demirbaş, suçun unsurlarını tipe uygun fiil, hukuka aykırılık ve kusurluluk olarak üçe ayırmakta ve bu tasnifin doktrinde genel olarak kabul gören dörtlü tasniften (kanuni unsur, maddi unsur, hukuka aykırılık unsuru ve manevi unsur) önemli bir farkı olmadığını ve neticenin, tipe uygun fiil nedeniyle dış dünyada gerçekleşen değişiklik olduğunu söylemektedir. Bkz. T. Demirbaş (2016). *Ceza Hukuku Genel Hükümler*. (11. Baskı). Ankara: Seçkin Yayınevi, s. 205-207, 240.; Akbulut, suçun unsurlarını tipiklik ve hukuka aykırılık olarak ikiye ayırmakta, geniş anlamda tipikliğin cezalandırılabilirliğin tüm koşullarını içerdiğini söylemekte, dar anlamda tipikliği ise suçun maddi ve manevi unsurları olarak görmekte ve suçun maddi unsurlarını, fail, hareket (fiil), netice, nitelikli haller ve konu gibi kanuni tanımda yer verilen tüm unsurlar olarak belirtmektedir. Bkz. B. Akbulut (2016). *Ceza Hukuku Genel Hükümler*. (3. Baskı). Ankara: Adalet Yayınevi, s. 200-203.; Hakeri, suçun unsurlarının kanuni unsur (tipiklik), tipikliğin maddi ve manevi unsuru ve hukuka aykırılık unsuru olduğunu, tipikliğin maddi unsurunu ise hareket (fiil), netice ve nedensellik bağı oluşturduğunu ve neticenin failin fiiliyle meydana gelmiş olması gerekir. Bkz. H. Hakeri (2014). *Ceza Hukuku Genel Hükümler*. (17. Baskı). Ankara: Adalet Yayınevi, s. 123-124, 138-177.
[145]Artuk, Gökçen ve Yenidünya, 2016, a.g.k., 250-251.; Soyaslan, 2012, a.g.k., 236-237.; Hakeri, 2014, a.g.k., 162-163.; Akbulut, 2016, a.g.k., 277-278.; Demirbaş, 2016, a.g.k., 240.

tipi için ayrı ayrı inceleyeceğiz.

Bilişim sistemine hukuka aykırı olarak girme suçunun maddi unsurunu, bilişim sisteminin tamamına veya bir kısmına hukuka aykırı olarak girmek ya da hukuka uygun olarak girilen bilişim sisteminde daha sonra hukuka uygunluk sebebi ortadan kalktığı halde kalmaya devam etmek fiili oluşturur. Bilişim sistemine girme açısından belli bir yöntem öngörülmediğinden herhangi bir hareketle bilişim sistemine hukuka aykırı olarak girmiş olmak suçun oluşumu için yeterlidir.[146] Bu yönüyle suç serbest hareketli bir suçtur.

Bilişim sistemine hukuka aykırı olarak girmek veya orada kalmaya devam etmek fiilinden kasıt; bilişim sistemi aracının parçalarına fiziken bir şekilde girebilmiş olmak değildir. Burada girmek kavramı, sistemin soyut unsuru olan yazılım kısmının bir bölümüne veya tamamına erişmek, dahil olmak anlamındadır.[147] Bu suç, bir kimsenin emanet ettiği bilgisayarın açılarak içindeki verilerin görülmesi ya da bir ağ aracılığıyla bilişim sisteminde oturum açılması şeklinde veya bir kamu kurumunun bilgisayarına dışarıdan hukuka aykırı olarak girerek sistem içerisindeki bilgileri öğrenmek şeklinde gerçekleşebilir.[148]

Bilişim sisteminde kalmaya devam etme hareketi açısından, devamlılığın ne kadar olması gerektiği doktrinde tartışılmaktadır. Çünkü, bu konuda kanun koyucu herhangi bir süre öngörmemiştir. Kanun koyucunun burada süre öngörmemesini kanun tekniği açısından isabetli bir tercih olarak değerlendiren Kurt'a göre, bu suç ile sistem sahibinin özel hayatının gizliliği ve sistemdeki verilerin gizliliği korunmak istendiğine göre bu değerleri ihlal edecek kadar sistemde kalmış olmak suçun oluşumu için yeterlidir. Bu süre her olaya göre ayrı değerlendirilmeli ve hakim bu konuda takdir yetkisini kullanmalıdır.[149] Karakehya'ya göre de bu süre her olaya göre ayrı değerlendirilmelidir. Bu bakımdan sisteme girip hukuki menfaatlere zarar vermeksizin derhal sistemden çıkan kimsenin fiili süre açısından maddi unsura uymadığından suç oluşturmamaktadır.[150] Diğer bir görüşe göre; fail, bilişim sistemine dahil olduğunu öğrendiği andan itibaren sistemden çıkması için gerekecek makul süreyi az ya da çok

[146]Parlar, 2011, a.g.k., 16.
[147]Erdoğan, 2012, a.g.k., 1375.; Erol, 2010, a.g.k., 3749.
[148]Yaşar, Gökçan ve Artuç, 2010, a.g.k., 6744.
[149]Kurt, 2005, a.g.k., 154-155.
[150]Karakehya, 2009, a.g.k., 13-14.

aştıysa suç tamamlanmış kabul edilecektir.[151] Kanımızca, devamlılık süresinin belirlenmesinde, failin korunan hukuki değerleri ihlal edecek kadar bilişim sisteminde bilerek ve isteyerek kalmış olması durumu her somut olayda özellikle incelenmelidir. Burada hakim takdir yetkisini kullanmalıdır.

Failin, sisteme bilfiil girmeksizin elektronik posta yollaması bu suçu oluşturmayacaktır. Çünkü, kanun koyucu burada açıkça bilişim sistemine girmiş olma şartını aramaktadır. Fakat, örneğin, elektronik posta yoluyla truva atı özellikli programla sisteme girilmesi halinde bu suç oluşacaktır. Çünkü, fail bu yöntemle sisteme fiili anlamda girmese bile program vasıtasıyla her an sisteme ulaşabilir hale gelmekte ve sistem içerisindeki verileri elde edebilme imkanına sahip olmaktadır. Dolayısıyla da bu suçla korunan hukuki yararları ihlal etmektedir.[152]

Bilişim sistemine suç işlemek amacıyla değil de marifet göstermek, kendi firmasının reklamını yapmak, eğlenmek, güvenliği denemek, protesto etmek gibi amaçlarla girilmiş olsa bile suç oluşacaktır. Yani, amaç ne olursa olsun bilişim sistemine haksız ve kasten girilmiş olması ve orada bir süre kalınması fiili gerçekleştiğinde suç oluşacaktır.[153] Kanun koyucu hem madde metninde hem de gerekçede bilişim sisteminde yer alan verilerin zarar görmesi ihtimalini suçun oluşumu açısından yeterli görmüştür.[154]

Kanundaki değişiklikten önce bilişim sistemine hukuka aykırı olarak girme ve orada kalmaya devam etme fiili cezalandırıldığından dolayı bu suç mütemadi (kesintisiz) suç[155] özelliği taşıyordu. Fakat, bu maddedeki "ve" ibaresinin "veya" olarak değişmesiyle birlikte, bilişim sistemine hukuka aykırı girme fiili açısından kesintisizlik şartı artık aranmayacaktır.

Yapılan bu değişiklik neticesinde bilişim sistemine hukuka aykırı olarak girme veya orada kalmaya devam etme suçu klasik suçlardan olan konut dokunulmazlığının ihlali suçuna çok daha fazla benzerlik taşımaktadır. Değişiklik öncesi de bu suç, konut

[151]Erdoğan, 2012, a.g.k., 1377.; Artuk, Gökçen ve Yenidünya, 2009, a.g.k., 4632.; Özbek, Doğan, Bacaksız ve Tepe, 2016, a.g.k., 937.
[152]Kurt, 2005, a.g.k., 149.; Tezcan, Erdem ve Önok, 2017, a.g.k., 981.
[153]Biçkin, 2006, a.g.k., 151.; Yaşar, Gökçan ve Artuç, 2010, a.g.k., 6738.
[154]Parlar, 2011, a.g.k., 16-17.; Kurt, 2005, a.g.k., 150-151.
[155]Kesintisiz suç, hareket ve bunun doğurduğu neticenin bir süre devam etmesi gereken suçlardır. Yani fiil ve hukuki zararın tek olması ancak bir süre devam etmesidir. Bkz. Soyaslan, 2012, a.g.k., 272.

dokunulmazlığının elektronik ihlali olarak değerlendiriliyordu.[156] TCK 116. maddede düzenlenen konut dokunulmazlığında, rızaya aykırı konuta girmek ve rıza ortadan kalkmasına rağmen konutta kalmaya devam etmek suç olarak düzenlenmiştir. 243. maddede de benzer şekilde, bilişim sistemine hukuka aykırı girmekle hukuka uygunluk ortadan kalktığı halde, sistemde kalmaya devam etmek suçu dijital olarak konut dokunulmazlığı ihlali sayılmaktadır. Şeklen bilişim sistemine haksız erişim konut dokunulmazlığını ihlal fiiline benzemekteyse de bilişim sistemlerinin hayatın nerdeyse her alanında kullanılıyor olması sebebiyle haksız erişim bazı durumlarda çok daha vahim sonuçlar meydana getirebilir.[157]

Bilişim sistemine girmek veya orada kalmaya devam etmek suçuna, uygulamada sıklıkla karşılaşılan, mağdura ait e-mail adresine şifresini kırmak suretiyle hukuka aykırı olarak girilmesi ve orada kalmaya devam edilmesi[158], yine mağdura ait Facebook hesabına sanık tarafından şifresini kırmak suretiyle girilmesi[159] gibi sosyal medya hesaplarına hukuka aykırı olarak erişim sağlanması fiilleri örnek olarak verilebilir.

2.3.1.3.3.2. Fail ve mağdur

Bilişim sistemine hukuka aykırı olarak girme veya orada kalma suçunda fail bakımından özel bir nitelik aranmamıştır. Dolayısıyla herkes bu suçun faili olabilir. Mağdur açısından da özel bir durum söz konusu değildir. Hukuka aykırı olarak bilişim sistemine girilen herhangi bir kimse bu suçun mağdurudur.[160]

2.3.1.3.3.3. Netice

Netice açısından 243. maddedeki suç tipi genel olarak değerlendirildiğinde, failin bilişim sistemine hangi amaçla girmiş olduğunun öneminin olmadığı, suçun oluşması için belirli bir sonucun meydana gelmesi gibi bir şartın da aranmadığı anlaşılacaktır. Fakat, doktrinde bilişim sistemine girme veya kalmayı bir hareket değil netice olarak

[156]Ketizmen, 2008, a.g.k., 92.; Yücel, 1992, a.g.k., 509.
[157]Karagülmez, 2010, a.g.k., 236, 247.
[158]Yargıtay 8. Ceza Dairesi'nin 07.04.2014 tarih ve 2013/ 3214 Esas ve 2014/8845 Karar sayılı kararı.; Yargıtay 8. Ceza Dairesi'nin 09.06.2014 tarih ve 2014/5592 Esas ve 2014/14132 Karar sayılı kararı.; Yargıtay 8. Ceza Dairesi'nin 18.03.2015 tarih ve 2014/30051 Esas ve 2015/13973 Karar sayılı kararı.; Yargıtay 8. Ceza Dairesi'nin 02.06.2015 tarih ve 2014/37839 Esas ve 2015/18101 Karar sayılı kararı.
[159]Yargıtay 8. Ceza Dairesi'nin 08.04.2014 tarih ve 2014/33371 Esas ve 2015/15859 Karar sayılı kararı.; Yargıtay 8. Ceza Dairesi'nin 14.10.2015 tarih ve 2015/3445 Esas ve 2015/22717 Karar sayılı kararı.; Yargıtay 8. Ceza Dairesi'nin 18.11.2015 tarih ve 2015/7531 Esas ve 2015/24704 Karar sayılı kararı.
[160]Koca ve Üzülmez, 2016, a.g.k., 808-809.; Mahmutoğlu, 2013, a.g.k., 859.

gören yazarlar da vardır.[161] Bu görüşe katılmak mümkün değildir. Çünkü kanun lafzından bilişim sistemine girme veya orada kalmaya devam etmenin suçun hareket unsurunu oluşturduğu açıkça anlaşılmaktadır. Suç, bir soyut tehlike suçudur.[162]

2.3.1.3.4. Manevi unsur

Bir suçtan bahsedebilmek için salt maddi unsurların mevcut olması yeterli değildir. Ayrıca, manevi unsurunda var olması gerekir. Manevi unsur, suçun varlığı için gerekli olan fiil ile fail arasındaki psikolojik bağdır. Ceza hukuku anlamında sorumluluktan bahsedebilmek için hareketin bilerek ve istenerek yapılmış olması gerekir. Bunun yanı sıra, fail neticeyi de biliyor ve istiyorsa failin kasta dayanan sorumluluğu, eğer netice fail tarafından öngörülemediyse bu durumda da failin taksire dayanan sorumluluğu söz konusu olacaktır.[163] Bir suçun oluşabilmesi TCK'nın 21. maddesine göre kastın varlığına bağlıdır. Kast, suçun kanuni tanımındaki unsurların bilerek ve istenerek gerçekleştirilmesidir. Taksirli suçlar istisnadır. Failin taksirli fiilinden sorumlu tutulabilmesi, TCK'nın 22/1. maddesindeki düzenlemeye göre ancak kanunun açıkça belirttiği hallerde söz konusu olabilir.

Bilişim sistemine girme veya orada kalmaya devam etme suçu kasten işlenebilir. Taksirle bu suçun işlenmesi mümkün değildir. Suçun kasten işlenebileceği maddenin gerekçesinde de açıkça belirtilmiştir.[164]

Suçun oluşması için genel kast yeterlidir. Kanun koyucu failde özel kast[165] aramamıştır. Bundan dolayı failin mağdura zarar vermek, kendisi için yarar sağlamak,

---

[161]Erdoğan, 2012, a.g.k., 1391.

[162]Zarar suçunda, fiilin yönelmiş olduğu konuda bir zararın meydana gelmiş olması gerekirken, tehlike suçunda zarar tehlikesinin olması yeterlidir. Kanun koyucu tehlike suçunda zarar ihtimalini tek başına suçun oluşumu için yeterli görmüştür (Örn. Anayasayı ihlale teşebbüs suçu), tehlike suçları somut tehlike ve soyut tehlike suçları olmak üzere ikiye ayrılır. Somut tehlike suçlarında gerçek bir zarar tehlikesinin meydana gelmiş olması şartı aranırken, soyut tehlike suçlarında fiilin yapılmış olması yeterli olup gerçek bir somut tehlikenin oluşmasına gerek yoktur. Bkz. Hakeri, 2014, a.g.k., 164-165.; Demirbaş, 2016, a.g.k., 244-245.; Soyaslan, 2012, a.g.k., 247-248.

[163]Artuk, Gökçen ve Yenidünya, 2016, a.g.k., 293-296.; Soyaslan, 2012, a.g.k., 426-427.: Hakeri, 2014, a.g.k., 200-202.; Doktrinde farklı görüşteki yazarlardan Akbulut'a göre, kast ve taksir yalnızca haksızlığın gerçekleştiriliş şeklidir, kusurluluk şekli değildir ama aynı zamanda haksızlık kusur yargısının dayanağıdır, fiil failin kusuru bulunmaksızın işlense dahi haksızlık ve suç teşkil eder. Yine yazara göre, kastta ayrıca isteme unsuruna gerek yoktur. TCK'nın 21/1. maddesinde geçen isteme kavramı kanuni tanımda yer alan maddi unsurları gerçekleştirme iradesini ifade eder. Bkz. Akbulut, 2016, a.g.k., 344-351.

[164]Madde gerekçesi: "...sisteme haksız ve kasten girilmiş olması suçun oluşması için yeterlidir."

[165]TCK'nın 21. maddesine göre, bir suçun oluşması, suçun kanuni tanımındaki unsurların bilerek ve istenerek gerçekleştirilmesi şeklindeki genel kastın varlığına bağlıdır. Ancak kanun koyucu genel kastın yanı sıra bazı suç tipleri için failde özel bir saik, amaç aramıştır. Örneğin, adam öldürme suçunda failin bir insanı öldürdüğünü bilmesi ve istemesi şeklindeki genel kast yeterlidir. Ancak hırsızlık suçunda, kanun koyucu failin "bir yarar sağlamak maksadıyla hareket etmesi" şartını aradığından bu suç özel kastla işlenebilir. Bkz. Demirbaş, 2016, a.g.k., 379-380.; Artuk, Gökçen ve Yenidünya, 2016, a.g.k., 319.; Hakeri'ye göre, genel kast-özel kast ayrımı 765 sayılı TCK da vardır, ancak kanun koyucu 5237 sayılı TCK'da bu ayrıma yer vermemiştir. bkz. Hakeri, 2014, a.g.k., 217

sistemden bir şey elde etmeye çalışmak, eğlenmek ya da oyun oynamak gibi amaçlarının suçun oluşumuna herhangi bir etkisi yoktur.[166]

2.3.1.3.5. Hukuka aykırılık unsuru

Suçun oluşumu için bir fiilin açıkça hukuk düzenine aykırılığı gerekir. Hukuka aykırı olan fiil, hukuk düzenince suç teşkil eder ve cezalandırılır. Fakat, kanun koyucu bazı fiilleri suç oluşturmasına rağmen bazı durumlarda suç olarak değerlendirmez, dolayısıyla da cezalandırmaz. Bu durumlara hukuka uygunluk sebepleri denir. Suçun oluşması için hukuka uygunluk sebeplerinin bulunmaması gerekir.[167] Genel olarak hukuka uygunluk sebepleri, kanunun hükmünü icra (TCK 24/1), yetkili merciin hukuka uygun olan emrini yerine getirme (TCK 24/2)[168], meşru savunma (TCK 25/1), hakkın icrası (TCK 26/1), ilgili kişi veya hak sahibinin rızası (TCK 26/2)'dır.[169]

Bilişim sistemine hukuka aykırı olarak girme veya orada kalmaya devam etme suçu bakımından özel bir hukuka uygunluk nedeni söz konusu değildir. Genel hukuka uygunluk nedenleri burada da geçerli olacaktır. Örneğin, sahibinin rızasıyla girmek ya da bir sözleşmenin tanıdığı hakla sisteme girmek veya kalmaya devam etmek ya da kanun hükmü gereği ya da amirin hukuka uygun emrinin yerine getirilmesi için veya mahkeme kararıyla sisteme girilmiş olması ya da orada kalınması suç oluşturmayacaktır.[170]

Burada özellikle üzerinde durulması gereken konu ise internet üzerinden erişilen bazı internet sitelerine ilişkindir. İnternet aracılığıyla erişilen bazı siteler vardır ki bu sitelere herkes giriş yapabilmektedir. Herhangi bir kişinin bu tarz bir siteye girmiş olması bu suçu oluşturmayacaktır. Yani, bu sitelere belirli kişilerin girebilmesi için belirli şifreleme yöntemi kullanılmamıştır. Dolayısıyla, bu sitelere erişim herkese açıktır. Fakat sadece belirli kişilerin siteye erişimini sağlamaya yönelik bir şifreleme

---

[166]Parlar, 2011, a.g.k., 17-18.; Erol, 2010, a.g.k., 3747.; K. Doğan (2005). Bilişim Suçları ve Yeni Türk Ceza Kanunu. *Hukuk ve Adalet Eleştirel Hukuk Dergisi*. (6-7), s. 297.; Mahmutoğlu, 2013, a.g.k., 862.

[167]Artuk, Gökçen ve Yenidünya, 2016, a.g.k., 378-380.; Soyaslan, 2012, a.g.k., 363.; Benzer görüşteki Akbulut'a göre, hukuka aykırılık suçun unsuru niteliğini taşımaktadır ve hukuka uygunluk nedenleri gerçekleşmişse fiilin haksızlığından bahsedilemeyeceğinden dolayı suç oluşmayacaktır. Akbulut, 2016, a.g.k., 413-414.

[168]Yetkili mercii tarafından verilen ve fakat hukuka aykırı olan emrin yerine getirilmesi hukuka uygunluk nedeni değil kusurluluğu ortadan kaldıran bir nedendir (Anayasa 137, TCK 24). Çünkü üstün, hukuka aykırı emrini yerine getiren astın hareketi, hukuka uygun hale gelmemektedir. Ancak, bu durumda astın kusuru da bulunmamaktadır, dolayısıyla ast cezalandırılmayacaktır. Bkz. Hakeri, 2014, a.g.k., 379-383.; Demirbaş, 2016, a.g.k., 280-283.; Artuk, Gökçen ve Yenidünya, 2016, a.g.k., 488-491.; Akbulut, 2016, a.g.k., 517-519.

[169]Soyaslan, 2012, a.g.k., 373.; Hukuka uygunluk sebepleri ile ilgili ayrıntılı bilgi için bkz. Artuk, Gökçen ve Yenidünya, 2016, a.g.k., 383-476.

[170]Karakehya, 2009, a.g.k., 16.; Parlar, 2011, a.g.k., 18.; Kurt, 2005, a.g.k., 158.; Doğan, 2005, a.g.k., 297.

yapıldıysa ve fail bu şifreyi hukuka aykırı olarak kırmak suretiyle siteye erişim sağlamışsa bu fiil suç oluşturacaktır.[171]

2.3.1.3.6. Suçun nitelikli halleri

2.3.1.3.6.1. Daha hafif cezayı gerektiren nitelikli hal

Kanun koyucu 243. maddenin 2. fıkrasında, bu suç açısından daha hafif cezayı gerektiren nitelikli hal öngörmüştür. Bu fıkraya göre, bilişim sistemine hukuka aykırı olarak girme veya orada kalmaya devam etme fiili bedeli karşılığı yararlanılabilen sistemler hakkında işlenirse birinci fıkrada öngörülen ceza yarı oranında indirilecektir.

Böyle bir cezayı hafifleten halin öngörülmüş olmasının sebebi, korunan hukuki yararla ilgilidir. Bilişim sistemine hukuka aykırı erişim suçunda korunan değer, kişinin dijital ortamdaki özel hayatıdır. Fakat, bedeli karşılığı yararlanılabilen sistemlere karşı bu suçun işlenmesinde kişinin mahremiyeti yerini ekonomik menfaate bırakmaktadır. Bu sebepten dolayı da kanun koyucu ekonomik menfaati kişi mahremiyetine göre daha önemsiz gördüğünden böyle bir hafifletici hal düzenlemiştir.[172] Kanaatimizce, kanun koyucunun kişi mahremiyetini ekonomik menfaatten üstün tutması isabetli olmuştur. Ancak, doktrinde kimi yazarlar tarafından bu hüküm eleştirilmekte, suçla ihlal edilen menfaatin sadece ekonomik olmadığı ayrıca bedeli ödenmeden sistemin kullanılmasından ötürü bilişim sisteminin işleticisinin sistem üzerindeki haklarının da ihlal edildiği, dolayısıyla böyle bir hafifletici nedenin gereksiz olduğu düşünülmektedir.[173]

Kanun'da ya da gerekçede bedeli karşılığı yararlanılabilen sistem ifadesinden ne anlaşılması gerektiğine dair bir açıklama yoktur. Fakat, bu sistemin bir bilişim sistemi olduğu şüphesizdir. Bedeli karşılığı yararlanılabilen sistem kavramından, internet üzerinden ücret karşılığı hizmet veren web siteleri, manuel olarak girilebilen bilişim sistemleri, belirli bir bedel ile bilişim sisteminin kiralanması imkanı sağlayan internet

[171]Karakehya, 2009, a.g.k., 16-17.
[172]Yaşar, Gökçan ve Artuç, 2010, a.g.k., 6749.; Artuk, Gökçen ve Yenidünya, 2015, a.g.k., 874.; Kurt, 2005, a.g.k., 147.; Koca ve Üzülmez, 2016, a.g.k., 816.; Karagülmez, 2010, a.g.k., 242.
[173]Özbek, Doğan, Bacaksız ve Tepe, 2016, a.g.k., 939.; Doğan'a göre, bu durumda cezanın hafifletilmesi değil bilakis ağırlaştırılması gerekir. Bkz. Doğan, 2005, a.g.k., 299.

kafeler anlaşılabilir.[174]

Belirtmek gerekir ki karşılıksız yararlanma suçunun konusunu oluşturan otomatlar bu fıkra kapsamına girmemektedir. Çünkü, TCK 163. maddede otomatlar aracılığı ile sunulan ve bedeli ödendiği takdirde yararlanılabilen bir hizmetten ödeme yapmadan yararlanmak zaten ayrı bir suç tipi olarak öngörülmüştür.[175] Aynı şekilde dekoderler [176] de bu madde kapsamında değerlendirilemez. Çünkü, 163. maddenin 2. fıkrasında telefon hatları ile frekanslarından veya elektromanyetik dalgalarla yapılan şifreli veya şifresiz yayınlardan sahibinin veya zilyedinin rızası olmadan yararlanan kişinin eylemi suç olarak düzenlenmiştir.[177]

2.3.1.3.6.2. Daha ağır cezayı gerektiren nitelikli hal

243. maddenin 3. fıkrasında bu suç açısından daha ağır cezayı gerektiren nitelikli hal öngörülmüştür. Bu fıkraya göre; 1. fıkrada öngörülen fiiller nedeniyle sistemin içerdiği veriler yok olur veya değişirse faile 1. fıkradaki cezadan daha ağır bir ceza verilecektir.

Bu hükmün uygulanabilmesi için failin verileri yok etmek veya değiştirmek kastıyla hareket etmemiş olması gerekir. Buradaki sonuç failin taksirli hareketiyle meydana gelmektedir. Madde metninde "yok olur veya değişirse" denilerek bu fıkradaki suçun oluşumu için manevi unsur olarak kastın değil, taksirin gerektiği belirtilmiştir. Eğer fail, fiilini gerçekleştirirken verileri yok etmek veya değiştirmek kastıyla hareket ederse bu halde 243/3. madde değil, 244/2. madde uygulama alanı bulacaktır.[178] Nitekim 243. maddenin gerekçesinde de bu hükmün uygulanabilmesi için failin verileri yok etmek veya değiştirmek kastıyla hareket etmemesi gerektiği ayrıca bu fıkrada düzenlenen suçun neticesi sebebiyle ağırlaşan suç olduğu açıkça belirtilmiştir.

Fıkrada sözü edilen veri, gerekçede şu şekilde açıklanmıştır: "veri, sistem içindeki bütün soyut unsurları ifade etmektedir."

---

[174]Artuk, Gökçen ve Yenidünya, 2015, a.g.k., 875.; Dülger, 2013, a.g.k., 351-352.; Tezcan, Erdem, Önok'a göre, internet kafeler, bedeli karşılığında yararlanılabilen sistemler kapsamına girmemektedir. Bkz. Tezcan, Erdem ve Önok, 2017, a.g.k., 982.

[175]Dülger, 2013, a.g.k., 351.

[176]Dekoder: kendilerine gönderilen şifreli bilgiyi alıp, işleme tabi tutup üzerindeki yüklü programları veri üzerine uygulayıp, bundan farklı bir veri çıkartıp, alıcıya ulaştıran bilişim sistemleridir. Bkz. Artuk, Gökçen ve Yenidünya, 2009, a.g.k., 4651.

[177]Yaşar, Gökçan ve Artuç, 2010, a.g.k., 6750.; Erdoğan, 2012, a.g.k., 1398.

[178]Erdağ, 2010, a.g.k., 284.; Parlar, 2011, a.g.k., 19.; Erdoğan, 2012, a.g.k., 1403.; Yaşar, Gökçan, Artuç, 2010, a.g.k., 6748.; Koca ve Üzülmez, 2016, a.g.k., 817.; Karagülmez, 2010, a.g.k., 243-244.

2.3.1.3.7. Suçun özel görünüş şekilleri

2.3.1.3.7.1. Teşebbüs

Suça teşebbüs, elverişli vasıta ile bir suçun icrasına başlandıktan sonra, failin elinde olmayan sebeplerden dolayı icra hareketlerinin veya neticenin tamamlanamamasını ifade etmektedir.[179] Buradan da anlaşılacağı üzere teşebbüsten bahsedebilmek için, suçun kasten işlenebilen bir suç olması, elverişli hareketlerle suçun icrasına başlanmış olması ve failin elinde olmayan sebeplerle icra hareketlerini bitirememiş olması ya da neticenin gerçekleşmemesi gerekir. Teşebbüs TCK'nın 35. maddesinde düzenlenmiştir.[180]

Bilişim sistemine hukuka aykırı olarak girmek veya orada kalmaya devam etmek suçu teşebbüse elverişlidir. Yukarıda da belirttiğimiz gibi suç, neticesiz bir suç olduğu için fail tarafından elverişli vasıtalarla icra hareketlerinin yapılmış olması suçun oluşumu için yeterlidir. Ayrıca bir zarar meydana gelmiş olması gerekmez. Bilişim sistemine hukuka aykırı olarak girme açısından teşebbüs, elverişli vasıtalarla suçun icra hareketlerine başlanması ve fakat failin elinde olmayan sebeplerle icra hareketlerinin tamamlanamaması halinde mümkündür. Elverişli vasıta olmaksızın sisteme girmeye çalışılması halinde işlenemez suç söz konusu olur. Örneğin, yüksek güvenlikli kodlama sistemiyle korunan bir bilişim sisteminin şifresini deneme yanılma yöntemiyle çözmeye çalışan herhangi bir internet kullanıcısının bu fiili işlenemez suç oluşturur, ancak şifre kırma konusunda uzman olan kimsenin bir bilişim sistemine girmeye çalışması ve fakat kıl payı bunu başaramaması halinde teşebbüs söz konusu olur.[181]

Teşebbüs durumuna bir başka örnek vermek gerekirse, örneğin fail bilişim sistemine girmek için gerekli olan şifreyi ele geçirmişse ve sisteme girmek üzere ise fakat bu esnada elektrik kesintisi yaşanmışsa, bilgisayarda herhangi bir teknik arıza

---

[179]Teşebbüsle ilgili ayrıntılı bilgi için bkz. Artuk, Gökçen ve Yenidünya, 2016, a.g.k., 586-615.; Demirbaş, 2016, a.g.k., 448-465.; Akbulut, 2016, a.g.k., 548-572.; Hakeri, 2014, a.g.k., 456-487.

[180]Suça teşebbüs

Madde 35- (1) Kişi, işlemeyi kastettiği bir suçu elverişli hareketlerle doğrudan doğruya icraya başlayıp da elinde olmayan nedenlerle tamamlayamaz ise teşebbüsten dolayı sorumlu tutulur.

(2) Suça teşebbüs halinde fail, meydana gelen zarar veya tehlikenin ağırlığına göre, ağırlaştırılmış müebbet hapis cezası yerine onüç yıldan yirmi yıla kadar, müebbet hapis cezası yerine dokuz yıldan onbeş yıla kadar hapis cezası ile cezalandırılır. Diğer hallerde verilecek cezanın dörtte birinden dörtte üçüne kadarı indirilir.

[181]Karakehya, 2009, a.g.k., 19.

meydana gelmişse ya da internet bağlantısı kesilmişse yine suçun teşebbüs aşamasında kaldığını kabul etmek gerekir.

Bilişim sisteminde hukuka aykırı olarak kalmaya devam etme açısından suçun teşebbüse elverişli olup olmadığıyla ilgili doktrinde farklı görüşler ileri sürülmüştür. Bir görüşe göre, sisteme girildikten sonra sistemde kalmanın başarılamaması halinde somut duruma göre teşebbüse ilişkin değerlendirme yapılması gerekmektedir.[182] Diğer bir görüşe göre, suçla korunan hukuki yararlar, sistem sahibinin özel hayatı, huzur ve sükunu, sırrın masuniyeti ve verilerin gizliliği olduğundan failin bahsedilen değerleri ihlal edecek kadar sistemde kalmış olması tamamlanmış bir suç oluşturacaktır. Aksi halde teşebbüsten söz edilecektir. Süreyi ise hakim takdir edecektir.[183] Bir başka görüşe göre ise, suç failin sisteme girmesi ve çok kısa bir süre de olsa sistemde kalması ile tamamlanacağından, benzer olaylar için hakimlerin farklı yorumuyla faillerden bazıları tamamlanmış suçtan bazıları ise teşebbüsten sorumlu tutulacağı böylece adil olmayan sonuçlar doğacağından bu suç açısından suça teşebbüs uygulanmamalıdır.[184]

Kanaatimizce, bilişim sisteminde kalmaya devam etme suçu bakımından teşebbüs mümkündür. Doktrindeki sürenin tespitinin zor olduğu, benzer olaylarda faillerin bazılarının teşebbüsten bazılarının tamamlanmış suçtan cezalandırılacağı uygulama birliğinin olmayacağına yönelik görüş haklı görülmekle birlikte, farklı sonuçlar doğacağını düşünerek sisteme girmiş ancak sistem içerisinde mağdurun hukuki yararını ihlal edecek bir fiil gerçekleştirecek kadar kalamamış bir kimseyle, örneğin, sisteme girmiş ve ayrıca mağdurun özel hayatına ilişkin verileri de öğrenebilecek kadar sistemde kalmış kimsenin aynı hukuki durumda olduğunu kabul edip her ikisine tamamlanmış suçtan ceza vermek de adil olmayacaktır. Çünkü, teşebbüsün mümkün olmadığının kabulü halinde sistemde çok kısa bir süre bile kalmış olan fail tamamlanmış suçtan sorumlu tutulacağından hakkında fazla ceza tayin edilmiş olacaktır. Dolayısıyla, failin mağdurun yukarıda bahsetmiş olduğumuz korunan hukuki yararlarını ihlal edecek kadar bir süre (somut duruma göre bu süre birkaç saniye ya da birkaç

[182]Karagülmez, 2009, a.g.k., 187.
[183]Kurt, 2005, a.g.k., 154,155.
[184]Ş.C. Taşkın (2008). *Bilişim Suçları*. İstanbul: Beta Yayınevi, s. 29-30..; Tezcan, Erdem ve Önok'a göre suç tamamlanmış ya da tamamlanmamıştır, teşebbüs hali bu suç için söz konusu olamaz. Bkz. Tezcan , Erdem ve Önok, a.g.k., 984.

dakika olabilir) sistemde kalmış olması durumunda suçun tamamlandığının aksi takdirde suçun teşebbüs aşamasında kaldığının kabulü gerekir.

2.3.1.3.7.2. İştirak

Kanunda tek kişi tarafından işlenebileceği belirtilen suçların birden fazla kişi tarafından işlenmesi halinde iştirak söz konusu olur.[185] TCK'ya göre iştirak, faillik ve suç ortaklığı (şeriklik) şeklinde gerçekleşebilir. Faillik TCK'nın 37. maddesinde düzenlenmiştir. [186] Suç ortaklığı (şeriklik) ise azmettirme (TCK 38) ve yardım etme (TCK 39) olmak üzere iki şekilde meydana gelebilir. [187]

Bilişim sistemine hukuka aykırı olarak girme veya orada kalmaya devam etme suçu iştirak açısından bir özellik göstermez.

2.3.1.3.7.3. İçtima

Ceza hukukunda fiil kadar suç ve suç kadar ceza kuralı geçerlidir. Suçların içtiması ise bu kuralın istisnasıdır. İçtima durumunda oluşan her suç için ayrı ceza verilmez, bunun yerine birden fazla suç tek suç kabul edilip suç için öngörülen ceza artırılarak verilir ya da en ağır cezayı gerektiren suçtan cezalandırma yoluna gidilir.[188] TCK'da suçların içtimaı başlığı altında içtimanın 3 farklı şekline yer verilmiştir. Bunlar

---

[185]İştirak ile ilgili ayrıntılı bilgi için bkz. Artuk, Gökçen ve Yenidünya, 2016, a.g.k., 630-688.; Demirbaş, 2016, a.g.k., 485-524.; Hakeri, 2014, a.g.k., 508-566.; Akbulut, 2016, a.g.k., 592-657.

[186]Faillik

Madde 37- (1) Suçun kanuni tanımında yer alan fiili birlikte gerçekleştiren kişilerden her biri, fail olarak sorumlu olur.

(2) Suçun işlenmesinde bir başkasını araç olarak kullanan kişi de fail olarak sorumlu tutulur. Kusur yeteneği olmayanları suçun işlenmesinde araç olarak kullanan kişinin cezası, üçte birden yarısına kadar artırılır.

[187]Azmettirme

Madde 38- (1) Başkasını suç işlemeye azmettiren kişi, işlenen suçun cezası ile cezalandırılır.

(2) Üstsoy ve altsoy ilişkisinden doğan nüfuz kullanılmak suretiyle suça azmettirme halinde, azmettirenin cezası üçte birden yarısına kadar artırılır. Çocukların suça azmettirilmesi halinde, bu fıkra hükmüne göre cezanın artırılabilmesi için üstsoy ve altsoy ilişkisinin varlığı aranmaz.

(3) Azmettirenin belli olmaması halinde, kim olduğunun ortaya çıkmasını sağlayan fail veya diğer suç ortağı hakkında ağırlaştırılmış müebbet hapis cezası yerine yirmi yıldan yirmibeş yıla kadar, müebbet hapis cezası yerine onbeş yıldan yirmi yıla kadar hapis cezasına hükmolunabilir. Diğer hallerde verilecek cezada, üçte bir oranında indirim yapılabilir.

Yardım etme

Madde 39- (1) Suçun işlenmesine yardım eden kişiye, işlenen suçun ağırlaştırılmış müebbet hapis cezasını gerektirmesi halinde, onbeş yıldan yirmi yıla; müebbet hapis cezasını gerektirmesi halinde, on yıldan onbeş yıla kadar hapis cezası verilir. Diğer hallerde cezanın yarısı indirilir. Ancak, bu durumda verilecek ceza sekiz yılı geçemez.

(2) Aşağıdaki hallerde kişi, işlenen suçtan dolayı yardım eden sıfatıyla sorumlu olur:

a) Suç işlemeye teşvik etmek veya suç işleme kararını kuvvetlendirmek veya fiilin işlenmesinden sonra yardımda bulunacağını vaat etmek.

b) Suçun nasıl işleneceği hususunda yol göstermek veya fiilin işlenmesinde kullanılan araçları sağlamak.

c) Suçun işlenmesinden önce veya işlenmesi sırasında yardımda bulunarak icrasını kolaylaştırmak.

[188]İçtima ile ilgili ayrıntılı bilgi için bkz. Artuk, Gökçen ve Yenidünya, 2016, a.g.k., 688-728.; Demirbaş, 2016, a.g.k., 524-545.; Hakeri, 2014, a.g.k., 571-618.; Akbulut, 2016, a.g.k., 658-730.

bileşik suç, zincirleme suç ve fikri içtimadır. 42. maddede bileşik suç, biri diğerinin unsurunu veya ağırlaştırıcı nedenini oluşturması dolayısıyla tek fiil sayılan suç şeklinde tanımlanmış ve bu tür suçlarda içtima hükümlerinin uygulanmayacağı belirtilmiştir. 43. maddede zincirleme suç düzenlenmiştir. Zincirleme suç, bir suç işleme kararının icrası kapsamında değişik zamanlarda, bir kişiye karşı aynı suçun birden fazla kez işlenmesi ya da aynı suçun birden fazla kişiye karşı tek fiille işlenmesi şeklinde gerçekleşebilir. Fikri içtima durumunda ise kanunun 44. maddesi gereği işlediği bir fiil ile birden fazla farklı suçun oluşmasına sebebiyet vermiş olan kişiye, bunlardan en ağır cezayı gerektiren suçtan dolayı ceza verilecektir.

Bilişim sistemine hukuka aykırı olarak girme suçunda zincirleme suç hükümleri uygulanabilir. Örneğin, failin aynı suç işleme kararı kapsamında, aynı kimseye ait bir ya da birden fazla bilişim sistemine farklı zamanlarda girmesi durumunda zincirleme suç oluşacaktır. Ancak, fail uzun zaman aralıklarıyla birden fazla kez sisteme giriş yapıyorsa artık aynı suç işleme kararı kapsamında hareket ettiği kabul edilemeyeceğinden failin her fiili için ayrı cezalandırılması gerekmektedir.[189]

Bilişim sisteminde hukuka aykırı olarak kalmaya devam etme suçunda zincirleme suç hükümleri uygulanabilir. Örneğin, fail çalışmış olduğu işyerinde farklı zamanlarda bir suç işleme kararının icrası kapsamında mesai arkadaşının açık (girilmiş) olan bir ya da birden fazla bilişim sisteminde kalmaya devam ediyorsa zincirleme suç söz konusu olabilecektir.

Suç oluşturan seçimlik hareketlerden bilişim sistemine hukuka aykırı olarak girme veya orada kalmaya devam etme hareketleri aynı mağdurun bir ya da birden fazla bilişim sistemine karşı bir suç işleme kararının icrası kapsamında gerçekleştirilirse yine zincirleme suç hükümleri uygulanabilir. Örneğin, fail aynı mağdura ait bir ya da birden fazla bilişim sistemine ilk seferde girmeyi başarmış ve fakat bir şekilde kalmayı başaramamışsa ikinci seferde sisteme girmiş ve bir süre orada kalmışsa üçüncü seferde ise açık (girilmiş) olan bilişim sisteminde bir süre kalmışsa ve bu fiillerin aynı suç işleme kararının icrası kapsamında işlendiği kabul edilebiliyorsa zincirleme suç hükümleri uygulanmalıdır.

Fikri içtima açısından suç incelendiğinde, bilişim sistemine hukuka aykırı olarak

[189]Dülger, 2013, a.g.k., 379.; .Karakehya, 2009, a.g.k., 20.

girilmesi veya orada kalınması fiilleri bu suç yanında bir başka suçu daha oluşturabilir. Failin, bilişim sistemine girdikten sonra örneğin, mağdura ait kişisel bilgileri ele geçirmesi ya da bu suretle hırsızlık, dolandırıcılık gibi suçları işlemesi veyahut bilişim sistemine ya da sistemde yer alan verilere zarar vermesi durumunda nasıl bir yol izleneceği konusunda doktrinde farklı görüşler ileri sürülmüştür. Bir görüşe göre, bilişim sistemine girme veya orada kalmaya devam etme, bilişim sistemlerine girerek işlenmesi zorunlu olan suçlar açısından araç suç niteliği taşımaktadır. Böyle bir durumda failin amaç olarak işlemek istediği suç her ne ise sadece ona göre cezalandırılmalıdır.[190] Benzer bir görüşe göre, bu suç geçit suç oluşturmaktadır ve fail bu suçu işleyerek örneğin, özel hayatın gizliliğinin ihlali, kişisel verilerin ele geçirilmesi, bilişim sistemlerinin araç olarak kullanılması suretiyle hırsızlık veya dolandırıcılık suçunu da işlediyse TCK 44 gereği bu suçtan değil, cezası daha ağır olan bahsettiğimiz suçlardan cezalandırılacaktır.[191] Bir başka görüşe göre, bilişim sistemine girme veya orada kalmaya devam etme suçuyla örneğin, bilişim sistemine zarar verme, özel hayatın gizliliğini ihlal vb. bir suç birlikte gerçekleşmesi durumunda bu suçla diğer suçlar arasında geçit suçu ilişkisi bulunmamaktadır.[192] Buraya kadar yer verdiğimiz görüşler kanun metnindeki "ve" ifadesi "veya" olarak değiştirilmeden önceki döneme ilişkindi. Yasa değişikliği sonrası dönemdeki bir görüşe göre ise, araç suç amaç suç ilişkisinin olduğu durumlarda suçları oluşturan icra hareketleri arasında kısmen veya tamamen bir örtüşme yoksa fail her suçtan ayrı cezalandırılmalıdır.[193]

Kanaatimizce, bilişim sistemine girme veya orada kalmaya devam etme suçunda fail, bilişim sistemine ya da sistemde yer alan verilere zarar verme kastıyla hareket ediyorsa artık bu durumda 243. maddenin uygulanmaması gerekir, çünkü failin amaçladığı suçu işleyebilmesi için bu suçu zaten işlemesi gerekmektedir. Dolayısıyla, böyle bir durumda bu suç araç suç niteliği taşımaktadır. Fail sadece 244. madde uyarınca cezalandırılmalıdır. Aynı şekilde kanunda suçun nitelikli halleri olarak düzenlenen bilişim sistemlerinin araç olarak kullanılması suretiyle dolandırıcılık ve hırsızlık suçlarının işlenebilmesi için de bilişim sistemlerine girilmiş ya da orada kalınmış olması gerektiğinden failin ayrıca 243. maddeye göre cezalandırılmaması

[190]Artuk, Gökçen ve Yenidünya, 2016, a.g.k., 4655.
[191]Taşkın, 2008, a.g.k., 33-34.
[192]Dülger, 2016, a.g.k., 380-384.
[193]Koca ve Üzülmez, 2016, a.g.k., 818-819.; Benzer görüş için bkz. Tezcan, Erdem ve Önok, 2017, a.g.k., 984-985.

gerekir. Ancak, fail, bilişim sistemine girmesi veya orada kalmaya devam etmesiyle örneğin kişisel verileri ele geçirmiş ya da özel hayatın gizliliğini ihlal etmişse ve suçların icra hareketleri arasında da örtüşme yoksa failin her iki suçtan da cezalandırılması gerekir.

2.3.1.3.8. Yaptırım, soruşturma ve kovuşturma

Bilişim sistemine hukuka aykırı olarak girme veya orada kalmaya devam etme suçunda kanun koyucu, hapis cezası ile adli para cezasını seçimlik yaptırım olarak düzenlemiştir. Faile, kanunun açık hükmü gereği hem hapis cezası hem de adli para cezası verilemez. Suçun üst sınırının bir yıl hapis veya adli para cezası olduğu belirtilmiş, fakat alt sınırın ne olduğuna dair madde metninde bir düzenleme yapılmamıştır. Suçun yaptırımı genel hükümlere göre belirlenecektir.

Bilişim sistemine hukuka aykırı girme veya orada kalmaya devam etme suçu 2. fıkrada belirtildiği gibi bedeli karşılığı yararlanılabilen sistemler aracılığıyla işlenirse, faile birinci fıkra gereğince verilmiş olan cezada yarı oranına kadar indirim yapılacaktır.

3. fıkrada düzenlenmiş olan suçun neticesi sebebiyle ağırlaşmış hali gerçekleşirse, faile daha ağır ceza verilecektir. Bu cezanın alt sınırı altı ay, üst sınırı ise iki yıl hapis cezasıdır.

Görevli mahkeme, 5235 sayılı Adli Yargı İlk Derece Mahkemeleri ile Bölge Adliye Mahkemelerinin Kuruluş, Görev ve Yetkileri Hakkında Kanun'un 11. ve 12. maddelerine göre asliye ceza mahkemeleridir. 2. ve 3. fıkradaki suçun nitelikli hallerinde de asliye ceza mahkemeleri görevlidir. Suçun takibi şikayete bağlı değildir, resen soruşturulur.

2.3.1.4. Bilişim sistemine girmeksizin teknik araçlarla veri nakillerini izleme (TCK 243/4)

2.3.1.4.1. Genel olarak

243. maddeye, 24/3/2016 tarihli ve 6698 Sayılı Kişisel Verilerin Korunması Hakkındaki Kanun'un 30. maddesiyle yeni bir fıkra eklenmiştir. Fıkranın metni şu şekildedir: "Bir bilişim sisteminin kendi içinde veya bilişim sistemleri arasında gerçekleşen veri nakillerini, sisteme girmeksizin teknik araçlarla hukuka aykırı olarak izleyen kişi, bir yıldan üç yıla kadar hapis cezası ile cezalandırılır."

Kanun koyucu bu düzenlemeyle, bilişim sisteminin ve sistemde yer alan verilerin daha etkin olarak korunmasını amaçlamıştır. Ayrıca, bu suç tipiyle kanun koyucunun ASSS'nin 3. maddesinde düzenlenmiş olan kanunsuz araya girme başlıklı yükümlülüğünü de yerine getirdiği söylenebilir. Sözleşmede suçun oluşması için veri nakillerinin izlenmesinde, teknik yöntemler kullanılması gerekirken, kanunda teknik araçlar kullanılması şartı aranmış, bunun yanı sıra sözleşmede sistemden elektromanyetik dalgalarla yayılma da sistemler arasındaki iletimin bir parçası olarak kabul edilmiştir.

Gelişen teknolojiyle birlikte bilişim alanında kişilerin güvenliğini daha etkin sağlayabilmek ve olası saldırıları önleyebilmek için bu suç tipinin kanuna eklenmesi isabetli olmuştur, ancak kanun sistematiği açısından bakıldığında, bilişim sistemine girmeksizin teknik araçlarla işlenmesi mümkün olan bu suçun bilişim sistemine girme başlığını taşıyan 243. maddede düzenlenmesi kanımızca isabetsiz olmuştur. Bunun yerine, ayrı bir madde olarak düzenlenmesi daha uygun olurdu. Çünkü, bilişim sistemine girmeksizin veri nakillerinin teknik araçlarla izlenmesi ayrı bir suç tipidir, unsurları itibariyle bilişim sistemine hukuka aykırı erişim suçuyla farklılık arz etmektedir ve bu farklılıklar ayrıca incelenmelidir.

2.3.1.4.2. Korunan Hukuki yarar

Suçla korunan hukuki yarar bilişim sistemine hukuka aykırı olarak girme veya sistemde kalmaya devam etme suçuyla benzerdir, bu düzenleme kişilerin dijital ortamdaki özel alanına müdahaleyi engellemeye yöneliktir.

Korunan hukuki yararların özel hayatın gizliliğinin ihlali, sırrın masuniyeti, haberleşme özgürlüğü, bilişim sistemi sahibi ya da ilgilisinin sistem üzerindeki tasarruf hakkı olduğu söylenebilir. Bilişim sistemlerinde sistemin kullanım alanına göre, kişilerin özel bilgileri, firmaların ticari sırları, kamu kurumlarının yürüttükleri faaliyetlere ilişkin verileri bulunabilmektedir. Kanun koyucu burada mahiyeti itibariyle önemli ve gizli kalması gereken verileri barındıran bilişim sistemlerinin, sisteme girilmeksizin teknik araçlarla izlenmesi suretiyle sistemde bulunan verilerin failler tarafından öğrenilmesini cezalandırmak istemiştir.

Suçla korunan bir başka hukuki yarar ise bilişim sisteminin düzenli işleyişi ve güvenliğidir. Ayrıca, bu suçla bilişim sistemlerine oluşan güven duygusu

korunmaktadır**.**

2.3.1.4.3. Maddi Unsur

2.3.1.4.3.1. Fiil

Suçun maddi unsurunu, bilişim sistemlerinde gerçekleşen veri nakillerini sisteme girmeksizin teknik araçlarla izlemek oluşturur. Bu fıkradaki suç, serbest hareketli bir suç değildir. Suçun oluşumu için kanun koyucu veri nakillerinin sisteme girmeksizin teknik araçlarla izlenmesini suç olarak düzenlenmiştir. Failin sisteme girmesi ya da başkasının girmiş olduğu sistemde kalmaya devam etmesi halinde bu suç değil, 243/1. maddedeki suç oluşur.[194]

Burada özellikle, teknik araç kavramı üzerinde durmak gerekir. Teknik araç, insanın görme ve işitme duyusunun, algılama yeteneğinin sınırlarını aşmaya yarayan her türlü alete denmektedir. Teknik araçlar fonksiyonlarına göre ikiye ayrılmaktadır. Bunlardan biri, optik gözetlemeye yarayan teknik araçlar diğeri ise akustik gözetlemeye yarayan teknik araçlardır. Akustik gözetlemeye yarayan teknik araçlara, mini mikrofonlar, dinleyiciler ve gönderdikleri sinyallerle herhangi bir aracın ya da eşyanın yerini tespit edebilen cihazlar örnek verilebilir. Optik gözetlemeye yarayan teknik araçlara da video kameralar, fotoğraf makineleri, dürbünler, gece görüşü sağlayan kızıl ötesi araçlar örnek olarak verilebilir. Bunların yanı sıra, kullanılan aracın teknik kapasitesine göre bu iki fonksiyonu bir arada gerçekleştiren cihazlar da vardır.[195] Teknik araçlarla izleme ise, belli bir yerdeki seslerin, konuşmaların, görüntülerin, kişilerin eylemlerinin tespiti amacıyla yapılan belli bir yerin dinlenmesi ya da görüntülenmesi işlemidir.[196]

Teknik araçlarla izleme Ceza Muhakemesi Kanunu (CMK)'nda bir koruma tedbiri olarak düzenlenmiştir. CMK 140. maddesinde hangi suçlar açısından bu koruma tedbirine başvurulacağı tahdidi olarak sayılmıştır. Fakat, teknik araçlarla izlemenin ne olduğuna dair bir açıklamaya madde metninde yer verilmemiştir. Teknik araçlarla izlemeye dair mevzuatta yer alan bir başka düzenleme olan Ceza Muhakemesi Kanunu'nda Öngörülen Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi,

[194]Tezcan, Erdem ve Önok, 2017, a.g.k., 986.
[195]B. Öztürk (2015). *Nazari ve Uygulamalı Ceza Muhakemesi Hukuku.* (9. Baskı). Ankara: Seçkin Yayınevi, s. 560.
[196]Y. Ünver ve H. Hakeri (2015). *Ceza Muhakemesi Hukuku*.(10. Baskı). Ankara: Adalet Yayınevi, s. 484.

Gizli Soruşturmacı ve Teknik Araçlarla İzleme Tedbirlerinin Uygulanmasına İlişkin Yönetmelik'te, CMK'da yer verilen teknik araçlarla izleme koruma tedbirindeki izlemeden maksadın, belirli bir süre devam eden kişilerin hareket veya ilişkilerinin görüntülenmesi ya da yaptıkları konuşmalarının tespiti amacını güden işlemler olduğu belirtilmiştir.

Teknik araçlar ve yöntemler ile sisteme dahil olmaksızın, sistemin ve sistemde yer alan verilerin güvenliğini ve gizliliğini ihlal eden fiillerin varlığı suçun oluşumu için yeterlidir. Yani fail veri nakledilirken bahsedilen teknik araçlarla bu veriyi sisteme girmeksizin izlemiş olmalıdır.[197] Bilişim sistemlerindeki veri akışını izlemek için kullanılan sniffing yöntemi ya da ağ trafiğini izlemeye yarayan wireshark programı bu suça örnek olarak verilebilir.[198]

2.3.1.4.3.2. Fail ve mağdur

Suç fail ve mağdur açısından özellik göstermez. Bilişim sistemlerindeki veri nakillerini sisteme girmeksizin teknik araçlarla izleyen herhangi bir kişi suçun faili olabilir. Suçun mağduru ise, teknik araçlarla veri nakilleri izlenen bilişim sistemleri üzerinde tasarruf yetkisi bulunan kimsedir.

2.3.1.4.3.3. Netice

Sistemler arasında gerçekleşen veri nakillerinin teknik araçlarla izlenmesi suçun oluşması için yeterlidir, failin verilerin içeriği ile ilgili bir bilgiye veya verinin kendisine sahip olması ya da verilerin niteliğinin önemi yoktur.[199] Dolayısıyla, suçun oluşması için bir sonuç meydana gelmiş olması gerekmez, soyut zarar tehlikesi yeterlidir.

2.3.1.4.4. Manevi unsur

Bir bilişim sisteminin kendi içinde veya bilişim sistemleri arasında gerçekleşen veri nakillerini, sisteme girmeksizin teknik araçlarla hukuka aykırı olarak izleme suçu genel kastla işlenebilir. Özel kast aranmaz. Suçun taksirli hali kanunda yer almadığı için cezalandırılmayacaktır.

---

[197]İzlemekten kasıt failin kullandığı teknik araçlarla veriyi adeta havada kapması kontrol etmesi, izlemesidir. Bkz. Koca ve Üzülmez, 2016, a.g.k., 822.

[198]http://www.sertels.av.tr/avukat/hukuk/bilişim-hukuku/yeni-bilişim-suçları-zararli-yazilim-veri-izleme.html (Erişim Tarihi: 10/07/2017)

[199]Tezcan, Erdem ve Önok, 2017, a.g.k., 986.

2.3.1.4.5. Hukuka aykırılık unsuru

Kanun koyucu bu suç açısından herhangi bir hukuka uygunluk sebebi öngörmemiştir.

2.3.1.4.6. Suçun nitelikli halleri

243. maddenin 2. ve 3. fıkralarında suçun nitelikli hallerini yukarıda belirtmiştik. Burada üzerinde önemle durulması gereken husus, bahsedilen nitelikli hallerin 4. fıkra açısından uygulanıp uygulanamayacağıdır. Kanaatimiz uygulanamayacağı yönündedir. Çünkü, kanun sistematiği açısından bakıldığında, kanun koyucu nitelikli hallerin veri nakillerinin teknik araçlarla izlenmesi suçu için geçerli olmasını dileseydi, 243. maddeye son fıkra olarak eklemek yerine 1. fıkradan hemen sonra bu suç tipini 2. fıkra olarak düzenlerdi. Ayrıca, her ne kadar bu suç bilişim sistemine girme başlıklı 243. maddede düzenlenmiş ise de farklı bir suç tipidir. 4. fıkrada açıkça sisteme girmeksizin bu suçun işleneceği belirtilmiştir. Başka bir suç için öngörülmüş olan nitelikli hallerin veri nakillerinin teknik araçlarla izlenmesi suçu için de geçerli olduğunu söylemek suçta ve cezada kanunilik ilkesiyle de bağdaşmayacaktır.[200]

2.3.1.4.7. Suçun özel görünüş şekilleri

2.3.1.4.7.1. Teşebbüs

Teknik araçlarla veri nakillerinin izlenmesi suçunda bir zarar meydana gelmesi suçun oluşması için şart değildir. Neticesiz bir suç olduğundan hareketin tamamlanmasıyla suç oluşacaktır. Bu suç açısından teşebbüs, icra hareketleri parçalara bölünebiliyorsa söz konusu olabilecektir. Kanaatimizce, örneğin, fail veri nakillerini izlemek üzere teknik aracını hazırladıktan sonra izleme fiiline başlamışken araçta bir arıza çıkması, kullanılan teknik aracın elektronik bir cihaz olması ve fiil esnasında elektrik kesintisi yaşanması ya da cihazın şarjının bitmesi, teknik aracın çalışması için internet bağlantısının gerekmesi ancak bağlantı kesilmesi gibi durumlarda teşebbüsten bahsedilebilir.

2.3.1.4.7.2. İştirak

Sistemdeki veri nakillerini teknik araçlarla izleme suçu iştirak açısından bir

[200] Aynı yönde bkz. Tezcan, Erdem ve Önok, 2017, a.g.k., 987.

özellik göstermez.

2.3.1.4.7.3. İçtima

Bilişim sistemlerinde gerçekleşen veri nakillerini teknik araçlarla izlemek suçu zincirleme suç şeklinde işlenebilir. Örneğin, bir kişiye ait bilişim sistemi içerisindeki veri nakillerinin bir suç işleme kararının icrası kapsamında değişik zamanlarda teknik araçlarla izlenmesi halinde faile verilecek ceza zincirleme suç hükümleri uyarınca artırılacaktır. Kanaatimizce failin teknik araçlarla izlemiş olduğu veriler farklı kişilere aitse suç yine zincirleme şekilde işlenmiş sayılmalıdır. Örneğin, fail iki ya da daha fazla bilişim sisteminde karşılıklı olarak gerçekleşen veri naklini izlemişse, verilerin birden fazla kişiye ait ve mağdur sayısının birden fazla olduğunun kabulü halinde failin cezası TCK 43/2 gereği artırılmalıdır. Bu duruma facebook, twitter vb. sosyal medya ağlarındaki veri nakillerinde rastlanılabilir.

Failin yalnızca bilişim sistemine girmeksizin teknik araçlarla veri nakillerini izlemiş olması bu suçu oluşturacaktır. Fail, teknik araçlarla izleme fiiliyle ayrıca veri bütünlüğüne ya da veri nakline müdahale ederse, veri naklini engellerse, verinin içeriğini öğrenirse, verileri izlerken kayda alırsa sadece bu suçtan değil, somut olaya göre haberleşmenin gizliliğinin ihlali, haberleşmenin engellenmesi veya kayda alınması, özel hayatın gizliliğinin ihlali, kişisel verileri ele geçirilmesi suçundan sorumlu olacaktır. Burada gerçek içtima kuralları uygulanmalıdır.[201]

2.3.1.4.8. Yaptırım,soruşturma ve kovuşturma

Kanun koyucu, Bilişim sistemine girmeksizin teknik araçlarla veri nakillerini izleme suçu için hapis cezası öngörmüştür. Hapis cezasının alt sınırı bir yıl, üst sınırı ise üç yıldır.

Görevli mahkeme, 5235 sayılı Adli Yargı İlk Derece Mahkemeleri ile Bölge Adliye Mahkemelerinin Kuruluş, Görev ve Yetkileri Hakkında Kanun'un 11. ve 12. maddelerine göre asliye ceza mahkemeleridir. Suçun takibi şikayete bağlı değildir, resen soruşturulur.

[201]Koca ve Üzülmez, 2016, a.g.k., 822-823.

2.3.1.5. Bilişim sistemine zarar verme suçu (m. 244/1)

2.3.1.5.1. Genel olarak

TCK'nın 244. maddesinde birden fazla suç tipine yer verilmiştir. Maddenin 1. fıkrasında bir bilişim sisteminin işleyişini engellemek veya bozmak, 2. fıkrasında ise bilişim sistemindeki verilere zarar vermek suç olarak düzenlenmiştir.

ASSS'nin sistem müdahalesi başlığını taşıyan 5. maddesine göre, her bir devlet, veri yükleyerek, aktararak, zarar vererek, silerek, bozarak, değiştirerek veya müdahale ederek bilgisayar sisteminin kullanımında hakkı olmadığı halde bilerek ve isteyerek bilgisayarın sisteminin çalışmasını sekteye uğratma fiilini ulusal kanununda suç olarak düzenleme ve gerekli diğer düzenlemeleri yapmakla yükümlüdür. 244/1. maddesi bu yükümlülüğü yerine getirmeye yöneliktir. Bu fıkra, 765 sayılı TCK'da yer alan 525/b-1 maddesinin TCK'daki karşılığıdır.

Ayrıca, 1. fıkradaki düzenleme ASSS'nin bilgisayarla ilişkili sahtekarlık başlıklı 7. maddesi ile bilgisayarla ilgili dolandırıcılık başlıklı 8. maddesindeki yükümlülükleri de yerine getirmeye yönelik unsurlar içermektedir.

3. fıkrada ise suçun ağırlaştırılmış hali düzenlenmiştir. Buna göre, bilişim sistemine veya sistemde yer alan verilere zarar verme suçu bir banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna karşı işlenirse ilk iki fıkraya göre verilecek ceza yarı oranında artırılacaktır.

2.3.1.5.2. Korunan hukuki yarar

ASSS'nin 5. maddesine uygun olarak düzenlenmiş olan bu suç tipi bilgisayar sabotajı olarak nitelendirilen eylemlerin önlenmesini sağlamakta ve bilişim sistemlerinin kullanıcılarının bu sistemleri uygun bir şekilde kullanma haklarını korumaktadır. Ayrıca, bu suç tipiyle bilgisayar verilerine ya da programlarına zarar verilmesini ve veri programların bozulmasını engellemek amaçlanmaktadır. Böylece, bilişim sistemi üzerinde 3. kişiler tarafından gerçekleştirilecek müdahalelere karşı ilgili kişinin tasarrufta bulunabilme yetkisi korunmak istenmektedir.[202]

Kurt'a göre, bilişim sistemine zarar verme suçunda korunan hukuki yararlar,

[202]Ketizmen, 2008, a.g.k., 119.

sistemin ve sistem içinde yer alan verilerin dokunulmazlığı, bilişim sistemi sahibinin ya da zilyedinin sistem üzerindeki mülkiyet hakkı ile teknolojik gelişim özgürlüğüdür.[203]

Maddenin gerekçesinde, 244. madde ile bilişim sistemlerine yöneltilen zarar fiillerinin özel bir suç haline getirildiği ve sistemin fiziki varlığı ve işlemesini sağlayan bütün diğer unsurların bu suçun konusunu oluşturduğu söylenmektedir. Buna göre, bilişim sistemine zarar verme suçunda korunan hukuki değerin, klasik suçlardan olan mala zarar verme suçunun koruduğu hukuki değerle benzer olduğu kabul edilebilir. Yani, bu düzenleme ile sistemin sahibi veya zilyedinin sistem üzerindeki her türlü tasarruf hakkı ve buna bağlı olarak da toplum düzeni korunmaktadır.[204] Aynı düşüncedeki Ketizmen'e göre ise, bu suç tipine kanunda yer verilme sebebi, klasik mala zarar verme suçunun bilişim sistemlerinde sistemin soyut unsuru olan yazılımı meydana getiren veri ve programlara yönelik müdahaleleri kapsayıp kapsamadığına dair tereddütleri ortadan kaldırmaktır.[205]

Burada özellikle belirtmek gerekir ki bu suç, sadece yazılım kısmını değil, donanım kısmını da koruma altına almıştır. Ancak, bilgisayarın donanım unsurları olan kasa, klavye, disket ya da monitöre yönelik salt kişinin malvarlığına zarar vermeyi amaçlayan fiiller bakımından bu suç değil, TCK'nın 151. maddesindeki mala zarar verme suçu oluşacaktır. Bunun dışında fail, donanım unsurlarına zarar vermek suretiyle bilişim sisteminin çalışmasını engellemeyi amaçlıyorsa bu suç oluşacaktır.[206]

Bilişim sisteminin işleyişine yönelik gerçekleştirilecek fiiller, internetin gündelik hayatımızdaki önemi dikkate alındığında haberleşme özgürlüğünü de sınırlayan hatta ortadan kaldıran bir niteliğe de sahiptir. Dolayısıyla, bu suçun koruduğu hukuki değerler arasında haberleşme özgürlüğü de vardır.[207]

Bu suçla korunan bir başka hukuki değer ise toplumun, bilişim sistemlerinin işleyişine olan güvenleri ve ekonomik düzenin sağlıklı işleyişidir. Bu sebepten dolayı da kanun sistematiği içerisinde bilişim sistemine veya sistemde yer alan verilere zarar

[203]Kurt, 2005, a.g.k., 162.
[204]S. Yılmaz (2011). 5237 Sayılı TCK'nın 244. Maddesinde Düzenlenen Bilişim Alanındaki Suçlar. *TBB Dergisi*, (92), s. 68.
[205]Ketizmen, 2008, a.g.k., 128.; Benzer görüş için bkz. Tezcan, Erdem ve Önok, 2017, a.g.k., 954.
[206]Dülger, 2013, a.g.k., 390.
[207]Artuk, Gökçen ve Yenidünya, 2009, a.g.k., 4660.

verme suçu, isabetli olarak topluma karşı suçlar kısmında düzenlenmiştir.[208]

2.3.1.5.3. Maddi unsur

2.3.1.5.3.1. Fiil

Türk Ceza Kanunu'nun 244. maddesinin birinci fıkrasında suç olarak sayılan fiiller bir bilişim sisteminin işleyişini engellemek veya bozmaktır. Görüldüğü üzere, suç seçimlik hareketli bir suçtur.[209] İki hareketin birlikte gerçekleştirilmiş olması suçun tekliğini etkilemeyecek fail tek bir suçtan sorumlu olacaktır.[210]

Bilişim sisteminin işleyişini, hem engelleme hem de bozma fiilleri çeşitli şekillerde meydana gelebilir. ASSS'nin 5. maddesine göre, bu fiiller bilişim sisteminin çalışmasını veri yükleyerek, aktararak, zarar vererek, silerek, değiştirerek veya müdahale ederek sekteye uğratmak suretiyle gerçekleştirilebilir.

Engelleme fiili, bilişim sisteminin işleyişini geçici bir süre sekteye uğratmak anlamına gelmektedir. Böyle bir durumda sistemin bozulması söz konusu olmamakta, sadece sistem normal zamandaki fonksiyonlarını yerine getirememektedir. Buna örnek olarak, işletim sistemine yapılacak bir müdahale ile sistemin geçici süre devre dışı bırakılması, elektronik posta bombardımanı yollanması ile sistemin kilitlenmesi ve zararlı virüslerle sistemin yavaşlatılması fiilleri verilebilir. Bilişim sisteminin işleyişini bozma ise kalıcı bir şekilde sistemin devre dışı bırakılması, sistemin veri işleme faaliyetini yapamayacak hale getirilmesidir. Buna örnek olarak da sisteme gizlice erişim sağlanarak sistem içerisinde yapılacak işlemlerle onu çalışamaz hale getirmeye yönelik fiiller verilebilir.[211]

244. maddenin birinci fıkrasında düzenlenen suç, genel olarak icrai hareketle işlenebilecek bir suçtur. Fakat, bazen bu suçun ihmal suretiyle de meydana gelmesi mümkün olabilir. Örneğin, bir kuruluşta bilişim alanında teknik sorumlu olarak çalışan personelin veri işleme engel olmak kastıyla virüs saldırısının önlenmesi için gerekli olacak yazılımları bilişim sistemine yüklememesi durumu suçun ihmal suretiyle

[208]Parlar, 2011, a.g.k., 25.; Benzer görüş için bkz. Koca ve Üzülmez, 2016, a.g.k., 825.
[209]Erdağ, 2010, a.g.k., 289-290.;mahmutoğlu, 866; aksi yönde bkz. Özbek, Doğan, Bacaksız ve Tepe, 2016, a.g.k., 951.; Koca ve Üzülmez, 2016, a.g.k., 812.
[210]Artuk, Gökçen ve Yenidünya, 2009, a.g.k., 4660.
[211]Artuk, Gökçen ve Yenidünya, 2015, a.g.k., 881-882.; Ketizmen, 2008, a.g.k., 129.; Başka örnekler için bkz. Kurt,2005, a.g.k., 165-166.; Koca ve Üzülmez, 2016, a.g.k., 827.

işlenmesi durumuna örnektir.[212]

2.3.1.5.3.2. Fail ve mağdur

Bu suç tipleri fail ve mağdur açısından bir özellik arz etmez. Dolayısıyla, herkes bu suçun faili veya mağduru olabilir. Suçun mağduru, bilişim sistemi üzerinde tasarruf yetkisi bulunan kimselerdir. Çünkü, bu kimseler söz konusu suça sebebiyet veren eylemler nedeniyle bilişim sistemine erişememekte ve sistemi kullanamamakta dolayısıyla tasarruf yetkileri zedelenmektedir.[213]

2.3.1.5.3.3. Netice

Netice açısından bu suç incelendiğinde, kanun koyucu madde metninde suçun oluşumu için, bilişim sisteminin işleyişinin engellenmesi ve bozulması şeklinde bir sonuç meydana gelmiş olması şartını aradığından dolayı, suçun neticeli bir suç olduğu sonucu çıkmaktadır. Ayrıca, madde metninde sayılan fiiller sonucunda bilişim sisteminde bir zarar meydana geleceğinden dolayı bu suç zarar suçudur.[214]

2.3.1.5.4. Manevi unsur

244. maddenin birinci fıkrasında düzenlenen suç tipi kasten işlenebilir. Kanunda açıkça düzenlenmemesinden dolayı suçun taksirle işlenmesi mümkün değildir. Maddenin 3. fıkrasındaki suçun nitelikli hali de ancak kastla gerçekleştirilebilir.

Kanun koyucu burada suçun oluşumu için genel kastı yeterli görmüştür. Özel kast aramamıştır.[215] Halbuki 765 sayılı TCK'da 244. maddenin karşılığı olan 525/b-1'de suçun oluşması için failde, başkasına zarar vermek veya kendisine veya başkasına yarar sağlamak şeklinde bir özel kast aranmaktaydı.

2.3.1.5.5. Hukuka aykırılık unsuru

244. maddenin birinci fıkrasında tanımlanan suç bakımından bilişim sisteminin ilgilisi tarafından hukuka uygun olarak verilmiş olan rıza failin fiilini hukuka uygun hale getirir.[216]

Kanun hükmünü yerine getirmek, bir başka hukuka uygunluk sebebidir. Örneğin,

---

[212]Dülger, 2013, a.g.k., 401.
[213]Yılmaz, 2011, a.g.k., 70.
[214]Aksi yönde bkz. Özbek, Doğan, Bacaksız ve Tepe, 2016, a.g.k., 951.
[215]Avşar ve Öngören, 2010, a.g.k., 137.; Koca ve Üzülmez, 2016, a.g.k., 831.; Doğan, 2005, a.g.k., 305.
[216]Parlar, 2011, a.g.k., 27.; Yılmaz, 2011, a.g.k., 79.; Özbek, Doğan, Bacaksız ve Tepe, 2016, a.g.k., 959.

5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun kapsamında yetkilendirilmiş olan personelin, 244/1. maddede belirtilen hareketleri yapmış olması, yetkilerini aşmadıkları müddetçe, kanun hükmünü yerine getirmek anlamına gelir ve hukuka uygunluk sebebidir.[217]

Yetkili amirin emrinin hukuka uygun yerine getirilmesi de 244/1. maddedeki suç açısından hukuka uygunluk sebebidir.[218] Örneğin, CMK'nın 134. maddesine göre kolluk görevlilerinin yetkili makamın kararıyla sisteme girip arama, kopyalama ve el koyma işlemlerini gerçekleştirmesi veya bir kurumda çalışan bilişim uzmanının bir başka personelin kullanıcı hesabına amirinin emri ile girerek oradaki bazı verileri silmesi veya kurumun işleyişiyle ilgili gerekli birtakım verileri sisteme yerleştirmesi durumunda suç oluşmayacaktır.

2.3.1.5.6. Suçun özel görünüş şekilleri

2.3.1.5.6.1. Teşebbüs

Bilişim sistemine zarar verme suçuna teşebbüs mümkündür. Neticeli bir suç olduğundan failin bilişim sistemine zarar vermeye yönelik fiilleri gerçekleştirmesi ancak bilişim sisteminde herhangi bir zarar meydana gelmemesi ya da failin icra hareketlerine başladıktan sonra bu hareketleri tamamlayamaması halinde suçun teşebbüs aşamasında kaldığından bahsedilebilir.[219]

Örneğin, failin sisteme virüs yollaması ya da sisteme truva atı, mantık bombası gibi yöntemlerle zarar vermeye çalışması, ancak sistem sahibinin bu durumu fark ederek müdahale etmesi ve failin istediği sonuca ulaşamaması halinde suç teşebbüs aşamasında kalmış olacaktır.

Bu suç seçimlik hareketli bir suç olduğundan failin seçimlik hareketlerden bir ya da birkaçını yapması ancak sadece bazı hareketler için bir neticenin meydana gelmesi diğer hareketlerin teşebbüs aşamasında kalması durumunda suç tamamlanmıştır ve fail tamamlanmış suçtan cezalandırılmalıdır. Çünkü, seçimlik hareketlerden herhangi birinin tamamlanması ve neticenin oluşması halinde suç tamamlanmış olacaktır.[220]

---

[217] Dülger, 2013, a.g.k., 407.
[218] Yaşar, Gökçan ve Artuç, 2010, a.g.k., 6766.
[219] Artuk, Gökçen ve Yenidünya, 2015, a.g.k., 4663.; Kurt, 2005, a.g.k., 263.
[220] Dülger, 2013, a.g.k., 407-408.

2.3.1.5.6.2. İştirak

Bilişim sistemine zarar verme suçu iştirak açısından bir özellik göstermez.

2.3.1.5.6.3. İçtima

Bilişim sistemine zarar verme suçunda zincirleme suç hükümleri uygulanabilir. Örneğin, failin mağdura ait bir ya da birden fazla bilişim sistemine aynı suç işleme kararının icrası kapsamında farklı zamanlarda zarar vermişse zincirleme suç söz konusu olur. Fakat, aynı suç işleme kararından bahsedilemeyecek kadar uzun aralıklarla ya da farklı fiillerle, farklı amaçlara yönelik zarar verici fiiller varsa faile her fiil için ayrı ceza verilecektir. Failin farklı kişilere ait bilişim sistemlerine aynı fiille zarar vermesi halinde TCK 43/2 söz konusu olacaktır. Buna örnek olarak, bir virüsün fail tarafından internet sitesinde yayımlanması ya da failin aynı spam mailini çok sayıda kişiye göndermesi fiili verilebilir.[221]

Önemle belirtmek gerekir ki 244. maddenin birinci fıkrası incelendiğinde, bilişim sisteminin işleyişinin engellenmesi ve bozulması fiillerinin sadece yazılım unsuruna yönelik olarak işlenebilecek bir suç olmadığı görülecektir. Dolayısıyla, 244/1. maddenin klasik mala zarar verme suçunun özel bir şekli olduğu kabul edildiğine göre, yazılım unsuruna yönelik hareketler sonucunda bilişim sisteminin işleyişinin engellenmesi ya da bozulması halinde 244/1 kapsamında, yok etme tahrip etme gibi donanım unsuruna yönelen fiiller ise TCK 151. madde kapsamında değerlendirilecektir. Nitekim, kanun koyucunun böyle bir düzenleme yapmış olması bilişim sisteminin yazılım kısmını koruma altına almaya yöneliktir. Donanım kısmına yönelik fiiller klasik mala zarar verme suçundan dolayı zaten cezalandırılabilir.[222] Fakat, burada dikkat edilmesi gereken şey, bilişim sisteminin işleyişini engelleme veya bozma suçu, bilgisayarı kırmak gibi fiziki saldırılar neticesinde işlenirse, burada hem TCK 151. maddedeki suç, hem de TCK 244/1. maddedeki suç oluşacaktır. Ancak fail, TCK'nın 44. maddesi gereğince en ağır cezayı gerektiren suçtan ceza alacaktır. Burada 244/1 daha ağır bir ceza öngördüğünden fail, bu suçtan yargılanıp hakkında cezaya hükmedilecektir.[223]

---

[221]Dülger, 2013, a.g.k., 408.
[222]Ketizmen, 2008, a.g.k., 130-133.; Benzer yönde görüş için bkz. Özbek, Doğan, Bacaksız ve Tepe, 2016, a.g.k., 946-947.; Koca ve Üzülmez, 2016, a.g.k., 828-829.
[223]Kurt, 2005, a.g.k., 164-165.; Artuk, Gökçen ve Yenidünya, 2015, a.g.k., 4664.; Ayrıca bkz. Pallı, 2008, a.g..k, 172-176.

2.3.1.5.7. Yaptırım, soruşturma ve kovuşturma

Kanun koyucu 244. maddenin 1. fıkrasında düzenlediği suç açısından hapis cezası öngörmüştür. 1. fıkrada yer verilen bilişim sisteminin işleyişini engelleme veya bozma suçu için faile verilecek cezanın alt sınırı bir yıl, üst sınırı beş yıl hapis cezasıdır.

3. fıkrada düzenlenen suçun nitelikli halinde ise 1. fıkradaki suçların banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna karşı işlenmesi durumunda verilecek ceza yarı oranında artırılacaktır.

Görevli mahkeme, 5235 sayılı Adli Yargı İlk Derece Mahkemeleri ile Bölge Adliye Mahkemelerinin Kuruluş, Görev ve Yetkileri Hakkında Kanun'un 11. ve 12. maddelerine göre asliye ceza mahkemeleridir. Suçun takibi şikayete bağlı değildir, resen soruşturulur.

2.3.1.6. Bilişim sisteminde yer alan verilere zarar verme suçu (m. 244/2)

2.3.1.6.1. Genel olarak

TCK'nın 244. maddesinin 2. fıkrasında, bilişim sisteminde yer alan verilere karşı gerçekleşecek ihlal hareketleri suç olarak düzenlenmiştir. Burada yer verilen suç tipi, ASSS'nin veri müdahalesi başlığını taşıyan 4. maddesindeki her bir taraf devletin, bir kimsenin, bilgisayar verisine hakkı olmadığı halde bilerek ve isteyerek zarar verme, silme, bozma, değiştirme ya da ortadan kaldırma fiillerini işlemesini suç olarak düzenlemek üzere gerekli kanuni düzenlemeyi yapma ve gerekli diğer önlemleri alma yükümlülüğünü yerine getirmeye yöneliktir. Bu fıkranın 765 sayılı TCK'daki karşılığının birebir aynı olmamakla birlikte 525/b-1 olduğu söylenebilir. Dülger'e göre, bu suç tipi kısmen 525/a-2'nin de TCK'daki karşılığını oluşturmaktadır.[224]

Ayrıca, 2. fıkradaki düzenleme ASSS'nin bilgisayarla ilişkili sahtekarlık başlıklı 7. maddesi ile bilgisayarla ilgili dolandırıcılık başlıklı 8. maddesindeki yükümlülükleri de yerine getirmeye yönelik unsurlar içermektedir.

2.3.1.6.2. Korunan hukuki yarar

Bilişim sisteminde yer alan verilere zarar verme suçunda korunan hukuki yararla bilişim sisteminin kendisine zarar verme suçunda korunan hukuki yararlar benzerlik göstermektedir. Bilişim sistemine zarar verme suçunda olduğu gibi burada da öncelikle

[224]Dülger, 2013, a.g.k., 386.

korunan hukuki yararın, ASSS'nin açıklayıcı raporunda da belirtildiği üzere, sistemde var olan her türlü veriye yönelik olarak 3. kişiler tarafından gerçekleştirilecek müdahalelere karşı ilgili kişinin tasarrufta bulunabilme yetkisi olduğu söylenebilir.[225]

Bilişim sisteminin işleyişine zarar verme suçuyla benzer olarak korunan bir başka hukuki değer ise toplumun bilişim sistemlerinin işleyişine olan güvenleri ve ekonomik düzenin sağlıklı işleyişidir. Kanun koyucu toplumda var olan güvenin zedelenmemesi ve düzenli bir ekonomi için isabetli olarak topluma karşı suçlar bölümünde, bilişim sisteminde yer alan verilere zarar verme suçunu düzenlemiştir.[226]

Bundan başka, suçla korunan diğer hukuki yararlar ise sistem içinde yer alan verilerin dokunulmazlığı, bilişim sistemi sahibinin ya da zilyedinin bilişim sisteminde yer alan veriler üzerindeki mülkiyet hakkı ve teknolojik gelişim özgürlüğüdür. Ayrıca, sistem üzerindeki veriler özgün bir çalışmayı içeriyorsa fikri mülkiyet hakkı da korunan hukuki yararlardandır.[227]

2.3.1.6.3. Maddi unsur

2.3.1.6.3.1. Fiil

244. maddenin ikinci fıkrasındaki suçun maddi unsuru, bilişim sistemindeki verileri bozmak yok etmek, değiştirmek, erişilmez kılmak, sisteme veri yerleştirmek, var olan verileri başka bir yere göndermek fiilleridir. Bu suç tipi seçimlik hareketli olarak düzenlenmiştir. Madde metninde düzenlenen seçimlik hareketlerden birden fazlası fail tarafından gerçekleştirilse dahi yine tek suç oluşacaktır.[228]

Görüldüğü üzere, burada bilişim sisteminin işleyişini engelleme ve bozma suçunda olduğu gibi, mala zarar verme suçunun sistemdeki verilere karşı işlenmesi söz konusu olmaktadır. Klasik mala zarar verme suçunun mal üzerinde işlenebilmesi, bilişim sistemindeki verilerin ise mal olarak değerlendirilememesi dolayısıyla bu düzenleme yapılmıştır.[229]

Bozmak, verilerin niteliğinin değiştirilmesi şeklinde olabileceği gibi verilerin tamamen ya da kısmen tahribi şeklinde de olabilir. Bu suç, bilişim sistemine bilfiil

[225]Ketizmen, 2008, a.g.k., 119.
[226]Parlar, 2011, a.g.k., 25.; Benzer görüş için bkz. Koca ve Üzülmez, 2016, a.g.k., 825.
[227]Kurt, 2005, a.g.k., 162.
[228]M.E. Artuk, A. Gökçen ve A.C. Yenidünya (2011). *Ceza Hukuku Özel Hükümler*. (11. Baskı). Ankara: Adalet Yayınevi, s. 703.
[229]Parlar, 2011, a.g.k., 26.; Kurt, 2005, a.g.k., 166-167.

girilmek suretiyle işlenebileceği gibi bilişim sistemlerine sızmış olan virüs programları veya benzeri zararlı programlar vasıtasıyla da işlenebilir. Bilişim sisteminin işleyişinin bozulmasının ne şekilde gerçekleştiğinin suçun oluşumu açısından bir önemi yoktur. [230]

Yok etmek ise verilerin tamamen ortadan kaldırılması, varlığına son verilmesi anlamına gelmektedir. Verilerin yok edilmesi sadece fiziki müdahalelerle olabilir, bilgisayarda yapılan işlemlerle veriler yok olmamakta sadece silinmektedir.[231] Örneğin, verilerin bir taşıma aracında bulunduğu durumda (hard disk, disket,cd,usb vb.) aracın kırılması sonucu veriler yok olursa bu suç oluşacaktır.[232]

Değiştirmek hareketi, veriler üzerinde yapılan oynamaları ifade etmektedir. Böylece, veriler niteliği değiştirilerek farklı bir hale getirilmektedir.[233] Verilerin kısmen veya tamamen değiştirilmesinin suçun oluşumu açısından bir önemi yoktur. Failin hangi amaçla hareket ettiği de önemsizdir.[234]

Erişilmez kılmak, verilere ulaşmayı sağlayan yolların değiştirilmesi veya silinmesi şeklinde gerçekleşebilir. Aslında bu durumda veriler, mağdurun bilişim sisteminde bulunmaya devam etmektedir, fakat mağdur failin yapmış olduğu bazı işlemlerden dolayı kendi verilerine ulaşamamaktadır.[235]

Sisteme veri yerleştirmek, sistem içerisindeki verilere herhangi bir zarar verilmeksizin sistem sahibinin rızasına aykırı olarak birtakım yeni verilerin sisteme ilave edilmesi anlamına gelir. Bu durumda veri güvenliği zarar görmektedir. [236] Örneğin, bir öğrencinin okulun bilişim sistemine girerek yeni not girişi yapması ya da bir personelin iş yerinin bilişim sistemine girerek bordrosunda birtakım ek ödenekler oluşturması bu suçu oluşturur.

Var olan verileri başka bir yere göndermek, mağdurun verilerinin farklı bir bilişim sistemine transferini ifade etmektedir. Bunun yanı sıra, bu seçimlik hareket, mağdura ait olan verilerin yine mağdurun bilişim sistemi içerisinde farklı bir dosyaya

[230]Artuk, Gökçen ve Yenidünya, 2009, a.g.k., 4666.; Kurt, 2005, a.g.k., 167.; Yılmaz, 2011, a.g.k., 72.
[231]Yılmaz, 2011, a.g.k., 73.; Ayrıntılı bilgi için Dülger, 2013, a.g.k., 396-397.; Özbek, Doğan, Bacaksız, Tepe, 2016, a.g.k., 952.
[232]Kurt, 2005, a.g.k., 168.; Parlar, 2011, a.g.k., 26.
[233]Artuk, Gökçen ve Yenidünya, 2009, a.g.k., 4667.; Akıncı, 2001, a.g.k., 19.
[234]Parlar, 2011, a.g.k., 26.
[235]Artuk, Gökçen ve Yenidünya, 2009, a.g.k., 4667.; Özbek, Doğan, Bacaksız ve Tepe, 2016, a.g.k., 952.; Akıncı, 2001, a.g.k., 18-19.
[236]Artuk, Gökçen ve Yenidünya, 2009, a.g.k., 4667.; Koca ve Üzülmez, 2016, a.g.k., 830.

gönderilmesini de kapsamaktadır.[237] Bu suça örnek olarak, bilişim sisteminden casusluk amacıyla gizli askeri bilgilerin alınması, bir öğrencinin okulun bilişim sistemine girerek sınav sorularını alması ve failin hiç işine yaramayacak dahi olsa, mağdura ait özel bilgi veya fotoğrafları içeren verileri transfer etmesi sayılabilir.[238]

244.maddenin 2. fıkrasındaki suç tipine uygulamada sık rastlanmaktadır. Bu suça örnek olarak, failin, mağdura ait Facebook hesabına giriş yapmaya çalışması ancak başarılı olamaması dolayısıyla mağdurun kendi hesabına erişimini engellemesi[239], failin mağdura ait e-mail şifresini ele geçirmesi ve değiştirmesi suretiyle erişimi engellemesi[240], katılan şirkete ait olan internet sitesinde satışa sunulan malları kendi kurmuş olduğu internet sitesinde bu malların özelliklerini de yazarak tümüyle yayınlaması neticesinde alıcının tekrar katılan şirkete ait internet sitesine gitmesine gerek bırakmaması suretiyle katılanı zarara uğratması[241], faillerden birinin diğer faillerden bir ya da birkaçını fiilen çalışmadığı halde çalışıyormuş gibi göstererek SGK'ya, internet üzerinden işe giriş bildirgesi vermeleri[242] fiilleri sayılabilir.

244. maddenin ikinci fıkrasında düzenlenen suç, genel olarak icrai hareketle işlenebilecek bir suçtur. Fakat, bazen bu suçun ihmal suretiyle de meydana gelmesi mümkün olabilir. Örneğin, bir kuruluşta bilişim alanında teknik sorumlu olarak çalışan personelin veri işleme engel olmak kastıyla virüs saldırısının önlenmesi için gerekli olacak yazılımları bilişim sistemine yüklememesi durumu suçun ihmal suretiyle işlenmesi durumuna örnektir.[243]

2.3.1.6.3.2. Fail ve Mağdur

Bu suç tipi fail ve mağdur açısından bir özellik arz etmez. Dolayısıyla, herkes bu suçun faili veya mağduru olabilir. Suçun mağduru, bilişim sisteminde yer alan veriler

[237]Artuk, Gökçen ve Yenidünya, 2009, a.g.k., 4668.
[238]Kurt, 2005, a.g.k., 170.
[239]Yargıtay 8. Ceza Dairesi'nin 13.11.2014 tarih ve 2014/20966 Esas ve 2014/ 26063 Karar sayılı kararı.; Yargıtay 8. Ceza Dairesi'nin 11.12.2015 tarih ve 2015/9842 Esas ve 2015/25682 Karar sayılı kararı.
[240]Yargıtay 8. Ceza Dairesi'nin 16.10.2014 tarih ve 2013/12964 Esas ve 2014/ 22580 Karar sayılı kararı.; Yargıtay 8. Ceza Dairesi'nin 10.09.2015 tarih ve 2014/35013 Esas ve 2015/21341 Karar sayılı kararı.; Yargıtay 8. Ceza Dairesi'nin 18.11.2015 tarih ve 2015/ 11682 Esas ve 2015/ 24706 Karar sayılı kararı.; Yargıtay 8. Ceza Dairesi'nin 21.06.2016 tarih ve 2016/3802 Esas ve 2016/8259 Karar sayılı kararı.; Yargıtay 8. Ceza Dairesi'nin 23.11.2016 tarih ve 2016/6436 Esas ve 2016/ 10698 Karar sayılı kararı.
[241]Yargıtay 8. Ceza Dairesi'nin 14.05.2014 tarih ve 2013/4675 Esas ve 2014/12406 Karar sayılı kararı.
[242]Yargıtay 11. Ceza Dairesi'nin 19.11.2015 tarih ve 2013/25561 Esas ve 2015/31099 Karar sayılı kararı.; Yargıtay 11. Ceza Dairesi'nin 18.04.2016 tarih ve 2016/1332 Esas ve 2016/3310 Karar sayılı kararı.
[243]Dülger, 2013, a.g.k., 401.

üzerinde tasarruf yetkisi bulunan kimselerdir. Çünkü, bu kimseler söz konusu suça sebebiyet veren eylemler nedeniyle bilişim sistemine ve bilişim sistemindeki verilere erişememekte, sistemi ve verileri kullanamamakta dolayısıyla tasarruf yetkileri zedelenmektedir.[244]

2.3.1.6.3.3. Netice

Netice açısından bu suç incelendiğinde, kanun koyucu madde metninde yok etmek, yerleştirmek, göndermek, erişilmez kılmak, değiştirmek şeklinde bir sonuç meydana gelmiş olması şartını aradığından suçun neticeli bir suç olduğu sonucu çıkmaktadır. Aynı zamanda ikinci fıkrada sayılan fiiller sonucunda bilişim sisteminde yer alan veriler zarar göreceğinden dolayı suç bir zarar suçudur.[245]

2.3.1.6.4. Manevi unsur

244. maddenin ikinci fıkrasında düzenlenen suç tipi kasten işlenebilir. Kanunda açıkça düzenlenmemesinden dolayı suçun taksirle işlenmesi mümkün değildir. Maddenin 3. fıkrasındaki suçun nitelikli hali de ancak kastla gerçekleştirilebilir.

Kanun koyucu burada suçun oluşumu için genel kastı yeterli görmüştür. Özel kast aramamıştır.[246] Halbuki 765 sayılı TCK'da 244. maddenin karşılığı olan 525/b-1 de suçun oluşması için failde, başkasına zarar vermek veya kendisine veya başkasına yarar sağlamak şeklinde bir özel kast aranmaktaydı.

2.3.1.6.5. Hukuka aykırılık unsuru

244. maddenin ikinci fıkrasında tanımlanan suç bakımından bilişim sisteminde yer alan verilerin ilgilisi tarafından hukuka uygun olarak verilmiş olan rıza failin fiilini hukuka uygun hale getirir.[247]

Kanun hükmünü yerine getirmek, bir başka hukuka uygunluk sebebidir. Örneğin, 5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla işlenen suçlarla mücadele edilmesi hakkında kanun kapsamında yetkilendirilmiş olan personelin 244/2. maddede belirtilen hareketleri yapmış olması, yetkilerini aşmadıkları müddetçe, kanun hükmünü yerine getirmek anlamına gelir ve

[244]Yılmaz, 2011, a.g.k., 70.
[245]Aksi yönde bkz. Özbek, Doğan, Bacaksız ve Tepe, 2016, a.g.k., 951.
[246]Avşar ve Öngören, 2010, a.g.k., 137.; Koca ve Üzülmez, 2016, a.g.k., 831.; Doğan, 2005, a.g.k., 305.
[247]Parlar, 2011, a.g.k., 27.; Yılmaz, 2011, a.g.k., 79.; Özbek, Doğan, Bacaksız ve Tepe, 2016, a.g.k., 959.

hukuka uygunluk sebebidir.[248]

Yetkili amirin hukuka uygun emrinin yerine getirilmesi de 244/2. maddedeki suç açısından hukuka uygunluk sebebidir.[249] Örneğin, CMK'nın 134. maddesine göre kolluk görevlilerinin yetkili makamın kararıyla sisteme girip arama, kopyalama ve el koyma işlemlerini gerçekleştirmesi veya bir kurumda çalışan bilişim uzmanının bir başka personelin kullanıcı hesabına amirinin emri ile girerek oradaki bazı verileri silmesi veya kurumun işleyişiyle ilgili gerekli birtakım verileri sisteme yerleştirmesi durumunda suç oluşmayacaktır.

2.3.1.6.6. Suçun özel görünüş şekilleri

2.3.1.6.6.1. Teşebbüs

Bilişim sisteminde yer alan verilere zarar verme suçuna teşebbüs mümkündür. Neticeli bir suç olduğundan failin bilişim sisteminde yer alan verilere zarar vermeye yönelik fiilleri gerçekleştirmesi, ancak bilişim sistemindeki verilerde bir zarar meydana gelmemesi ya da failin icra hareketlerine başladıktan sonra bu hareketleri tamamlayamaması halinde suçun teşebbüs aşamasında kaldığından bahsedilebilir.[250]

Örneğin, failin sisteme virüs yollaması, ya da sisteme truva atı, mantık bombası gibi yöntemlerle zarar vermeye çalışması ancak sistem sahibinin bu durumu fark ederek müdahale etmesi ve failin istediği sonuca ulaşamaması halinde suç teşebbüs aşamasında kalmış olacaktır.

Bu suç, seçimlik hareketli bir suç olduğundan failin seçimlik hareketlerden bir ya da birkaçını yapması, ancak sadece bazı hareketler için bir neticenin meydana gelmesi diğer hareketlerin teşebbüs aşamasında kalması durumunda suç tamamlanmıştır ve fail tamamlanmış suçtan cezalandırılmalıdır. Çünkü, seçimlik hareketlerden herhangi birinin tamamlanması ve neticenin oluşması halinde suç tamamlanmış olacaktır.[251]

Failin sisteme girdikten sonra sisteme veri yerleştirmekten veya sistemdeki verileri başka bir yere göndermekten vazgeçmesi halinde TCK'nın 36. maddesinde

[248]Dülger, 2013, a.g.k., 407.
[249]Yaşar, Gökçan ve Artuç, 2010, a.g.k., 6766
[250]Artuk, Gökçen ve Yenidünya, 2009, a.g.k., 4669.; Kurt, 2005, a.g.k., 263.
[251]Dülger, 2013, a.g.k., 407-408.

düzenlenen gönüllü vazgeçme[252] söz konusu olacaktır. Böyle bir durumda fail 244/2. maddeye teşebbüsten değil, tamamlanmış olan 243/1. maddeden sorumlu tutulacaktır.[253]

2.3.1.6.6.2. İştirak

Bilişim sisteminde yer alan verilere zarar verme suçu iştirak açısından bir özellik göstermez.

2.3.1.6.6.3. İçtima

Bilişim sistemine zarar verme suçunun zincirleme şekilde işlenmesi mümkündür. Failin, aynı suç işleme kararının icrası kapsamında farklı zamanlarda aynı mağdura ait bir ya da birden fazla bilişim sisteminde yer alan verilere zarar vermeye yönelik fiilleri, somut olayın durumuna göre zincirleme suç oluşturabilir. Örneğin, bir öğrencinin öğretmeninin bilgisayarına ayrı günlerde birden fazla kez girerek sınav sorularını kısım kısım temin ederek bunları başka bir yere taşıması halinde, öğrencinin kastının bir derse ait sınav sorularını elde etmek olması nedeniyle gerçekleştirdiği fiillerin tamamı bir suç sayılacak ve hakkında zincirleme suç hükümleri uygulanacaktır.[254]

Fikri içtima açısından bakıldığında, sistemde yer alan verilerin başka bir yere gönderilmesi kişisel verileri hukuka aykırı olarak bir başkasına vermek, yaymak veya ele geçirmek suçlarını oluşturabilir. Böyle bir durumda somut olayın özelliğine göre, failin sadece en ağır cezayı gerektiren suçtan sorumluluğu olabileceği gibi, her iki suç için cezalandırılması da ihtimal dahilindedir.[255] Aynı şekilde, bilişim sisteminde yer alan verilere zarar vermeye yönelik madde metninde sayılan fiillerin bir başka suçu daha oluşturması halinde TCK'nın 44. maddesi gereği failin en ağır cezayı gerektiren suçtan cezalandırılması gerekir.

Bilişim sistemine zarar verme suçu başlığı altında, klasik mala zarar verme suçuyla ilgili içtimaya yönelik yapmış olduğumuz açıklamalar burada da geçerlidir.

---

[252]Gönüllü vazgeçme
madde 36- (1) 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.
[253]Artuk, Gökçen ve Yenidünya, 2015, a.g.k., 4669.; Taşkın, 2008, a.g.k., 54.
[254]Kurt, 2005, a.g.k., 269.
[255]Artuk, Gökçen ve Yenidünya, 2015, a.g.k., 4670.

2.3.1.6.7. Yaptırım, soruşturma ve kovuşturma

Kanun koyucu 244. maddenin ikinci fıkrasında düzenlediği suç açısından hapis cezası öngörmüştür. İkinci fıkrada yer verilen bilişim sisteminde yer alan verilere zarar verme suçunda faile verilecek cezanın alt sınırı altı ay, üst sınırı üç yıl hapis cezasıdır.

3. fıkrada düzenlenen suçun nitelikli halinde ise birinci fıkradaki suçların banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna karşı işlenmesi durumunda verilecek ceza yarı oranında artırılacaktır.

Görevli mahkeme, 5235 sayılı Adli Yargı İlk Derece Mahkemeleri ile Bölge Adliye Mahkemelerinin Kuruluş, Görev ve Yetkileri Hakkında Kanun'un 11. ve 12. maddelerine göre asliye ceza mahkemeleridir. Suçun takibi şikayete bağlı değildir, resen soruşturulur.

2.3.1.7. Bilişim sistemine ve sistem üzerindeki verilere zarar verme suçlarının nitelikli hali (m. 244/3)

Kanun koyucu 244. maddenin üçüncü fıkrasında birinci ve ikinci fıkrada yer verilen fiiller için "bir banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinde işlenmesi halinde, verilecek ceza yarı oranında artırılır" diyerek daha ağır cezayı gerektiren nitelikli bir hal öngörmüştür.

Bu fıkraya göre, nitelikli halin oluşabilmesi için suçun banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna karşı işlenmiş olması gerekir. Başkalarının banka hesaplarına girerek miktarları değiştirmek, nüfus müdürlüğünün ya da bir üniversitenin bilişim sistemine girerek orada yer alan ders notlarını yükseltmek fiilleri suçun nitelikli haline örnek olarak verilebilir.[256]

5411 Sayılı Bankacılık Kanunu'nun 157. maddesinde bu kanuna tâbi kuruluşlar, 5237 sayılı Türk Ceza Kanunu'nun 244. maddesinde tanımlanan sistemi engelleme, bozma, verileri yok etme veya değiştirme suçu açısından banka veya kredi kurumu olarak kabul edilir denmektedir. Yine aynı kanunun kapsam başlığını taşıyan ikinci maddesinde ise bu kanuna tabi olan kuruluşlar sayılmıştır. 2. maddeye göre, Türkiye'de kurulu mevduat bankaları, katılım bankaları, kalkınma ve yatırım bankaları, yurt dışında kurulu bu nitelikteki kuruluşların Türkiye'deki şubeleri, finansal holding şirketleri,

[256] Avşar ve Öngören, 2010, a.g.k., 139.

Türkiye Bankalar Birliği, Türkiye Katılım Bankaları Birliği, Bankacılık Düzenleme ve Denetleme Kurumu, Tasarruf Mevduatı Sigorta Fonu banka veya kredi kurumu olarak kabul edilecektir.

Madde metninde belirtilmiş olan kamu kurum veya kuruluşu, bir tanıma göre, devletin, yasama, yürütme ve yargı teşkilatlarını oluşturan veya bunlara bağlı olan il, belediye ve köyler gibi mahalli idareleri ve KİT'leri kapsayan kurum ve kuruluşlarını ifade etmektedir.[257] Başka bir tanıma göre, kamu kurumları, belli bir malvarlığının belirli bir amaç için tahsis edilmesiyle oluşan kamu tüzel kişileridir. Bunlara örnek olarak da, üniversiteler, TRT, KİT'ler vb. gibi kurumlar verilebilir.[258]

Banka veya kredi kurumlarının ya da kamu kurum veya kuruluşlarının bilişim sistemlerinde meydana gelebilecek bir sorun, kesinti, bozukluk ya da bunlara ait bilişim sistemlerindeki verilerde meydana gelecek değişiklik, bozulma, erişilmez kılınma vb. gibi sorunlar büyük çapta bir zarara sebebiyet verecektir. Çünkü bahsedilen kurum ve kuruluşlar, kamu ve altyapı hizmetlerini yerine getirmekte, ekonomik sistemin işleyişini sağlamakta ve bu suretle birçok insanın hayatını etkilemektedir. Dolayısıyla, bu alanda meydana gelecek problemler büyük çapta olacaktır. Kanun koyucu oluşması muhtemel bu tip problemleri önleyebilmek için haklı olarak böyle bir nitelikli hale yer vermiştir.[259]

2.3.1.8. Bilişim sistemini kullanarak hukuka aykırı yarar sağlama suçu (m. 244/4)

2.3.1.8.1. Genel olarak

ASSS'nin bilgisayar bağlantılı dolandırıcılık başlığını taşıyan 8. maddesindeki yükümlülüklerin yerine getirilmesi için bu suç tipi düzenlenmiştir. 244. maddenin 4. fıkrası "yukarıdaki fıkralarda tanımlanan fiillerin işlenmesi suretiyle kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlamasının başka bir suç oluşturmaması halinde, iki yıldan altı yıla kadar hapis ve beşbin güne kadar adlî para cezasına hükmolunur" demektedir.

Türk Ceza Kanunu'ndaki bu hükmün karşılığı 765 sayılı TCK'daki 525/b-2 maddesidir. Fakat TCK'da bu suç tipi açısından daha farklı bir düzenleme yöntemi

[257]H. Pallı (2008). *Türk Hukukunda ve Mukayeseli Hukukta Bilişim Suçları*. Yayımlanmamış Yüksek Lisans Tezi. Kayseri: Erciyes Üniversitesi, s. 166.; Yaşar, Gökçan ve Artuç, 2010, a.g.k., 6762-6763.
[258]Kamu kurum ve kuruluşlarının neler olduğuyla ilgili ayrıntılı bilgi için bkz. K. Gözler (2007). *İdare Hukukuna Giriş*. (7. Baskı). Bursa: Ekin Yayınevi, s. 86-97.
[259]Dülger, 2013, a.g.k., 405.; Pallı, 2008, a.g.k., 166

tercih edilmiş ve maddenin 4. fıkrası bilişim sistemine ve sistemdeki verilere müdahale suçunun ağırlatıcı nedeni olarak öngörülmüştür.[260] Bilişim sistemleri aracılığıyla hukuka aykırı yarar sağlama fiilleri, 765 sayılı TCK'da sadece 525/b-2 maddesi gereğince cezalandırılıyordu. Fakat, bu maddenin çok geniş bir şekilde düzenlenmiş olması doktrinde eleştirilmekte, uygulamada ise çeşitli zorluklara sebebiyet vermekteydi. 5237 sayılı TCK'da kanun koyucu bu hususları dikkate almış ve bilişim sistemleri aracılığıyla hukuka aykırı yarar sağlama fiillerini 4 farklı suç şeklinde düzenlemiştir. Bu suç tipleri, 244. maddenin 4. fıkrasındaki bilişim sistemini kullanarak hukuka aykırı yarar sağlamak, 245. maddedeki banka ve kredi kartlarının kötüye kullanılması, 158. maddenin 1. fıkrasının f bendindeki bilişim sistemlerinin kullanılması suretiyle dolandırıcılık ve 142. maddenin 2. fıkrasının e bendindeki bilişim sistemlerinin kullanılması suretiyle hırsızlıktır.[261]

244. maddenin 4. fıkrasına göre hüküm kurulabilmesi için haksız çıkar sağlamaya yönelik fiillerin başka bir suç oluşturmaması gerekmektedir. Burada madde metniyle gerekçesi arasında çelişki bulunmaktadır. Şöyle ki madde metninde, fiilin başka bir suç oluşturmaması durumunda bu fıkraya göre ceza verileceği belirtilmişken, gerekçede, fiilin daha ağır cezayı gerektiren başka bir suç oluşturmaması halinde bu fıkraya göre ceza verileceği belirtilerek, bu suçlara örnek olarak da dolandırıcılık, hırsızlık, güveni kötüye kullanma ve zimmet suçları verilmiştir. Bu gibi durumlarda, gerekçenin bağlayıcılığı olmadığı için kanun metninin esas alınması gerekmektedir. Dolayısıyla bir olayda, 244/4 ün uygulanması için bilişim sistemlerinin kullanılması suretiyle hukuka aykırı yarar sağlamaya yönelik fiillerin daha ağır cezayı gerektirip gerektirmeme durumuna bakılmaksızın, sadece başka bir suç oluşturup oluşturmaması değerlendirilmelidir.[262]

2.3.1.8.2. Korunan hukuki yarar

Bu suç tipiyle korunan hukuki yarar, özel hayatın gizliliğinden malvarlığı haklarının korunmasına kadar çok geniş kapsamlıdır. Burada, kişilerin maddi ve manevi

[260] Ketizmen, 2008, a.g.k., 156.
[261] Dülger, 2013, a.g.k., 410-411.
[262] Dülger, 2013, a.g.k., 411.; Yılmaz, 2011, a.g.k., 87.; M. Koca (2010). Yargıtay Kararları Işığında Bilişim Sistemleri Kullanılması Suretiyle Haksız Yarar Sağlama Suçları. *Prof. Dr. Ali Güzel'e Armağan,* 2. Cilt, s. 1658.; Karagülmez, 2009, a.g.k., 221-223.

haklarına yönelecek saldırılar önlenmek istenmiştir.[263] Madde metninde haksız bir çıkar sağlamaktan bahsedilmiş fakat bu yararın türünün ne olduğu açıkça belirtilmemiştir. Dolayısıyla, burada kişinin sahip olduğu her türlü maddi ve manevi hak suçla korunan hukuksal değer olarak kabul edilebilir.

2.3.1.8.3. Maddi unsur

2.3.1.8.3.1. Fiil

Türk Ceza Kanunu'nun 244. maddesinin 4. fıkrasına göre maddenin 1. ve 2. fıkrasında işlenen suçlar neticesinde kişinin kendisine veya bir başkasına haksız bir çıkar sağlaması başka bir suç oluşturmaz ise bu fıkraya göre ceza verilecektir. Dolayısıyla, bu suçun hareket unsuru 244. maddenin 1. ve 2. fıkrasında düzenlenmiş olan bir bilişim sisteminin işleyişini engellemek veya bozmak, bilişim sisteminde yer alan verilere 2. fıkrada sayılan fiillerle müdahalede bulunmaktır. Suç seçimlik hareketli bir suçtur.

Bu maddede tanımlanmış olan fiiller neticesinde başka suçların oluşması ihtimali de vardır. Nitekim, gerekçede olası suçlara dair örnekler verilmiştir.[264] Bu durumu öngörmüş olan kanun koyucu, 4. fıkrayı bir tamamlayıcı norm olarak düzenlemiştir.[265] 4. fıkra bir tamamlayıcı norm olarak öngörüldüğünden dolayı bilişim sistemleri aracılığıyla haksız bir çıkar sağlandığında öncelikle bilişim sistemlerinin kullanılması suretiyle hırsızlık, dolandırıcılık zimmet gibi başka bir suçun oluşup oluşmadığı incelenmeli, eğer bu suçlara ait unsurlar somut olayda oluşmadıysa 244/4. maddesi değerlendirilmelidir.[266] Örneğin, failin, mağdurun e-mail adresine yetkisiz erişim sağlayarak site yöneticisinin kontrolü altında oynanan bilgisayar oyununa ait itemleri kendisine ait oyuna eklemesi durumunda bilişim sisteminin hukuka aykırı olarak kullanılması suçu oluşacaktır.[267] Bir başka örnek vermek gerekirse fail, bir bilişim sistemine virüs, solucan ya da truva atı göndererek virüs koruma programları üreten bir firmanın ürün satışını artırmayı amaçlamış ve bu suretle haksız çıkar elde etmişse bu

[263]Artuk, Gökçen ve Yenidünya, 2009, a.g.k., 4671.; Koca ve Üzülmez'e göre, burada korunan hukuki yarar, ağırlıklı olarak malvarlığı değerleridir. Bkz. Koca ve Üzülmez, 2016, a.g.k., 839.
[264]TCK'nın 244. maddesinin gerekçesi: "... bu bakımdan fiilin, örneğin, dolandırıcılık, hırsızlık, görevi kötüye kullanma veya zimmet suçunu oluşturması halinde bu fıkra hükmüne istinaden cezaya hükmedilemez."
[265]Artuk, Gökçen ve Yenidünya, 2009, a.g.k., 4672.
[266]Yargıtay 8. Ceza Dairesi'nin 12.04.2016 tarih ve 2015/14782 Esas ve 2016/4928 Karar Sayılı Kararı.; Yargıtay 11. Ceza Dairesi'nin 28.05.2009 tarih ve 2009/ 3019 Esas ve 2009/ 6644 Karar Sayılı Kararı.
[267]Yargıtay 13. Ceza Dairesi'nin 06.06.2016 tarih ve 2015/2174 Esas ve 2016/10469 Karar Sayılı Kararı.

suça göre cezalandırılacaktır.[268]

2.3.1.8.3.2. Fail ve mağdur

Suç, fail ve mağdur açısından bir özellik taşımamaktadır. Herkes bu suçun faili veya mağduru olabilir.

2.3.1.8.3.3. Netice

Netice açısından suç, bir zarar suçudur. 4. fıkradaki suçun oluşması için zarar tehlikesi yeterli görülmemiş, kişinin kendisine veya bir başkasına haksız bir çıkar sağlaması şartı aranmıştır. Haksız bir çıkar sağlanması neticesinde mağdur da bir zarara uğrayacaktır. Bu zarar, mağdurun mal varlığının azalması ya da mağdurun muhtemel bir gelirden mahrum kalması şeklinde meydana gelebilir. Dolayısıyla, neticeli bir suç oluşur.[269]

2.3.1.8.4. Manevi unsur

Bu suç kasten işlenebilir. Kanun koyucu suçun oluşumu için failde genel kastın varlığını yeterli görmüş, ayrıca özel bir kast aramamıştır.[270] Kanunda 4. fıkradaki suçun taksirli şekline yer verilmediğinden suçun taksirle işlenebilmesi mümkün değildir.

2.3.1.8.5. Hukuka aykırılık unsuru

Hukuka aykırılık unsuru açısından yukarıda yapmış olduğumuz açıklamalar burada da geçerlidir. Burada sadece bir farklılık olarak belirtilmesi gereken, mağdurun rızası olması durumunda haksız bir çıkar sağlamış olmak şartı gerçekleşmeyeceğinden dolayı suçun oluşmayacağıdır. Geçerli bir rıza, bu suç açısından hukuka uygunluk sebebidir. Rızanın fiilden önce mevcut olması gerekir. Fiili hukuka uygun hale getirecek rızayı verecek olan kişi, bilişim sisteminin maliki ya da sistem üzerinde tasarruf hakkı olan kimsedir. [271]

---

[268]Doğan, 2005, a.g.k., 304.
[269]Aynı yönde görüş için bkz. Yılmaz, 2011, a.g.k., 88.; Taşkın, 2008, a.g.k., 58.; Aksi görüş için bkz. Dülger, 2013, a.g.k., 418-419.
[270]Farklı görüşteki yazarlardan Parlar'a göre, madde metnindeki "haksız çıkar sağlamak" ifadesi, suçun oluşması için failde genel kastın yanında özel kastın da arandığını göstermektedir. Bkz. Parlar, 2011, a.g.k., 27.
[271]Dülger, 2013, a.g.k., 420-421.

2.3.1.8.6. Suçun Özel görünüş şekilleri

2.3.1.8.6.1. Teşebbüs

Bilişim sistemini kullanarak hukuka aykırı yarar sağlama suçuna teşebbüs mümkündür. Suçun hareket unsurunu oluşturan 244. maddenin 1. ve 2. fıkrasında belirtilmiş fiillerin tamamlanması ve fakat hukuka aykırı yarar sağlanmamış olması halinde failin teşebbüsten cezalandırılması gerekir. Ancak, burada önemli bir ayrım vardır. Şöyle ki failin hukuka aykırı yarar sağlamak kastıyla 1. veya 2. fıkralarda belirtilen fiilleri gerçekleştirdiğinin tespit edilmesi, ancak failin istediği neticeye ulaşamaması halinde fail 244/4. maddesine teşebbüsten sorumlu tutulmalıdır. Aynı durumda failin kastının hukuka aykırı yarar elde etmek olduğunun tespit edilememesi halinde ise failin somut olayın özelliğine göre 1. veya 2. fıkraya göre sorumluluğu söz konusu olacaktır. [272]

Failin hukuka aykırı yarar sağlamak amacıyla sisteme girmesi ve fakat daha sonra 1. veya 2. fıkradaki fiilleri gerçekleştirmekten vazgeçerek sistemden çıkması halinde bu suça teşebbüsten değil, 243/1. maddedeki suçtan bahsedilebilir.[273]

2.3.1.8.6.2. İştirak

Bilişim sistemini kullanarak hukuka aykırı yarar sağlama suçu iştirak açısından bir özellik göstermez.

2.3.1.8.6.3. İçtima

Bilişim sistemini kullanarak hukuka aykırı yarar sağlama suçunun zincirleme şekilde işlenmesi mümkündür. Failin, hukuka aykırı yarar sağlamak için aynı suç işleme kararının icrası kapsamında farklı zamanlarda aynı mağdura ait bir ya da birden fazla bilişim sistemine karşı 244. maddenin 1. veya 2. fıkrasında belirtilmiş fiilleri gerçekleştirmesi halinde zincirleme suç hükümleri uygulanmalıdır.

Bu suçla bir başka suç arasında fikri içtimanın oluşabilmesi mümkün değildir. Çünkü, 244/4. maddenin uygulanabilmesi için fiilin başka bir suç oluşturmaması gerekmektedir. Bilişim alanında hukuka aykırı yarar elde etme amacına yönelik ihlal hareketleri, ancak başka bir suç oluşturmaması halinde bu maddeye göre

[272]Dülger, 2013, a.g.k., 421.
[273]Üzülmez ve Koca, 2016, a.g.k., 842.

cezalandırılabilir. Somut olayda öncelikle başka bir suçun özellikle de bilişim sistemlerinin araç olarak kullanılması suretiyle hırsızlık (142/2-e) veya dolandırıcılık (158/1-f) suçlarının oluşup oluşmadığı değerlendirilmelidir.

Son olarak, uygulamada çok sık karşılaşılan başkasına ait banka hesabına internet üzerinden girilerek para transferi yapılması fiilinin bu suç kapsamında olup olmadığını incelemek gerekir. Bu konuda benzer olayların farklı yorumlanması ve Yargıtay daireleri arasında konuya ilişkin görüş birliğinin olmaması uygulamada çelişkiler ortaya çıkarmıştır. Bunun üzerine Yargıtay Ceza Genel Kurulu 2009 yılında konuya ilişkin vermiş olduğu kararda bu durumda bilişim sistemlerinin araç olarak kullanılması suretiyle hırsızlık suçunun oluşacağını belirtmiştir. Kurul, kararında sanığın kastının mağdurun banka hesabında bulunan taşınır nitelikteki parayı bilişim sistemini kullanmak suretiyle kendi banka hesaplarına geçirmek olduğunu, fiil sonucu mağdurun mal varlığında azalma olduğunu, suçun işlenebilmesi için sanığın, mağdurun internet bankacılığı hesabında bulunan parasına ulaşırken bilişim sistemini kullanmaktan başka alternatifinin olmadığını, kısaca sanığın, sistemde bulunan verinin temsil ettiği parayı alarak mal edinmek amacıyla suç işlediğini söylemiştir. Karara muhalif kalan üyeler ise banka hesabına internet üzerinden girmek suretiyle sistemde gerçekleştirilen bazı değişiklikler sonucu para transferi yapılması durumunda, sistemde bulunan verilerin taşınır mal özelliğini haiz olmadığını, dolayısıyla hırsızlık suçunun unsurlarının oluşmadığını belirterek suçta ve cezada kanunilik prensibi gereği somut olayda 244/4. maddenin uygulanması gerektiğini belirtmişlerdir.[274] Kanaatimizce, Ceza Genel Kurulu'nun kararı isabetlidir. Çünkü, failin amacının açıkça mağdurun banka hesabındaki parayı onun rızası olmaksızın bulunduğu yerden almak olduğu bellidir. Bu haliyle fiil, hırsızlık suçunun kanuni tanımına uymaktadır. Kararda belirtildiği gibi fail, verinin temsil ettiği parayı ele geçirmeye çalışmaktadır. Günümüz teknolojisinde paranın her zaman kağıda basılı olması zorunluluğu yoktur. Para, veri formunda da olabilir. Ayrıca, failin mağdurun banka hesabına internet üzerinden girebilmesi için bilişim sistemini kullanması da zorunludur. Failin buradaki amacı, salt sistemde yer alan verilere zarar vermeye yönelik değildir. Dolayısıyla, 244/4. maddenin uygulanma imkanı yoktur.[275]

[274]Yargıtay Ceza Genel Kurulu'nun 17.11.2009 tarih ve 2009/11-193 Esas ve 2009/268 Karar sayılı kararı.
[275]Ayrıca bkz. Dülger, 2013, a.g.k., 549.

2.3.1.8.7. Yaptırım, soruşturma ve kovuşturma

Bilişim sisteminin kullanılması suretiyle haksız çıkar sağlanması suçu için hem hapis cezası hem de adli para cezası öngörülmüştür. Hapis cezasının alt sınırı iki yıl, üst sınırı ise altı yıldır. Adli para cezasının miktarı ise genel hükümlere göre belirlenecektir.

Görevli mahkeme, 5235 sayılı Adli Yargı İlk Derece Mahkemeleri ile Bölge Adliye Mahkemelerinin Kuruluş, Görev ve Yetkileri Hakkında Kanun'un 11. ve 12. maddelerine göre asliye ceza mahkemeleridir. Suçun takibi şikayete bağlı değildir, resen soruşturulur.

2.3.1.9. Banka veya kredi kartlarının kötüye kullanılması suçu (m. 245)

2.3.1.9.1. Genel olarak

Türk Ceza Kanunu'nun 245. maddesinde gündelik hayatın artık vazgeçilmez araçları olan banka ve kredi kartlarının kötüye kullanılması ile ilgili suçlar düzenlenmiştir. 765 sayılı TCK'da bu suçları açıkça düzenleyen bir madde yoktu. Eski yasa döneminde bu suçlar 525/b-2 maddesi kapsamında değerlendiriliyordu.[276] Ancak, eski yasa döneminde banka veya kredi kartlarının kötüye kullanılması suçu, uygulamada çok fazla karşılaşılan suç tiplerinden olmuş, hatta bilişim suçu denildiği zaman akla ilk gelen kredi kartlarının kötüye kullanılması fiilleri olmuştur.[277] Kanun koyucu 245. maddenin gerekçesinde[278] de belirttiği üzere, bu tarz fillerle mücadele edebilmek amacıyla TCK'da, 765 sayılı TCK'nın aksine banka veya kredi kartlarının kötüye kullanılmasını ayrı bir suç olarak düzenlemiştir.

Türk Ceza Kanunu'nun ilk halinde 245. madde 2 fıkra olarak düzenlenmiştir.[279] Daha sonra 29.06.2005 tarih ve 5377 sayılı Kanun'un 27. maddesiyle 245. maddeye 2

---

[276]Banka kartları ile kredi kartları ve bu kartlara ait şifreleri herhangi bir yolla haksız olarak ele geçiren kişilerce bu kartlar ile şifrelerin kullanılarak ATM'lerden nakit çekilmesi fiili, TCK'nın 525/b-2 maddesinde yazılı suçu oluşturmaktadır. Bkz. Ekinci ve Esen, 2003, a.g.k., 900.

[277]Kurt, 2005, a.g.k., 176.

[278]TCK'nın 245. maddesinin gerekçesi: "Madde, banka veya kredi kartlarının hukuka aykırı olarak kullanılması suretiyle bankaların veya kredi sahiplerinin zarara sokulmasını, bu yolla çıkar sağlanmasını önlemek ve failleri cezalandırmak amacıyla kaleme alınmıştır."

[279]Kanunun ilk hali: Banka veya kredi kartlarının kötüye kullanılması

MADDE 245. - (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 cezası ve adlî para cezası ile cezalandırılır.

(2) 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 yedi yıla kadar hapis cezası ile cezalandırılır.

fıkra eklenmiş ve madde 4 fıkradan teşekkül etmiştir. Yine bu değişiklikle, 245. maddenin 1. fıkrasındaki adli para cezasına "beşbin güne kadar" denilerek üst sınır getirilmiş, 2. fıkradaki hapis cezasının üst sınırı sekiz yıla çıkarılmış ve bu fıkradaki suç tipi için hapis cezasının yanı sıra beş bin güne kadar adli para cezası öngörülmüştür. Kanunda yapılan ikinci değişiklik ise 06.12.2006 tarih ve 5560 sayılı kanunun 11. maddesiyle yapılmış ve 245. maddeye 5. fıkra eklenerek madde bugünkü şeklini almıştır.

Maddenin ilk fıkrasında, bir banka veya kredi kartının sahibinin rızası hilafına kullanılması suretiyle haksız yarar sağlanması, 2. fıkrada, banka veya kredi kartlarının sahte olarak üretimi, satımı, devri, alınması ve kabul edilmesi, 3. fıkrada ise sahte banka veya kredi kartının kullanılması suretiyle haksız yarar elde edilmesi suç olarak düzenlenmiştir. Gereksiz tekrarlardan kaçınmak için bu çalışmada, 245. maddedeki bu suçların hepsini aynı başlık altında incelemek ama suçların farklılık arz eden yönlerini de ayrıca belirtmek doğru olacaktır.

245. maddenin 4. fıkrasında ilk üç fıkrada yer verilen suçlara yönelik şahsi cezasızlık sebebi öngörülmüştür. 5. fıkrada da bu maddede düzenlenmiş suçlarda malvarlığına karşı suçlar bölümünde düzenlenmiş olan etkin pişmanlık hükümlerinin uygulanacağı belirtilmiştir.

Türkiye'de son yıllarda banka ve kredi kartı kullanımında olağanüstü bir artış yaşanmaktadır. Neredeyse herkeste bu kartlardan vardır, hatta çok sayıda kişi, birden fazla banka ve kredi kartı kullanmaktadır. Özellikle, kredi kartlarının artık çok kolay elde edilebiliyor olması ve toplumda dar gelir grubundaki bireylerden üst gelir grubundaki bireylere kadar neredeyse herkesin kredi kartına sahip olması bu kartların kötüye kullanılması suçlarında büyük bir artış meydana getirmiştir. Banka veya kredi kartlarının kötüye kullanılması suçlarındaki bu artış, ekonomik ve ticari hayatı sarsmasının yanı sıra aile düzeni ve toplum yapısını da olumsuz etkilemektedir. Tüm bunlar göz önünde tutulduğunda kanun koyucunun TCK 245. maddeyi ihdas etmesinin ne kadar isabetli bir tercih olduğu anlaşılmaktadır. Bu hüküm 5237 sayılı TCK'nın en önemli ve olumlu düzenlemelerinden de biridir.[280]

[280]S. Yılmaz (2010). Banka veya Kredi Kartlarının Kötüye Kullanılması Suçu. *TBB Dergisi*, (87), s. 263-271.

2.3.1.9.2. Banka ve kredi kartı

Suçun unsurlarını incelemeye geçmeden önce, bu başlık altında 245. maddedeki suç tiplerinin konusunu oluşturan banka ve kredi kartı kavramlarını tanımlamak gerekmektedir.

245. maddenin gerekçesinde banka kartı, "kart sahibinin bankanın kurduğu sisteme saptanan ve kart sahibince bilinen bir numara marifetiyle banka görevlisinin yardımı olmaksızın hukuka uygun olarak girerek kendi hesabından para çekmesini sağlayan araç" olarak tanımlanmıştır.

Banka kartı ile ilgili başka bir tanıma 5464 Sayılı Banka Kartları ve Kredi Kartları Kanunu'nun 3. maddesinde yer verilmiştir. Buna göre, banka kartı, mevduat hesabı veya özel carî hesapların kullanımı dahil bankacılık hizmetlerinden yararlanmayı sağlayan karttır.

Banka kartının, fonksiyonunu yerine getirebilmesi için ilgililerin ilk olarak bankada bir mevduat hesabı açtırmaları gerekmektedir. Bu işlemden sonra banka kartı vasıtasıyla para havalesi, fon transferi, döviz veya hisse senedi alım satımı, ödeme işlemleri, para çekilmesi, yatırılması gibi tüm bankacılık işlemleri kolaylıkla yapılabilmektedir. Kart sahibinin banka görevlisiyle ya da başka herhangi biriyle muhatap olmasına gerek yoktur. Bankanın bilişim sistemine girebilmesi için gerekli olan ATM[281] , POS cihazı[282] gibi cihazlar veya internet bankacılığı[283] ya da mobil bankacılık sistemini[284] kullanabileceği araçlarının olması yeterlidir.[285]

245. maddenin gerekçesinde, kredi kartı ise "banka ile kendisine kart verilen kişi arasında yapılmış bir sözleşme gereğince kişinin bankanın belirli koşullarla sağladığı kredi olanağını kullanmasını sağlayan araç" olarak tanımlanmıştır.

Banka Kartları ve Kredi Kartları Kanunu'nun 3. maddesine göre kredi kartı, nakit

[281]ATM, automated teller machine sözcüklerinin baş harflerinden oluşur.
[282]POS: Banka kartı veya kredi kartı üzerindeki bilgileri esas alarak her türlü mal ve hizmet alımı veya nakit ödeme belgesi düzenlenmesi işlemleri ile bu Yönetmelik hükümleri uyarınca nakit kullanımı kapsamında değerlendirilebileceği belirtilen işlemlerin gerçekleştirilmesinde kullanılan elektronik cihaz. Bkz. Banka Kartları ve Kredi Kartları Hakkında Yönetmeliği 4/1-i maddesi.
[283]İnternet bankacılığı, bankacılık hizmetlerinin uzaktan dağıtım kanalı olarak internet üzerinden sunulmasıdır. Ayrıntılı bilgi için Bkz. C. Toraman (2002). Bankacılık Sektöründe İnternetin Yeri ve Türk Bankacılık Sistemi Uygulaması, *Kamu İş Hukuku ve İktisat Dergisi*, 6(3),s. 3.
[284]Mobil bankacılık sistemi, internet bankacılığı ile yapılabilecek banka işlemlerinin bir mobil cihaz ile yapılmasını sağlayan sistemdir.
[285]Kurt, 2005, a.g.k., 179.

kullanımı gerekmeksizin mal ve hizmet alımı veya nakit çekme olanağı sağlayan basılı kartı veya fizikî varlığı bulunmayan kart numarasını ifade eder.

Banka kartıyla kredi kartı arasındaki fark, banka kartı hamilinin mevduat hesabında nakit para olması halinde alışveriş yapabilmesi ya da para çekebilmesi mümkünken, kredi kartı, hamilinin hesabında nakit para bulunmaksızın alışveriş yapabilmesi ya da nakit avans işlemi yapabilmesidir.[286] Ancak, banka kartı hamilinin banka ile yapacağı anlaşma neticesinde, mevduat hesabında nakit para bulunmadığında bile belli bir limite kadar kendisine banka tarafından sağlanan krediyi alışveriş yaparken kullanabilmesi ya da para çekebilmesi mümkündür.

Banka ve kredi kartlarının mülkiyet hakkı, bu kartları çıkaran bankaya aittir ve banka tarafından istenildiğinde iadesi zorunludur. Tüm banka ve kredi kartlarının arka yüzünde bu husus yazılıdır. Müşteriler, banka ve kredi kartları üzerinde sadece kullanım hakkına sahiptirler.[287]

2.3.1.9.3. Korunan hukuki yarar

Türk Ceza Kanunu'nun 245. maddesinin gerekçesinde kanun koyucu "...aslında hırsızlık, dolandırıcılık, güveni kötüye kullanma ve sahtecilik suçlarının ratio legis'lerinin tümünü de içeren bu fiillerin duraksamaları ve içtihat farklılıklarını önlemek amacıyla bağımsız suç haline getirilmeleri uygun görülmüştür" diyerek suçla korunan hukuki yararın ne olduğunu açıklamıştır.

Gerekçeye bakıldığında, suçla korunan hukuki değerin, hırsızlık, dolandırıcılık ve güveni kötüye kullanma suçlarını içermesi dolayısıyla malvarlığı ve kişilere duyulan güven, sahtecilik suçunu içermesi dolayısıyla da kamuya duyulan güven ve itibar olduğu anlaşılmaktadır. Yani bu suçla korunan hukuki değer, karma bir nitelik taşımaktadır.[288]

Türk Ceza Kanunu'nun 245/2. maddesinde sahte banka veya kredi kartı üretimi ve dağıtımı bu kartlarla haksız bir yarar elde edilmiş olması şartı aranmaksızın suç haline getirilmektedir. Buna göre, bu suç tipiyle korunan hukuki değer, malvarlığı değerlerinin dışında ayrıca ve özellikle bankacılık hizmetlerinin güvenli ve süratli yapılabilmesi ve

[286]Kurt, 2005, a.g.k., 180.
[287]Dülger, 2013, a.g.k., 434.
[288]Artuk, Gökçen ve Yenidünya, 2015, a.g.k., 896.; Kurt, 2005, a.g.k., 177.; Yılmaz, 2010, a.g.k., 266.; Özbek, Doğan, Bacaksız ve Tepe, 2016, a.g.k., 967.

ekonomik yapının sağlıklı işlemesidir. [289] Çünkü, günümüzde mal ve hizmet alımlarında kredi kartı yoğun olarak kullanılmakta kamu sektörüyle özel sektörde maaş ödemeleri de banka kartlarıyla yapılmaktadır. Dolayısıyla, banka ve kredi kartları ekonomik yapının işleyişinde son derece önemli bir konumdadır.[290]

Korunan hukuki yarar açısından TCK'nın 245. maddesi incelendiğinde, bu hükmün kanunda bilişim alanında suçlar başlığı altında düzenlenmiş olması aslında kanun sistematiği açısından bakıldığında yanlıştır. Suçla korunan hukuki değerin malvarlığı olması dolayısıyla, doktrinde, banka ve kredi kartlarının kötüye kullanılması suçunun, malvarlığına karşı suçlar bölümünde düzenlenmesi gerektiğini düşünen yazarlar vardır.[291] Fakat, banka veya kredi kartının kötüye kullanılması suçu, bir bilişim sistemi olmaksızın işlenemeyeceğinden ötürü bilişim suçu olarak kabul edilmekte ve kanunda bilişim alanında suçlar başlığı altında düzenlenmektedir.[292]

2.3.1.9.4. Maddi unsur

2.3.1.9.4.1. Fiil

Türk Ceza Kanunu'nun 245. maddesinde, banka ve kredi kartlarının kötüye kullanılmasına yönelik her türlü hareket cezalandırılmak istenmiştir. Bundan dolayı, kanun koyucu 245. maddede 3 farklı suç tipini düzenlemiştir. 1. fıkrada banka veya kredi kartlarının hukuka aykırı kullanılması, 2. fıkrada sahte banka veya kredi kartı üretilmesi, satılması, devredilmesi, satın alınması, kabul edilmesi, 3. fıkrada sahte banka veya kredi kartı kullanılarak hukuka aykırı yarar sağlanması suç haline getirilmiştir. 245. maddede yer verilen suç tipleri her ne kadar unsurları yönünden benzerlik gösterse de suçun maddi unsurunu oluşturan fiil (hareket) açısından farklılık arz etmektedir. Dolayısıyla, her bir suçun hareket unsurunun birbirinden ayrı olarak incelenmesi doğru olacaktır.

Banka veya kredi kartlarının hukuka aykırı olarak kullanılması (m. 245/1)

245. maddenin birinci fıkrasında düzenlenen suçun hareket unsurunu failin,

[289] Yaşar, Gökçan ve Artuç, 2010, a.g.k., 6798.; Karagülmez, 2009,a.g.k., 261.; Koca ve Üzülmez, 2016, a.g.k., 846.; Doğan, 2005, a.g.k., 308.
[290] Dülger, 2013, a.g.k., 427.
[291] V.Ö. Özbek (2007). Banka veya Kredi Kartlarının Kötüye Kullanılması Suçu (TCK m.245). *Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi*, 9 (Özel Sayı), s. 1022.; Dülger, 2013, a.g.k., 428.; Ketizmen, 2008, a.g.k., 187.; Yılmaz, 2010, a.g.k., 267.; Özbek, Doğan, Bacaksız ve Tepe, 2016, a.g.k., 964-965.
[292] Kurt, 2005, a.g.k., 178.; Özbek, 2007, a.g.k., 1052.; Avşar ve Öngören, 2010, a.g.k., 140-141.

başkasına ait banka veya kredi kartını, sahibinin ya da kartın kendisine verilmesi gereken kişinin rızası hilafına kullanması veya kullandırması suretiyle kendisine veya başkasına yarar sağlaması fiili oluşturur. Serbest hareketli bir suçtur.

765 sayılı Kanun döneminde, banka veya kredi kartlarının kötüye kullanılması ile ilgili fiiller kanunun 525/b-2 maddesi kapsamında değerlendiriliyordu. TCK'da ise bu fiiller 245. maddenin 1. fıkrasında münhasıran suç olarak düzenlenmiştir. Bu fıkraya göre, failin başkasına ait olan banka veya kredi kartını ele geçirme şekline bakılmaksızın kart sahibinin rızası hilafına kullanması veya kullandırtması suç oluşturmaktadır.[293]

Başkasına ait banka veya kredi kartlarını hukuka aykırı olarak kullanma fiili çeşitli şekillerde meydana gelebilir. Kanun koyucu burada bir kısıtlama öngörmemiştir. Başkasına ait banka veya kredi kartı, ATM'lerde, alışveriş amacıyla ticari işletmelerde ya da veri iletim ağlarında kullanılmak suretiyle bu suç işlenebilir. Fakat, burada suçun tüm işlenme yöntemlerinin biliniyor olduğu söylenemez. Çünkü, teknoloji ve bilişim alanındaki gelişmelerle birlikte yeni suç işleme yöntemleri de ortaya çıkabilmektedir. Dolayısıyla, anlatılan tüm suç işlenme yöntemleri bugüne kadar sıklıkla rastlanmış olanları özetlemekten ibarettir.[294]

Başkasına ait banka veya kredi kartlarının hukuka aykırı olarak kullanma suçunun işlenme yöntemlerine örnek olarak, kartı ele geçirme ve elde bulundurma hareketleri, rıza dışında kartı fiziken kullanma ve kullandırtma, kart bilgilerinin kullanılması veya kullandırtılması, henüz hamiline teslim edilmeyen kartla yarar sağlanması, gerçeğe aykırı beyanda bulunarak kartın kullanılması ya da kullandırılması, başkasına ait banka veya kredi kartlarının alışverişte kullanılması, başkasına ait kredi kartına bağlı ek kart çıkartılıp kullanılması, sanal ağlar üzerinde kartla alışveriş yapılması, kartların hamil ile yapılan anlaşma ile belirlenmiş olan limitin üzerinde kullanılması, ATM cihazına müdahale sonucu veya ATM önünde kart hamili yanıltılarak ele geçen kartların kullanılması, ölen kişinin banka kartının kullanılması suretiyle hesabından para çekilmesi, başkasının banka veya kredi kartının üye işyerinde slip çekilerek kullanılması

[293]Artuk, Gökçen ve Yenidünya, 2009, a.g.k., 4692-4693.
[294]Dülger, 2013, a.g.k., 439.

örnek olarak verilebilir.[295] Bu yöntemlerin uygulanabilmesi için her durumda kartın fiziki varlığı da gerekmez. Fiziken ele geçirilmeyen veya elde bulundurulmayan kredi kartlarıyla da suç işlenebilir. Çünkü, Banka Kartları ve Kredi Kartları Kanunu (BKKKK)'nda kredi kartı fiziki varlığı bulunmayan kart numarasını da içerecek şekilde tanımlanmıştır. Fakat, aynı durum banka kartları için geçerli değildir. Banka kartlarının kötüye kullanılması için kart numarası tek başına yeterli değildir. Kartın fiziken de elde bulundurulması ya da ele geçirilmiş olması gerekir.[296] Doktrinde banka ve kredi kartlarının kötüye kullanılması suçunda gerek kredi kartı için gerek banka kartı için suçun oluşumunu kartın mutlak surette fiziken ele geçirilmiş olması şartına bağlayan yazarlar da vardır.[297]

Sahte banka veya kredi kartı üretilmesi, satılması, devredilmesi, satın alınması veya kabul edilmesi (m. 245/2)

245. maddenin 2. fıkrasında düzenlenen suçun hareket unsurunu, başkalarına ait banka hesaplarıyla ilişkilendirerek sahte kart üretilmesi, satılması, devredilmesi, satın alınması, kabul edilmesi fiilleri oluşturur. Suçun oluşabilmesi için seçimlik hareketlerden sadece birinin yapılmış olması yeterlidir. Bu fıkradaki suç, soyut tehlike suçudur. Çünkü, fıkrada belirtilen fiiller neticesinde yarar elde edilmiş olması gibi bir şart aranmamıştır.[298]

Madde metninde sayılan seçimlik hareketlerin birden fazlası, aynı kişi tarafından gerçekleştirilirse tek bir suç oluşacaktır. Örneğin, fail, sahte banka veya kredi kartını ürettikten sonra bu kartı satar veya devrederse 245. maddenin 2. fıkrasını bir kez ihlal etmiş olacaktır.[299]

Banka veya kredi kartlarının kötüye kullanılması fiilleri arasında yer alan sahte kredi kartı üretimi ve kullanımına sık rastlanmaktadır. Kart sahteciliği de denebilecek sahte kredi kartı üretilmesi fiili çeşitli yöntemlerle gerçekleştirilebilir. Son zamanlarda en sık rastlanan yöntemler, boş plastik, tahrif edilmiş kart, manyetik şerit sahteciliği ve

[295]Dülger, 2013, a.g.k. 439-449.; M.E. Yıldız (2011). *Banka veya Kredi Kartlarının Kötüye Kullanılması Suçu.* Yayımlanmamış Yüksek Lisans Tezi. İzmir: Dokuz Eylül Üniversitesi, s. 75-101.
[296]Yaşar, Gökçan ve Artuç, 2010, a.g.k., 6804.; Özbek, Doğan, Bacaksız ve Tepe, 2016, a.g.k., 972-973.
[297]Koca ve Üzülmez, 2016, a.g.k., 853.; Koca, 2010, a.g.k., 1654-1655. ; Özbek, Doğan, Bacaksız, Tepe, 2016, a.g.k., 972.
[298]Parlar, 2011, a.g.k., 54.; Kurt, 2005, a.g.k., 188.
[299]Özbek, 2007, a.g.k., 1048.

sahte müracaat yöntemidir.[300]

Faillerin, sahte banka veya kredi kartı üretebilmek için başkalarına ait kart bilgilerini ele geçirme yöntemleri arasında bugün için hacking, balık avlama, wireless, network hırsızlığı yöntemleri bilinmektedir. Uygulamada genellikle, yurt dışında ve özellikle de Avrupa ülkelerinde bulunan bankaların üretmiş olduğu banka veya kredi kartlarına ait bilgileri, saydığımız yöntemlerle ele geçiren failler bunları kopyalayarak çoğaltmaktadırlar.[301]

Belirtmek gerekir ki sahte banka veya kredi kartı üretilmesi fiziksel olarak değil de sanal ortamda gerçekleştirilse dahi bu suçu oluşturur. Bir banka hesabıyla ilişkilendirmek suretiyle, sanal ortamda hukuka aykırı bir şekilde o hesaba bağlı olarak bir sahte kart oluşturulması mümkündür. Oluşturulan sahte kartın, satılması, devredilmesi, satın alınması veya kabul edilmesi de 245/2. maddedeki suçu oluşturacaktır.[302]

Son olarak, başkasının kimliğiyle ya da gerçeğe aykırı düzenlenmiş olan bir belgeyle kart çıkarmaya yetkili olan kuruluşa başvurularak banka veya kredi kartı üretilmesinin sağlanması fiilinin bu suçu oluşturup oluşturmayacağını incelemek gerekir. Böyle bir durumda kimlik bilgileri kullanılan kişiden habersiz onun adına kart çıkartıldığı için üretilen banka veya kredi kartı sahtedir.[303] Dolayısıyla, burada 245/2' de düzenlenen suçun oluştuğu düşünülebilir. Ancak, buradaki sahtecilik doğrudan kartın üzerinde yapılmamıştır. Fail, kendisi sahte bir kart üretmemiş, gerçeğe aykırı belge veya beyanla sahte bir kartın üretilmesini sağlamıştır. Fiil, suçun kanuni tanımına uymamaktadır. Bu durumda fail BKKKK'nın 37/2. maddesine göre cezalandırılmalıdır. Bu maddeye göre, kredi kartı veya üye işyeri sözleşmesinde veya eki belgelerde

[300]Ayrıntılı bilgi için bkz. Artuk, Gökçen ve Yenidünya, 2009, a.g.k., 4694-4695.; Boş plastik yönteminde, fail, kredi kartı boyutundaki boş plastik plakalara gerçek kredi kartlarına ait numaraları basar, daha sonra müşteri sanki alışveriş yapmış gibi, bu kartı imprinter cihazından geçirerek satış belgesi düzenletir ve sonra bu parayı bankadan tahsil eder. Tahrif edilmiş kart yönteminde, fail, kendisine ait ya da bir şekilde ele geçirdiği kredi kartındaki numarayı, ütüleme yöntemiyle yok eder ve yerine başkasına ait bir numara basar. Manyetik şerit sahteciliği yönteminde, fail, kendisine ait kredi kartının arkasındaki manyetik şerit bilgilerini siler ve encoder cihazıyla başkasına ait bilgileri yükler. Sahte müracaat yönteminde, fail gerçek olmayan kimlik belgeleriyle banka şubesine müracaat ederek sahte kart çıkartır. Bkz. http://arsiv.ntv.com.tr/news/195214.asp#BODY (Erişim Tarihi: 06.08.2017)

[301]Esen, 2007, a.g.k., 645-646.

[302]Dülger, 2013, a.g.k., 451.

[303]Yıldız'a göre, bu durum belgede sahtecilik suçlarındaki fikri sahteciliğe benzemektedir. bkz. Yıldız, 2011, a.g.k., 143.

sahtecilik yapılması veya sözleşme imzalamak amacıyla sahte belge ibraz edilmesi halinde fail bir yıldan üç yıla kadar hapisle cezalandırılacaktır. Başkasının kimliğiyle ya da gerçeğe aykırı düzenlenmiş olan bir belgeyle kart çıkartılmasının sağlanması fiilinin TCK 245/2'de düzenlenen suçun kanuni tanımına uyduğunun kabulü halinde dahi BKKKK 37/2'nin daha sonra yürürlüğe girmesi ve 245/2 hükmüne göre özel bir norm olması sebebiyle failin yine BKKKK 37/2'de düzenlenen suç tipinden cezalandırılması gerekir.[304]

Sahte banka veya kredi kartlarının kullanılması suretiyle yarar sağlanması (m. 245/3)

245. maddenin 3. fıkrasında düzenlenen suçun hareket unsurunu sahte oluşturulmuş veya üzerinde sahtecilik yapılmış bir banka veya kredi kartını kullanmak suretiyle kendisine veya başkasına yarar sağlamak fiili oluşturur. Serbest hareketli bir suçtur. Failin sahte banka veya kredi kartını kendi oluşturması gerekmemektedir, bu tür kartları kullanarak haksız yarar elde etmesi suçun oluşması için yeterlidir. Örneğin, fail sahte olarak oluşturulan banka veya kredi kartını kullanarak ATM'den kendisi veya bir başkası hesabına para havale etmesi halinde suç tamamlanmış olacaktır, bu kişilerden birinin anılan parayı bankadan çekmesine gerek yoktur.[305]

Burada dikkat edilmesi gereken husus, failin bu fıkra kapsamında cezalandırılabilmesi için madde metninde de belirtildiği üzere fiilinin, daha ağır cezayı gerektiren başka bir suçu oluşturmamasıdır. Aksi takdirde, fail, daha ağır cezayı gerektiren başka suçu her neyse ona göre cezalandırılacaktır.

3. fıkradaki suç tipi serbest hareketli olarak düzenlendiğinden dolayı suç çeşitli yöntemlerle işlenebilir. Gelişen teknoloji ve bilişim alanındaki ilerlemeler de bu çeşitliliği artırmaktadır. Bu sebepten ötürü, tüm yöntemlerin bilindiği söylenemez. Dolayısıyla, burada sadece bugüne kadar uygulamada rastlanmış ve artık bilinen işlenme yöntemleri belirtilebilir. Bu yöntemler, gerçeğe aykırı sahte belgelerle çıkarılan kartlarla yarar sağlanması, sahte kartlarla gerçek olmayan satış belgesi düzenlenmesi, sahte kartların alışverişte kullanılması, sahte banka veya kredi kartının üye işyerinde slip çekilerek kullanılması olarak sayılabilir.[306]

[304]Aynı yönde bkz. Yıldız, 2011, a.g.k., 143-144.; Taşkın, 2008, a.g.k., 74-75.; Özbek, Doğan, Bacaksız ve Tepe, 2016, a.g.k., 974.; Dülger, 2013, a.g.k., 469-470.
[305]Yaşar, Gökçan ve Artuç, 2010, a.g.k. 6809.
[306]Dülger, 2013, a.g.k., 463.

2.3.1.9.4.2. Fail ve mağdur

Banka ve kredi kartlarının kötüye kullanılması suçunun faili herkes olabilir. Madde metninde fail için herhangi bir özellik aranmamıştır. Banka veya kredi kartlarını ele geçiren veya elinde bulundurarak bunları sahibinin rızası hilafına kullanmak suretiyle yarar sağlayan ya da sahte banka veya kredi kartı oluşturan veya gerçek bir kart üzerinde sahtecilik yapmak suretiyle yarar sağlayan herhangi bir kişi suçun faili olabilir.[307]

Bu maddede mağdur açısından da bir özellik öngörülmemiştir. Dolayısıyla, herkes suçun mağduru olabilmektedir. Fakat, belirtmek gerekir ki 245. maddedeki suçun işlenmesi sırasında kendi şirketlerine ait olan banka veya kredi kartları kullanılan banka veya kredi kurumlarının bu suçun mağduru mu, suçtan zarar göreni mi olduğu doktrinde tartışmalıdır. Suçtan zarar gören, ceza hukuku normuyla korunan hukuki yararı ihlal edilmiş kişidir. Bu kişiye aslında suçun mağduru da denilebilir. Fakat, bazı suçlar açısından mağdur ile suçtan zarar gören farklılaşır. Örneğin, adam öldürme suçunda, suçun mağduru ölen kişi, suçtan zarar gören ise mağdurun yakınlarıdır.[308] Doktrinde, banka veya kredi kartlarının kötüye kullanılması suçunda da mağdur ile suçtan zarar gören kişinin farklılaştığını söyleyen yazarlardan olan Yılmaz, bu suçlarda banka veya kredi kurumunun mağdur değil, suçtan zarar gören olacağını söyleyerek esas mağdurun kartın hamili olduğunu belirtmektedir.[309] Yargıtay'ın da mağdurun kart hamili olduğuna yönelik kararı vardır.[310] Başka bir görüşe göre, bu suçun mağduru banka veya kredi kartının hamilidir. Kart hamili gerçek ya da tüzel kişi olabilir. Fakat, aynı zamanda bu suçlarda mağdur banka veya kredi kartının asıl sahibi olan banka ya da finans kuruluşudur.[311] Yargıtay vermiş olduğu bir kararda[312] kartın henüz kullanılmamış olması sebebiyle, suçun mağdurunun kredi kartı çıkartma yetkisini haiz banka olacağını söyleyerek bankanın suçun mağduru olduğunu kabul etmiştir. Yargıtay başka bir kararında[313] da sanığın, katılan adına düzenlenen sahte kredi kartıyla birden fazla bankadan kredi kartı çıkartması şeklinde gerçekleşen fiilinin mağdur banka sayısınca

[307]Esen, 2007, a.g.k., 643.
[308]Ünver ve Hakeri, 2010, a.g.k., 307-310.
[309]Yılmaz, 2010, a.g.k., 268.; aynı yönde bkz. Koca ve Üzülmez, 2016, a.g.k., 848.
[310]Yargıtay Ceza Genel Kurulu'nun 18.10.2011 tarih ve 2011/6-166 Esas ve 2011/213 Karar sayılı kararı.
[311]Özbek, 2007, a.g.k., 1029.; Özbek, Doğan, Bacaksız ve Tepe, 2016, a.g.k., 970.; Koray doğan, 309.
[312]Yargıtay 11. Ceza Dairesi'nin 20.02.2008 tarih ve 2007/ 8458 Esas ve 2008/ 915 Karar sayılı kararı.
[313]Yargıtay 8. Ceza Dairesi'nin 08.02.2016 tarih ve 2015/12565 Esas ve 2016/1121 Karar sayılı kararı.

suç oluşturacağını söyleyerek burada mağdurun banka olduğunu belirtmiştir. Kanımızca, banka ve kredi kartlarının kötüye kullanılması suçunda, bu kartların hamili mağdur olmaktadır. Çünkü, mağdur hukuki yararı ihlal edilen kişidir. Banka ve kredi kartı rızası hilafına kullanılan kart hamili burada maddi bir zarara uğrayacak, yani mülkiyet hakkı ihlal edilmiş olacaktır. Banka veya kredi kurumlarının ise bu kartların kötüye kullanılması neticesinde genel olarak, bankacılık sektörüne olan güvenle birlikte kendilerine duyulan güven de zedeleneceğinden ve ayrıca maddi bir zarara uğrama ihtimali de olmasından dolayı hukuki yararı ihlale uğrayacaktır.

2.3.1.9.4.3. Netice

Netice açısından, 245. maddenin birinci fıkrasındaki suç tipi zarar suçudur. Madde metninde failin, fiili neticesinde kendisine veya bir başkasına yarar sağlaması gerektiği belirtilmiştir. 2. fıkrada düzenlenen suç tipinde yarar sağlamak gibi bir şart aranmamıştır. Failin, fıkrada sayılan hareketlerden birini gerçekleştirmiş olması durumunda suç oluşacaktır. Dolayısıyla, burada bir soyut tehlike suçu söz konusudur. 3. fıkrada düzenlenen suç tipinde 1. fıkrada olduğu gibi failin kendisine veya bir başkasına yarar sağlaması gerektiği belirtildiğinden bu suç zarar suçudur. Failin, kendisi veya bir başkası lehine sağlayacağı yarar mağdur açısından bir zarara sebebiyet verecektir. Fakat, mağdurun zarar görmüş olması şartı ayrıca madde metninde aranmamıştır.[314]

2.3.1.9.5. Manevi unsur

Banka veya kredi kartlarının kötüye kullanılması suçu ancak kastla işlenebilir. Genel kast yeterlidir, kanun koyucu failde özel bir kast aramamıştır. Kanunda suçun taksirli hali açıkça düzenlenmediğinden dolayı cezalandırılmaz.[315] TCK'nın 245. maddesinde, 765 sayılı TCK'nın 525/b-2 maddesinin aksine, failin, belli bir saikle hareket etmiş olması şartı aranmamıştır.[316]

2.3.1.9.6. Hukuka aykırılık unsuru

Türk Ceza Kanunu'nun 245. maddesindeki suç tipi açısından öngörülen hukuka uygunluk sebebi ilgilinin rızasıdır.[317] İlgilinin rızasından kasıt, şekli anlamda kart sahibi

[314]Dülger, 2013, a.g.k., 463-464.; Özbek, Doğan, Bacaksız ve Tepe, 2016, a.g.k., 991.
[315]Yılmaz, 2010, a.g.k., 282.; Koca ve Üzülmez, 2016, a.g.k., 854.
[316]Artuk, Gökçen ve Yenidünya, 2009, a.g.k., 4698.; Mahmutoğlu, 2013, a.g.k., 875.
[317]Parlar, 2011, a.g.k., 54.; Dülger, 2013, a.g.k., 465-467.

olan kişi veya kartın kendisine verilmesi gereken kişinin rızasıdır. Bu kişiler, kartın kullanılmasından önce veya kart kullanıldıktan sonra rıza gösterirlerse, fail cezalandırılmaz.[318]

2.3.1.9.7. Şahsi cezasızlık sebebi

245. maddenin 4. fıkrasında, "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 evlatlığın, c) aynı konutta beraber yaşayan kardeşlerden birinin zararına işlenmesi halinde, ilgili akraba hakkında cezaya hükmolunmaz" denilerek belli akrabalar açısından şahsi cezasızlık sebebi öngörülmüştür.

245. maddenin birinci fıkrasındaki "her ne suretle olursa olsun ele geçirmek veya elinde bulundurmak" ifadesi karşısında böyle bir şahsi cezasızlık sebebinin düzenlenmiş olması isabetli olmuştur.[319] Çünkü, böyle bir hüküm olmasaydı, örneğin, babası uyurken onun kredi kartını alan çocuğun bu kartla alışveriş yapması suç oluşturacak ve çocuğun cezalandırılması gerekecekti.

Birinci fıkradaki suç tipi açısından şahsi cezasızlık sebebinin öngörülmüş olması, bu suçla korunan hukuki değer açısından da isabetli olmuştur. Bu fıkrada korunan hukuki değerin özellikle malvarlığı hakları olduğunu yukarıda belirtmiştik. Hatta bu hüküm, 245/1 deki suç tipinin aslında malvarlığına karşı bir suç olduğunun da üstü kapalı kabulü anlamına gelmektedir.[320]

Kanun koyucu 5237 sayılı TCK'nın malvarlığına karşı suçlar başlıklı bölümündeki suç tipleri açısından (yağma ve nitelikli yağma hariç) şahsi cezasızlık sebebi öngörmüştür. TCK'nın 167. maddesinin birinci fıkrasında haklarında şahsi cezasızlık sebebi uygulanacak ilgili akrabaların kimler olduğu sayılmıştır. 245/4. maddede de bu kişiler aynen tekrarlanmıştır. Fakat, 167. maddenin 2. fıkrasında bazı akrabalar için öngörülmüş olan cezada indirim yapılmasını gerektiren düzenlemeye 245. madde açısından yer verilmemesi isabetsiz olmuştur. Yine malvarlığına karşı suçlarda hakkını almak amacıyla bu suçların işlenmesi durumu daha az cezayı gerektiren hal

[318]Kurt, 2005, a.g.k., 194.
[319]Parlar, 2011, a.g.k., 55.; Yaşar, Gökçan ve Artuç, 2010, a.g.k., 6810
[320]Özbek, 2007, a.g.k., 1036.; Özbek, Doğan, Bacaksız ve Tepe, 2016, a.g.k., 976.

olarak düzenlenmiştir. Fakat, 245. maddede bu düzenlemeye de ceza hukukunun genel ilkelerine aykırı olarak yer verilmemiştir.[321] Ayrıca TCK 147. maddedeki ağır ve acil bir ihtiyacın karşılanması için suçun işlenmesi durumuna bu suç tipinde yer verilmemiş olması da haklı olarak doktrinde eleştirilmektedir.[322]

245. maddenin 4. fıkrasındaki düzenleme açısından yapılacak bir başka eleştiri ise, haklarında ayrılık kararı verilmemiş eşler için şahsi cezasızlık sebebi öngörülmesidir. Çünkü, boşanma sürecinde olan eşler haklarında ayrılık kararı verilmeksizin birbirlerinden ayrı yaşamaktadırlar. Ayrıca, ülkemizde aile mahkemelerinin pek ayrılık kararı vermediği de bilinen bir gerçektir. Bu fıkraya göre, ise boşanma sürecindeki eşlerden biri, diğerine sırf zarar vermek amacıyla onun banka veya kredi kartını ele geçirerek alışveriş yapabilir. Görüldüğü gibi, buradaki şahsi cezasızlık sebebi, amacını aşarak kötü niyetli eşler için bir ödül haline gelmektedir. Dolayısıyla, kanun koyucu bu hükmü tekrar gözden geçirmelidir.[323] Burada, haklarında ayrılık kararı verilmemiş olan eşler açısından şahsi cezasızlık sebebinin uygulanması için hakime takdir yetkisi verilmesi düşünülebilir.[324] Böylece, boşanma sürecinde eşlerden birinin sırf diğer eşe zarar vermek için onun banka ve kredi kartlarını kötüye kullanabilmesinin önüne geçilebilir.

2.3.1.9.8. Etkin pişmanlık

245. maddenin 5. fıkrasına göre, birinci fıkrada sayılan fiillerle ilgili malvarlığına karşı suçlara ilişkin etkin pişmanlık hükümleri uygulanacaktır. TCK'nın ilk halinde yer almayan bu hüküm, anayasal eşitliği sağlamak amacıyla 19.12.2006 tarih ve 5560 sayılı Kanun'la getirilmiştir. Böylece, bu suç malvarlığına karşı işlenen suçlarla benzerlik göstermiştir.[325]

Malvarlığına karşı suçlara ilişkin etkin pişmanlık, TCK'nın 168. maddesinde düzenlenmiştir. Bu hükme göre, failin etkin pişmanlıktan yararlanması için: 1) Suçun tamamlanmış olması, 2) Failin azmettirenin veya yardım edenin bizzat pişmanlık göstererek mağdurun uğradığı zararı aynen geri verme veya tazmin suretiyle gidermiş

[321]Kurt, 2005, a.g.k., 195.
[322]Tezcan, Erdem ve Önok, 2017, a.g.k., 995.
[323]Dülger, 2013, a.g.k., 509.; Özbek, 2007, a.g.k., 1037.; Özbek, Doğan, Bacaksız ve Tepe, 2016, a.g.k., 976-977.
[324]Yıldız, 2011, a.g.k., 110-111.
[325]Yaşar, Gökçan ve Artuç, 2010, a.g.k., 6812.

olması, eğer kısmen giderme söz konusuysa mağdurun buna rıza göstermesi, 3) Aynen geri verme veya tazminin kovuşturmadan önce veya kovuşturma başlamışsa hüküm verilmeden önce gerçekleştirilmiş olması gerekir. Etkin pişmanlık için suçun tamamlanmış olması şartı arandığından teşebbüs aşamasında kalmış fiiller için bu hüküm uygulanamayacaktır.[326]

Failin, etkin pişmanlık hükümlerinden yararlanabilmesi için bizzat pişmanlık göstererek iadeyi yapmış olması gerekir. Bu pişmanlık ifadesi, failin pişmanım demesinin yanı sıra mağdurdan özür dilemesi ya da bir daha yapmayacağını beyan etmesi şeklinde de gerçekleşebilir. Fail, hiçbir etki altında kalmadan pişmanlık göstermelidir.[327] Bunun yanı sıra, failin, pişmanlık göstererek zararı bizzat gidermesi gerekliliğinden kasıt, failin, bilgisi dahilinde iradesine uygun olarak ve talebi doğrultusunda bunun yapılmasıdır. Yani failin, fiziken zararı bizzat tazmin etme olanağı olmadığı durumlarda onun iradesine uygun olarak bir başkası bu zararı tazmin edebilir.[328] Bu durumlara örnek olarak, failin cezaevinde olması, ağır hasta olması ya da uzun bir süre yurtdışında olması gibi durumlar verilebilir.

Mağdurun, uğradığı zararın geri verme veya tazmin yolu ile giderilmesi şartı açısından, zararın tamamının giderilip giderilmediği konusunda karar verme yetkisi hakime aittir. Hakim, bu konuda uzman görüşünden de yararlanabilir. Eğer kısmen geri verme ya da tazmin söz konusuysa, burada ayrıca mağdurun rızası da aranacaktır.[329]

Etkin pişmanlığın uygulanabilmesinin bir diğer şartı olan zararın giderilmesinin kovuşturmadan önce veyahut en geç hükümden önce gerçekleşmesi açısından tartışma, zararın giderilmesi hükmün ilk derece mahkemesinde verilmesi aşamasına kadar mı yoksa istinaf mahkemesi veyahut Yargıtay tarafından kararın onanması aşamasına kadar mı gerçekleştirileceği noktasındadır. Burada, ilk derece mahkemesinde karar verilmesi aşamasına kadar bunun mümkün olduğunun kabulü gerekir. Eğer istinaf mahkemesi veyahut Yargıtay tarafından kararın onanması aşamasına kadar bunun mümkün olduğu kabul edilirse, ilk derece mahkemesince hüküm verildikten sonra aynen iade veya

[326]Artuk, Gökçen ve Yenidünya, 2011, a.g.k., 723.
[327]Yaşar, Gökçan ve Artuç, 2010, a.g.k., 6814
[328]Dülger, 2013, a.g.k., 511.; Özbek, 2007, a.g.k., 1039.; Özbek, Doğan, Bacaksız ve Tepe, 2016, a.g.k., 978-979.
[329]Artuk, Gökçen ve Yenidünya, 2009, a.g.k., 4704.

tazminin yapılması durumunda mahkeme kararı tekrar incelemek zorunda kalacaktır, tekrar inceleme halinde ise istinaf mahkemesi veyahut Yargıtay bunu mutlak bozma sebebi sayarak bozacak ve dosyayı tekrar ilk derece mahkemesine yollayacaktır. Böylece, yargılama gereksiz yere uzayacak ve yargılama maliyeti de artacaktır. Ayrıca, bu süreç içerisinde zamanaşımına uğrayacak dosyalar hakkında da düşme kararı verilecektir.[330]

2.3.1.9.9. Suçun özel görünüş şekilleri

2.3.1.9.9.1. Teşebbüs

Banka veya kredi kartlarının kötüye kullanılması suçu teşebbüse elverişlidir. 245/1. maddede düzenlenen suç zarar suçudur. Failin kendisine veya bir başkasına yarar sağlaması şeklinde bir neticenin meydana gelmesiyle bu suç tamamlanır. Ancak, failin elverişli vasıtalarla icra hareketlerini tamamlaması ve fakat kendisine veya bir başkasına yarar sağlayamamış olması halinde suç teşebbüs aşamasında kalmış olacaktır. Teşebbüse örnek olarak, sanığın, kredi kartıyla yaptığı işlemlerin işyerleri tarafından iptal edilmesi ve satışa konu ürünlerin sanığa teslim edilmemesi[331], mağdurun kredi kartı bilgilerini ele geçiren sanığın internetten sipariş vermesi ancak mağdurun satıcı firmaya ulaşarak siparişleri iptal ettirmesi[332] verilebilir.

Failin, banka veya kredi kartını her ne suretle olursa olsun ele geçirmesi veya elinde bulundurması ancak kartı kullanamadan yakalanması durumunda bu suça teşebbüsün oluşup oluşmayacağını incelemek gerekir. Bu konuda doktrinde farklı görüşler ileri sürülmüştür. Bir görüşe göre, banka veya kredi kartlarının kötüye kullanılması suçunun icra hareketleri kartın kullanılması ya da kullandırılmasıdır. Bir şekilde kartı ele geçirmiş olan kimsenin kartı kullanmaya yönelik bir hareketi olmaksızın yakalanması halinde kartı ele geçirmesi ayrı bir suç oluşturuyorsa kişiye oluşan suçtan ceza verilmelidir.[333] Başka bir görüşe göre, bir şekilde kartı ele geçirmiş olan failin kartı kullanamadan yakalanmış olması durumunda fiilin nitelendirilmesinde failin kastına bakılmalıdır. failin kastı eğer 245/1. maddedeki suçu işlemekse bu suça teşebbüsten, eğer failin böyle bir kastı yoksa kartı ele geçiriş şekli hangi suçu

[330]Dülger, 2013, a.g.k., 510.; Artuk, Gökçen ve Yenidünya, 2009, a.g.k., 4704.; karşı görüş için bkz. Yaşar, Gökçan ve Artuç, 2010, a.g.k., 6815.
[331]Yargıtay 8. Ceza Dairesi'nin 21.02.2017 tarih ve 2016/10914 Esas ve 2017/1618 Karar sayılı kararı.
[332]Yargıtay 8. Ceza Dairesi'nin 16.04.2014 tarih ve 2013/11662 Esas ve 2014/9785 Karar sayılı kararı.
[333]Yıldız, 2011, a.g.k., 120-121.; Dülger, 2013, a.g.k., 468-469.

oluşturuyorsa sadece ona göre cezalandırılmalıdır.[334] Kanımızca, birinci görüş daha isabetlidir. Çünkü, her ne kadar banka veya kredi kartını ele geçiren kişinin bir sonraki aşamada bu kartı kullanarak yarar sağlamaya çalışacağı çoğu zaman aşikar olsa bile 245/1. maddede düzenlenen suçun icra hareketleri ele geçirilmiş ya da elde bulundurulan kartın kullanılması ya da kullandırılmasıdır. Kartın ele geçirilmesi bu suç için ancak hazırlık hareketi olarak değerlendirilebilir. Teşebbüsten bahsedebilmek için de elverişli vasıtalarla suçun icra hareketlerine başlanması gerekmektedir. Dolayısıyla, böyle bir durumda kartı ele geçirmesi bir suç oluşturuyorsa faile sadece oluşan suçtan dolayı ceza verilmelidir. Nitekim Yargıtay'ın görüşü de bu yöndedir. Örneğin, Yargıtay, failin yerleştirdiği düzenek sayesinde para çekmek amacıyla ATM'ye gelen banka müşterilerinin kartlarının sıkışmasını sağlayarak onlara ait kartları ele geçirmeye çalışırken yakalanmasından ibaret fiilini hırsızlığa teşebbüs olarak nitelendirmiştir.[335]

Maddenin 2. fıkrasında düzenlenen suç, soyut tehlike suçudur. Bu sebeple, fıkrada belirtilen seçimlik hareketlerin bir ya da birkaçının gerçekleşmiş olması halinde suç tamamlanmış olacaktır. İcra hareketlerinin parçalara bölünebildiği durumlarda teşebbüs failin, elverişli vasıtalarla suçun icra hareketlerine başlaması fakat elinde olmayan sebeplerle icra hareketlerini tamamlayamaması halinde mümkündür.[336] Örneğin, failin başkasına ait hesapla ilişkilendirerek kart üretmeye çalıştığı esnada yakalanması halinde kartı henüz üretemediğinden teşebbüsten sorumlu olacaktır.[337]

Maddenin 3. fıkrasında düzenlenen suç zarar suçudur. Failin kendisine veya bir başkasına yarar sağlaması şeklinde bir neticenin meydana gelmesiyle bu suç tamamlanır. Ancak failin elverişli vasıtalarla icra hareketlerini tamamlaması ve fakat kendisine veya bir başkasına yarar sağlayamamış olması halinde suç teşebbüs aşamasında kalmış olacaktır. 2. fıkradaki fiiller bu suç açısından hazırlık hareketi niteliğindedir. Bundan dolayı sahte kredi kartını satın almak ya da kabul etmek bu suça teşebbüs olarak değerlendirilemez. Failin bu suça teşebbüsten sorumlu tutulabilmesi için kartı kullanması gerekmektedir.[338] Bir görüşe göre, failin sahte bir kart oluşturması ve bu esnada yakalanması halinde eğer kastı 3. fıkradaki suçu işlemekse faile 3.

[334]Karagülmez, 2009, a.g.k., 279, 339.
[335]Yargıtay 8. Ceza Dairesi'nin 22.09.2014 tarih ve 2014/6182 Esas ve 2014/20376 Karar sayılı kararı.; Yargıtay 8. Ceza Dairesi'nin 31.03.2014 tarih ve 2014/2161 Esas ve 2014/8038 Karar sayılı kararı.
[336]Yıldız, 2011, a.g.k., 150.
[337]Karagülmez, 2009, a.g.k., 339.
[338]Yıldız, 2011, a.g.k., 164-165.; Dülger, 2013,a.g.k., 470-471.

fıkradaki suça teşebbüsten ceza verilmesi gerektiğini söylemektedir.[339] Ancak suçun icra hareketinin kartın kullanılması olması ve sahte kart oluşturulmasının bu suç için hazırlık hareketi olması dolayısıyla bu görüşe katılmak mümkün değildir.

2.3.1.9.9.2. İştirak

Banka ve kredi kartlarının kötüye kullanılması suçu iştirak açısından bir özellik göstermez.

2.3.1.9.9.3. İçtima

Banka ve kredi kartlarının kötüye kullanılması suçunun zincirleme şekilde işlenmesi mümkündür. Suçun, bir suç işleme kararının icrası kapsamında farklı zamanlarda aynı mağdura karşı işlenmesi halinde zincirleme suç hükümleri uygulanacaktır. Örnek vermek gerekirse, aynı hamilin kullanmış olduğu banka veya kredi kartını ele geçiren failin bu kartla farklı zamanlarda alışveriş yapmış olması ya da aynı hamilin kullanımında olan fakat farklı bankalara ait olan banka veya kredi kartıyla farklı zamanlarda alışveriş yapmış olması halinde bu suçun mağdurunun kart hamili olması sebebiyle zincirleme suç oluşacaktır. Bunun yanı sıra, aynı bankaya ait fakat farklı hamiller tarafından kullanılan banka veya kredi kartlarının kullanılması halinde zincirleme suç hükümleri uygulanmayacak, hamil sayısı kadar suç oluşacaktır.[340]

Suçun bir bileşik suç olup olmadığı konusunda birinci fıkrada banka veya kredi kartının her ne suretle olursa olsun ele geçirilmiş olması ifadesinden ne anlaşılması gerektiğini açıklamak gerekir. Burada kanun koyucu, bir bileşik suç oluşturma amacında değildir. Hatta bu ifadeyle kanun koyucu, hukuka uygun fiilleri kastetmektedir. Diğer bir deyişle, fail banka veya kredi kartını hukuka uygun yollarla elde etmiş olsa bile, bu kartları hukuka aykırı olarak kullanarak kendisine veya başkasına yarar sağlarsa suç oluşacaktır. Fail, banka veya kredi kartını örneğin, dolandırıcılık, hırsızlık, güveni kötüye kullanma ya da yağma suretiyle[341] hukuka aykırı olarak ele geçirse ve 245/1. maddedeki suçu işlemiş olsa, hem kartı ele geçirmek için

[339]Karagülmez, 339.
[340]Aynı yönde Dülger, 2013,a.g.k., 475-479.; Yıldız, 2011, a.g.k., 133-134.; Özbek, Doğan, Bacaksız ve Tepe, 2016, a.g.k., 981.; Koca ve Üzülmez, 2016, a.g.k., 861.
[341]Yargıtay, sanıkların cebir ve tehditle katılanın 600 TL parasıyla birlikte farklı bankalara ait kredi kartlarını ele geçirmeleri ve yine cebir ve tehditle kartların şifrelerini öğrenmelerinden ibaret fiillerinin banka veya kredi kartlarının kötüye kullanılması suçunun yanı sıra yağma suçunu da oluşturacağını belirtmiştir. Bkz. Yargıtay Ceza Genel Kurulu'nun 18.10.2011 tarih ve 2011/6-166 Esas ve 2011/213 Karar sayılı kararı.

işlediği suçtan, hem de 245/1. maddedeki suçtan dolayı cezalandırılacaktır.[342] Yargıtay uygulaması da bu yöndedir. Yargıtay, konuya ilişkin vermiş olduğu kararlarında her ne surette olursa olsun ele geçirme tabirinin hukuka uygun olarak ele geçirmeyi ifade ettiği, kartın hukuka aykırı olarak ele geçirilmesinden sonra kullanılmasının iki ayrı suçu oluşturacağı, banka veya kredi kartının hukuka aykırı olarak ele geçirilmesi eyleminin hırsızlık, kartın kullanılarak menfaat elde edilmesi eyleminin banka veya kredi kartının kötüye kullanılması suçunu oluşturacağını belirtmiştir.[343] Sonuç olarak, kanun koyucunun bu maddede, her ne suretle olursa olsun ele geçirme ifadesine bir bileşik suç oluşturmak için değil, hukuka uygun olarak ele geçirilen banka veya kredi kartlarının dahi kötü niyetli kullanımını cezalandırmak amacıyla yer verdiği söylenebilir.[344]

Failin sahte olarak ürettiği ya da gerçek bir kart üzerinde sahtecilik yaptığı banka veya kredi kartını kullanarak haksız yarar elde etmesi durumunda içtima sorununun nasıl çözüleceğiyle ilgili doktrinde iki farklı görüş vardır. Birinci görüşe göre[345], burada bir geçitli suç oluşmaktadır. Şöyle ki failin sahte bir banka veya kredi kartını kullanmak suretiyle kendisi veya bir başkası için hukuka aykırı yarar elde edebilmesi için öncelikle bu kartı üretmesi, satın alması ya da bir şekilde kabul etmiş olması gerekir. Yani, 245. maddenin 3. fıkrasındaki suçun işlenebilmesi için 2. fıkrada düzenlenen suç geçit suçu olmaktadır. Bu durumda fail sadece 245/3. maddeye göre cezalandırılmalıdır. İkinci görüşe göre[346], fail sahte bir banka veya kredi kartı oluşturduktan sonra ya da gerçek bir kart üzerinde sahtecilik yaptıktan sonra ayrıca bu kartı kullanırsa hem TCK' nın 245/2. maddesini hem de 245/3. maddesini ihlal etmiş olacaktır. Aynı şekilde fail, sahte olan ya da üzerinde sahtecilik yapılan banka veya kredi kartını satın almış veya kabul etmiş, daha sonra da kullanmışsa yine hem TCK'nın 245/2. maddesini hem de 245/3. maddesini ihlal etmiş olacaktır ve her iki suçtan da cezalandırılmalıdır. Çoğunlukla

[342]Esen, 2007, a.g.k., 644.; Özbek, Doğan, Bacaksız ve Tepe, 2016, a.g.k., 982.; Yıldız, 2011, a.g.k., 128; Bu durumda failin sadece 245/1. maddesi uyarınca cezalandırılması gerektiğine yönelik karşı görüş için bkz. Tezcan, Erdem ve Önok, 2017, a.g.k., 998.; Mahmutoğlu, 2013,a.g.k., 878.

[343]Yargıtay Ceza Genel Kurulu'nun 30.03.2010 Tarih ve 2010/11-17 Esas ve 2010/65 Karar Sayılı Kararı. Ayrıca Genel Kurul, bu kararında banka veya kredi kartlarını ekonomik değeri olan menkul mal niteliğini haiz, hırsızlık suçuna konu olabilecek eşya olarak kabul etmiştir; Yargıtay 8. Ceza Dairesi'nin 23.06.2016 Tarih ve 2016/4589 Esas ve 2016/8439 Karar Sayılı Kararı.

[344]Aynı yönde bkz. F.G. Taner (2007). Banka veya Kredi Kartlarının Kötüye Kullanılması Suçu Bileşik Suç mudur?. *AÜHFD*, 56 (2), 78-80.; Yıldız, 2011, a.g.k., 177.; Yılmaz, 2010, a.g.k., 283-284.

[345]Yılmaz, 2010, a.g.k., 281.; Dülger, 2013, a.g.k., 506.

[346] Yaşar, Gökçan ve Artuç, 2010, a.g.k., 6798.; Özbek, 2007, a.g.k., 1053.; Karagülmez, 2009, a.g.k., 316. ; Yıldız, 152-154.; Üzülmez, koca, 866.

kabul gören görüş 2. görüştür. Uygulamada Yargıtay'ın ikinci görüşe uygun olarak vermiş olduğu çok sayıda kararı vardır.[347]

Son olarak, 3. fıkradaki suçu içtima açısından değerlendirmek gerekir. Kanun koyucu faile bu suçtan dolayı ceza verilebilmesi için fiilin daha ağır cezayı gerektiren başka bir suç oluşturmaması şartını aramaktadır. Dolayısıyla, suç tamamlayıcı norm niteliğindedir. Faile, 3. fıkradaki suçtan ceza verebilmek için öncelikle fiilinin daha ağır cezayı gerektiren başka bir suç oluşturup oluşturmadığına bakılacaktır. Burada oluşabilecek muhtemel suçlar dolandırıcılık ve özel belgede sahteciliktir. Bu suçların yaptırımlarına bakılacak olursa, dolandırıcılık suçunun basit hali için öngörülen ceza bir yıldan beş yıla kadar hapis, nitelikli dolandırıcılık için üç ya da dört yıldan on yıla kadar hapis, özel belgede sahtecilik için bir yıldan üç yıla kadar hapis cezasıdır. Buna karşılık, 245/3. maddedeki suç için dört yıldan sekiz yıla kadar hapis cezasıdır. Görüldüğü üzere sahte banka veya kredi kartlarının kullanılması suretiyle oluşabilecek muhtemel suçlarda 245/3. maddedeki suçun yaptırımı diğerlerinden fazladır ve herhalde 245/3. madde uygulama alanı bulacaktır. Ayrıca TCK 44. maddedeki fiilin birden fazla suç oluşturması halinde faile cezası en ağır olan suçtan dolayı ceza verileceği hükmü karşısında 3. fıkradaki fiilin daha ağır cezayı gerektiren başka bir suçu oluşturmaması ifadesi gereksizdir. Belirttiğimiz nedenlerden dolayı kanaatimizce, kanun koyucunun bu suçu tamamlayıcı norm olarak düzenlemesi yerinde değildir.[348]

2.3.1.9.10. Yaptırım, soruşturma ve kovuşturma

Türk Ceza Kanunu'nun 245. maddesinin birinci fıkrasında düzenlenen başkasına ait kredi kartını kullanmak suretiyle kendisine veya başkasına yarar sağlamak suçu için hem hapis cezası hem de adli para cezası öngörülmüştür. Hapis cezasının alt sınırı üç yıl, üst sınırı altı yıldır. Adli para cezasının miktarı genel hükümlere göre belirlenecektir.

Maddenin ikinci fıkrasında düzenlenen sahte oluşturulan ya da üzerinde sahtecilik yapılmış olan banka veya kredi kartlarının, üretilmesi, satılması, devredilmesi, satın

[347]Yargıtay 8. Ceza Dairesi'nin 19.04.2016 tarih ve 2015/ 9501 Esas ve 2016/ 5237 Karar sayılı kararı.; Yargıtay 8. Ceza Dairesi'nin 29.03.2016 tarih ve 2016/ 1881 Esas ve 2016/ 4107 Karar sayılı kararı.; Yargıtay 8. Ceza Dairesi'nin 04.04.2016 tarih ve 2016/ 1781 Esas ve 2016/ 4371 Karar sayılı kararı.

[348]Aynı yönde bkz. Yıldız, 2011,a.g.k., 165-166.; Koca ve Üzülmez, 2016, a.g.k., 870. ; Karagülmez, 2009, a.g.k., 332.

alınması, kabul edilmesi suçu için hem hapis hem de adli para cezası öngörülmüştür. Hapis cezasının alt sınırı üç yıl, üst sınırı yedi yıldır. Adli para cezasının miktarı ise genel hükümlere göre belirlenecektir.

Maddenin üçüncü fıkrasında düzenlenen sahte oluşturulan ya da üzerinde sahtecilik yapılan banka veya kredi kartını kullanmak suretiyle kendisine veya başkasına yarar sağlamak suçu için de hem hapis hem de adli para cezası öngörülmüştür. Hapis cezasının alt sınırı dört yıl, üst sınırı sekiz yıldır. Adli para cezasının miktarı ise genel hükümlere göre belirlenecektir. Fakat, 245/3'te düzenlenmiş olan suçu işleyen faillerin bu fıkraya göre cezalandırılabilmesi fiillerinin daha ağır cezayı gerektiren başka bir suç oluşturmaması şartına bağlıdır.

Görevli mahkeme, 5235 sayılı Adli Yargı İlk Derece Mahkemeleri ile Bölge Adliye Mahkemelerinin Kuruluş, Görev ve Yetkileri Hakkında Kanun'un 11. ve 12. maddelerine göre asliye ceza mahkemeleridir. Suçun takibi şikayete bağlı değildir, resen soruşturulur.

2.3.1.10. Bilişim suçlarının işlenmesinde kullanılabilecek yasak cihaz ya da programları imal etme, bulundurma ve bunların alış veya satışını yapma suçu (m. 245/A)

2.3.1.10.1. Genel olarak

245/A maddesi, 24.03.2016 tarihli 6698 Sayılı Kişisel Verilerin Korunması Kanunu'nun 30. maddesiyle TCK'ya eklenmiştir. Türk Hukukunda ilk kez böyle bir hükme yer verilmiştir.[349] Madde başlığı "Yasak Cihaz veya Programlar"dır.[350] Bu suç tipi, 22.04.2014 tarihinde 6533 Sayılı Sanal Ortamda İşlenen Suçlar Sözleşmesinin Onaylanmasının Uygun Bulunduğuna Dair Kanun'la kabul edilen ASSS'nin cihazların kötüye kullanımı başlıklı 6. maddesindeki yükümlülükleri yerine getirmeye yönelik bir düzenlemedir. Sözleşmenin 6. maddesi, sözleşmenin 2 ila 5. maddeleri arasında yer verilen yasadışı erişim, yasadışı müdahale, verilere müdahale ve sisteme müdahale

[349]ASSS'nin 6. maddesindeki yükümlülüğün TCK'da karşılığının olmaması doktrinde eleştirilmekteydi. Bu eleştiriler için bkz. Özen ve Baştürk, 2011, a.g.k., 125-126.

[350]Doktrinde, Yasak Cihaz veya Programlar ifadesi eleştirilmektedir. Çünkü, sistematik olarak TCK'ya bakıldığında, suçların fiil unsuruna göre madde başlıkları belirlenmektedir. Fakat, burada, fiil unsuruna göre belirlenmemesi ve madde metninde yasak cihaz ya da program ifadesine yer verilmemesi madde içeriğiyle madde başlığının uyumsuz olması sonucunu doğurmuştur. Başlık olarak "suçta kullanılacak cihaz veya programların üretilmesi yayılması veya bulundurulması" kullanılsaydı madde içeriğiyle başlık daha uyumlu olurdu. Bkz. Özbek, Doğan, Bacaksız, Tepe, 2016, a.g.k., 998.

suçlarından herhangi birinin işlenmesi amacıyla bazı unsurların üretiminin, satışının, kullanım amaçlı tedarikinin, ithal edilmesinin, dağıtımının veya başka şekilde erişilebilir hale getirilmesinin suç olarak düzenlenmesini tavsiye etmektedir. Bazı unsurlardan kasıt ise, bir bilgisayar programı da dahil olmak üzere yukarıdaki suçların işlenmesi amacıyla tasarlanmış veya uyarlanmış cihazlar ile bir bilgisayar sistemine erişimi mümkün kılan bir bilgisayar şifresi, erişim kodu veya benzeri bir veridir. Sözleşmede ayrıca 2. ila 5. maddeler arasındaki suçların işlenmesi amacıyla yukarıda sayılan bazı unsurları bulundurmasının da suç olarak düzenlenmesi tavsiye edilmiştir.

Kanun koyucu bu suç tipini sözleşmenin 6. maddesine göre çok daha geniş bir şekilde düzenlemiştir. Sözleşmede sadece bilişim alanında suçların işlenmesi amacıyla 6. maddede sayılan fiillerin gerçekleştirilmesinden bahsetmektedir. Oysa TCK 245/A maddesinde sadece bilişim alanında suçlar bölümünde yer verilen suçlar için değil, ayrıca bilişim sistemlerinin araç olarak kullanılması suretiyle işlenen suçlar (örneğin TCK 142/2-e, 158/1-f) için de maddede sayılan fiillerin gerçekleştirilmesi suç olarak düzenlenmiştir. Suçu oluşturan fiiller de madde metninde tek tek sayılmıştır. Bu maddenin oldukça geniş bir şekilde düzenlenmiş olması teknolojinin sürekli gelişmesi ve bilişimin günlük hayatın neredeyse her alanına girmesi ve buna bağlı olarak da faillerin yeni suç işleme yöntemleri bulması dolayısıyla isabetli olmuştur. Bunun yanı sıra, bu suç tipindeki fiillerin diğer bilişim suçlarının işlenmesi için ön aşama ya da hazırlık evresi hareketleri olması sebebiyle suç olarak düzenlenmesi doğru bir tercih olmuştur.[351]

2.3.1.10.2. Korunan hukuki yarar

Bu suç, TCK'da bilişim alanında suçlar başlığı altında düzenlenen suçlar ile bilişim sistemlerinin araç olarak kullanılması suretiyle işlenen suçların işlenmesi amacıyla yasak cihaz, bilgisayar vb. unsurlarla ilgilidir. Bu unsurlar kullanılarak diğer suçlar işlenecektir. Kanun koyucu bu suçların işlenmesini önlemeye yönelik olarak bu düzenlemeyi yapmıştır. Dolayısıyla, bu suçla korunan hukuki yarar, bilişim suçlarıyla korunan hukuki yararın aynısıdır. [352] Yukarıda TCK'nın 243., 244. ve 245. maddesindeki düzenlemelere yönelik, korunan hukuki yarar başlığı altında yapılan

[351]Ayrıntılı bilgi için Özbek, Doğan, Bacaksız ve Tepe, 2016, a.g.k., 997.; Koca ve Üzülmez, 2016, a.g.k., 871.: S. Yılmaz (2016). *Türk Ceza Hukuku Sisteminde Siber Suçlar*. Ankara: Adalet Yayınevi, s. 376.
[352]Özbek, Doğan,Bacaksız ve Tepe, 2016, a.g.k., 998.

açıklamalar burada da geçerlidir. Bunların yanı sıra bilişim sistemleri araç olarak kullanılmak suretiyle işlenen hırsızlık ve dolandırıcılık suçlarının koruduğu hukuki yarar olan mülkiyet hakkı da 245/A maddesindeki suç tipi için geçerlidir.

2.3.1.10.3. Maddi unsur

2.3.1.10.3.1. Fiil

Suçun maddi unsurunu, bir cihazın, bilgisayar programının, şifrenin veya sair güvenlik kodunun bilişim suçlarını işlemek amacıyla yapılması veya oluşturulması durumunda, bunların imal edilmesi, ithal edilmesi, sevk edilmesi, nakledilmesi, depolanması, kabul edilmesi, satılması, satışa arz edilmesi, satın alınması, başkalarına verilmesi ya da bulundurulması hareketleri oluşturur. Suç, seçimlik hareketli bir suçtur. Madde metninde sayılan hareketlerden herhangi birinin gerçekleştirilmesi durumunda suç oluşacaktır. Failin birden fazla hareketi yapmış olması suçun tekliğini etkilemeyecektir.[353]

Suça örnek olarak, şifre kırıcı program, brute force attack, crack, keylogger, virüs, solucan yazılımları verilebilir.[354] Bu tarz program ve yazılımlar, bilgisayarlara veya cep telefonlarına yüklenmek suretiyle başkalarına ait olan sosyal medya hesaplarına, banka hesaplarına veya diğer kişisel hesaplara sahibinin rızası olmaksızın girmeyi sağlamaktadır. Hesaba giriş yapan fail buradaki verileri silmekte, erişilmez kılmakta, hesabın şifresini değiştirerek asıl hesap sahibinin sisteme girişine engel olmaktadır. İşte bu tarz işlemlerin yapılabilmesini sağlayan cihaz ve programların depo edilmesi, imal edilmesi, satılması gibi fiiller TCK 245/A maddesinde düzenlenen suçu oluşturur. Şifreli TV kanallarının şifrelerini çözmeye yarayan cihazlar da yine bu suçu oluşturmaktadır.[355]

Bir başka örnek olarak, ATM'lere yerleştirilen cihazlar verilebilir. Bu cihazlar sayesinde failler, müşterilerin banka veya kredi kartlarına ait bilgileri öğrenerek kart hamilinin rızası hilafına bunları kötüye kullanmaktadırlar. ATM'lere yerleştirilecek bu cihazların üretimi, satışı, ithali gibi fiiller de TCK 245/A maddesindeki suçu

[353]Koca ve Üzülmez, 2016, a.g.k., 873.; Yılmaz, 2016, a.g.k., 377-378.
[354]http://www.sertels.av.tr/avukat/hukuk/bilişim-hukuku/yeni-bilişim-suçları-zararli-yazilim-veri-izleme.html (Erişim Tarihi: 10/07/2017)
[355]Yılmaz, 2016, a.g.k., 378.

oluşturacaktır.[356]

2.3.1.10.3.2. Fail ve mağdur

Fail açısından herhangi bir özellik öngörülmemiştir. Dolayısıyla yasak cihaz veya programları imal eden, ithal eden, sevk eden, nakleden, depolayan, kabul eden, satan, satışa arz eden, satın alan, başkalarına veren ya da bulunduran herkes bu suçun faili olabilir.

Kanun koyucu mağdur açısından da herhangi bir özellik öngörmemiştir. Maddede sayılan fiiller, diğer bilişim suçlarının işlenmesi için araç suç niteliği taşımakta olduğundan suçun mağduru genel olarak toplumu oluşturan herkestir.[357]

2.3.1.10.3.3. Netice

Maddede sayılan fiillerin gerçekleşmesiyle suç oluşacaktır. Suçun oluşması için bir zararın meydana gelmiş olması şartı aranmamıştır. Suç, bir soyut tehlike suçudur.

2.3.1.10.4. Manevi unsur

Bu suç ancak kastla işlenebilir. Failde özel bir kastın olması gerekmez. Suçun oluşması için genel kast yeterlidir. Kanunda açıkça düzenlenmediği için suçun taksirli şekli cezalandırılmaz.

2.3.1.10.5. Hukuka aykırılık unsuru

Kanun koyucu 245/A maddesinde bu suç açısından herhangi bir hukuka uygunluk sebebi öngörmemiştir. Ancak, TBMM Alt Komisyonu'nun maddeye ilişkin raporuna göre, bu tür cihaz ve programların bilişim sistemlerinin güvenliğini test etmek amacıyla yapılması veya oluşturulması halinde belirtilen suç oluşmayacaktır. Buna göre, bilişim suçlarını işlemeye elverişli cihaz ve programlar bilişim sisteminin güvenliğini kontrol maksadıyla yapılmış veya oluşturulmuş ise fiil hukuka uygun hale gelecektir.[358]

2.3.1.10.6. Suçun özel görünüş şekilleri

2.3.1.10.6.1. Teşebbüs

Bilişim suçlarının işlenmesinde kullanılabilecek yasak cihaz ya da programları imal etme, bulundurma ve bunların alış veya satışını yapma suçuna teşebbüs

[356]A. Gül (2016). *Doğrudan, Dolaylı Bilişim Suçları*. Ankara: Seçkin Yayınevi, s. 208-209.
[357]Koca ve Üzülmez, 2016, a.g.k., 872.; Gül, 2016, a.g.k., 207.
[358]Gül, 2016, a.g.k., 206.

mümkündür. Yukarıda da belirttiğimiz gibi suç, neticesiz bir suç olduğu için fail tarafından elverişli vasıtalarla madde metninde sayılan seçimlik hareketlerin bir ya da birkaçının yapılmış olması suçun oluşumu için yeterlidir. Ayrıca, bir zarar meydana gelmiş olması gerekmez. Bu suç açısından icra hareketlerinin parçalara bölünebildiği durumlarda teşebbüs, failin elverişli vasıtalarla suçun icra hareketlerine başlaması fakat elinde olmayan sebeplerle icra hareketlerini tamamlayamaması halinde mümkündür.

2.3.1.10.6.2. İştirak

Yasak cihaz veya programların imali, bulundurulması, alış veya satışının yapılması suçu iştirak açısından bir özellik göstermez.

2.3.1.10.6.3. İçtima

Suçun zincirleme olarak işlenmesi mümkündür. Failin, aynı suç işleme kararının icrası kapsamında farklı zamanlarda madde metninde belirtilen seçimlik hareketlerin bir ya da birkaçını gerçekleştirmesi halinde zincirleme suç söz konusu olabilecektir. Suçun mağduru toplumu oluşturan herkes olduğundan, bu suçta ayrıca mağdurun kim olduğunun araştırılması gerekmez. Failin aynı suç işleme kararından bahsedilemeyecek kadar uzun aralıklarla ya da farklı suç işleme kastıyla seçimlik hareketleri yapması durumunda faile her fiil için ayrı ceza verilmelidir.

Yasak cihaz veya programların doğrudan veya dolaylı bir bilişim suçunun işlenmesi için kullanılması durumunda failin bu suçla birlikte işlediği diğer bilişim suçu her ne ise ondan da sorumluluğu doğacaktır. Örneğin, yasak cihaz veya programları imal eden fail ayrıca bunu bilişim sistemine hukuka aykırı olarak girmek için kullanmışsa, iki farklı suç oluşacağından gerçek içtima kuralı uygulanarak fail hem 245/A gereği hem de 243/1 gereği cezalandırılmalıdır.

2.3.1.10.7. Yaptırım, soruşturma ve kovuşturma

Türk Ceza Kanunu'nun 245/A maddesindeki suç için hem hapis cezası hem de para cezası öngörülmüştür. Hapis cezasının alt sınırı bir yıl, üst sınırı üç yıldır. Adli para cezasının miktarı ise genel hükümlere göre belirlenecektir.

Görevli mahkeme, 5235 sayılı Adli Yargı İlk Derece Mahkemeleri ile Bölge Adliye Mahkemelerinin Kuruluş, Görev ve Yetkileri Hakkında Kanun'un 11. ve 12.

maddelerine göre asliye ceza mahkemeleridir. Suçun takibi şikayete bağlı değildir, resen soruşturulur.

2.3.1.11. Tüzel kişiler hakkında uygulanacak güvenlik tedbirleri (m. 246)

Türk Ceza Kanunu'nun 246. maddesinde "bu bölümde yer alan suçların işlenmesi suretiyle yararına haksız menfaat sağlanan tüzel kişiler hakkında bunlara özgü güvenlik tedbirlerine hükmolunur" denilmektedir. Kanun koyucu bu maddede bilişim alanında suçlar başlığı altında düzenlenmiş suçlardan dolayı tüzel kişiler hakkında güvenlik tedbirlerine hükmedileceğini belirtmiştir.

Tüzel kişiler hakkında bunlara özgü olarak hükmedilecek güvenlik tedbirlerinin neler olduğu 246. maddede düzenlenmemiştir. Bu durumda, TCK'nın 60. maddesine göre uygulama yapılacaktır. TCK'nın 60. maddesine göre, tüzel kişi yararına işlenen kasıtlı suçlardan mahkumiyet halinde tüzel kişiler hakkında hükmedilebilecek güvenlik tedbirleri tüzel kişilerin faaliyet izinlerinin iptali ve müsaderedir.[359] Bu tedbirlere hükmedilebilmesi için 246. madde uyarınca, tüzel kişiler yararına haksız menfaat sağlanmış olması şartının gerçekleşmesi gerekmektedir.

2.3.2. Fikir ve Sanat Eserleri Kanunu'nda yer alan bilişim suçları

2.3.2.1. Genel olarak

Fikir ve sanat eserleri, bu eserlerin tüm insanlığa katkı sağlıyor olması, uygarlık tarihinde önemli bir yer edinmiş olması ve insan kimliğini en bariz şekilde temsil eden ürünler olması dolayısıyla korunması gerekmektedir.[360] Bunun yanı sıra, Anayasa'nın 27. maddesindeki Bilim ve Sanat Hürriyeti ile 64. maddesindeki Sanatın ve Sanatçının Korunması maddeleri ile uluslararası alandaki çeşitli düzenlemeler gereği fikir ve sanat eserleriyle birlikte bu eserlerin sahiplerinin hakları da koruma altına alınmalıdır.[361] 5 Aralık 1951 tarihinde kabul edilen 5846 sayılı Fikir ve Sanat Eserleri Kanunu bahsedilen eserleri ve sahiplerinin haklarını korumaya yönelik mevzuattaki en önemli kaynaktır. Nitekim, kanunun 1. fıkrasında, kanunun amacının mali ve manevi hakları belirlemek ve korumak olduğu açıkça belirtilmiştir.

Uluslararası hukukta, telif haklarının ihlaline ilişkin cezai hükümlere ilk kez

[359]Değirmenci, 2005, a.g.k., 207.
[360]Z. Hafizoğulları (1999). Fikir ve Sanat Eserlerinin Cezai Himayesi. *AÜHFD*, 48 (1), s. 1.
[361]R.Y. Yazıcıoğlu (2009). *Fikri Mülkiyet Hukukundan Kaynaklanan Suçlar*. İstanbul: XII Levha Yayıncılık, s. 160.

TRIPS sözleşmesinde yer verilmiş, bu sözleşmeyi WTO ve WIPO sözleşmeleri izlemiştir.[362] TRIPS sözleşmesinin amacı, fikir ve sanat eseri sahibinin haklarını uluslararası alanda korumak için alınacak önlemlerin, uluslararası ticarette engel teşkil etmemesini sağlamaktır. TRIPS, bugüne kadar uluslararası alanda yapılan en kapsamlı anlaşmadır. Daha sonra kabul edilen WTO sözleşmesi de fikri hakların uluslararası alanda korunmasına yöneliktir. WIPO sözleşmesinin amacı ise fikri hakların uluslararası alanda korunmasının yanı sıra, WIPO sözleşmesi gereği kurulan fikri mülkiyet birlikleri arasında koordinasyonu sağlamaktır.[363]

Bilişim suçları açısından değerlendirildiğinde, telif hakları ile bilişim teknolojisi alanındaki gelişmeler arasında önemli bir bağlantı vardır. Çünkü, günümüzde fikri hak ihlalleri önemli derecede internette meydana gelmektedir.[364] Özellikle, internet kullanılarak müzik, film, resim, bilgisayar programı vb. gibi fikir ve sanat eserlerinin bedelsiz ya da değerinin çok altında bir bedelle orijinaline yakın bir kaliteyle çoğaltılabilmesi ve dağıtılması mümkün olmakta, bu şekilde fikir ve sanat eseri sahibi büyük mağduriyetler yaşamaktadır. İnternet ortamında dosya transferinin hızlanması sahiplerinin izni olmaksızın fikir ve sanat eserlerinin kopyalanması ve dağıtılması, fikri hukuk alanında da oldukça büyük bir problem oluşturmakta[365], iletişim tekniklerinin ve internet ağının gelişmesiyle telif hakları alanındaki ihlaller artış göstermektedir.[366] Fakat, bu olumsuz etkilerinin yanı sıra, bilişim teknolojisi alanındaki gelişmeler eser sahibine, eserini her türlü hak ihlaline karşı korumasını sağlayacak yeni ve çok etkili kontrol mekanizmaları da sağlamaktadır. Dolayısıyla, bilişim suçları alanında yapılacak etkili hukuki ve idari düzenlemeler[367] sayesinde fikir ve sanat eserlerinin geliştirilmesi ve bu eserlerin sahiplerinin telif haklarının korunması sağlanmış olacaktır.[368]

Fikir ve Sanat Eserleri Kanunu her türlü eser için değil, sadece bu kanunda eser olarak kabul edilmiş olan fikri ürünler[369] için koruyucu önlemler almıştır.[370] Eser

[362]Sieber, 2014, a.g.k., 73.
[363]Bozbel, 2012, a.g.k., 9-18.; Uluslararası hukukta telif haklarının korunmasına ilişkin ayrıntılı bilgi için bkz. Topaloğlu, 2005, a.g.k., 135-139.
[364]Sieber, 2013, a.g.k., 30.
[365]Ayrıntılı bilgi için bkz. A.O. Özdilek (2002). *İnternet ve Hukuk*. İstanbul: Papatya Yayıncılık, s. 71-92.
[366]Telif haklarına yönelik ihlallerin neler olduğu ve karşılaşılma sıklığı ile ilgili sayısal veriler hakkında ayrıntılı bilgi için bkz. Sieber, 2014, a.g.k., 46-50.
[367]Ayrıntılı bilgi için bkz. R. Acun (2000). İnternet ve Telif hakları. *Bilgi Dünyası*, 1 (1), s. 22-23.
[368]Dülger, 2013, a.g.k., 631.
[369]Fikri ürün, insanın fikri emek ve çalışmalarıyla ortaya koyduğu neticelerdir. Ayrıntılı bilgi için bkz. S. Bozbel (2012). *Fikir ve Sanat Eserleri Hukuku*. İstanbul: On İki Levha Yayınları, s. 1.
[370]Yazıcıoğlu, 2009, a.g.k., 163

kavramı, FSEK'in 1/B-a maddesinde sahibinin hususiyetini taşıyan ve ilim ve edebiyat, musiki, güzel sanatlar veya sinema eserleri olarak sayılan her nevi fikir ve sanat mahsulü olarak tanımlanmıştır. Bu kanun kapsamında, bir fikir ve sanat ürününün eser olarak kabul edilebilmesi ve koruma altına alınabilmesi için 2 esaslı unsurun eserde var olması gerekir. Bunlardan ilki, fikir ve sanat ürününün sahibinin hususiyetini taşıması ikincisi ise kanunda belirtilen eser kategorilerinden birisine dahil olmasıdır. Bu unsurlar, kısaca, hususiyet ve aidiyet olarak belirtilebilir.[371] Görüldüğü üzere FSEK çerçevesinde eser kavramının ürün kavramına göre daha dar biçimde anlaşılması gerekir.[372]

FSEK'te yer verilen suçların, bilişim suçu olarak kabul edilmesindeki en önemli sebeplerden birisi olan bilgisayar programları da kanunun 2/1. maddesinde ilim ve edebiyat eserleri arasında sayılarak koruma altına alınmıştır. Kanun, bilgisayar programlarını, 1/B-g maddesinde "bir bilgisayar sisteminin özel bir işlem veya görev yapmasını sağlayacak bir şekilde düzene konulmuş bilgisayar emir dizgesi ve bu emir dizgesinin oluşum ve gelişimini sağlayan hazırlık çalışmaları" olarak tanımlanmıştır.

Bu kanun ile bilgisayarla işlenebilecek telif hakkı suçları ve diğer hukuka aykırı hareketler düzenlendiği gibi ayrıca, bilgisayar programları, web sayfaları dahil olmak üzere her türlü fikir ve sanat eserini izinsiz olarak kullanan, çoğaltan, işleyen, bilgisayar programlarını koruyan aygıtları geçersiz kılan teknik araçları bulunduran, dağıtan ve bu tip eser ve yayınları izinsiz olarak yayınlayanlar hakkında da yaptırım öngörülmüştür.[373]

Fikir ve sanat eserlerine yönelik mevzuattaki en önemli kaynak olan FSEK'te farklı tarihlerde çeşitli değişiklikler yapılmıştır. Bu çalışmanın konusu ile ilgisi açısından bahsedilebilecek ilk önemli değişiklik 07.06.1995 tarih ve 4110 sayılı yasayla FSEK'in 2. maddesindeki eser kavramının kapsamına bilgisayar programları kavramının dahil edilmesidir. Böylece, kanunun 71. ve 72. maddelerinde düzenlenmiş olan eser sahibinin haklarının korunmasına yönelik suçların kapsamına bilgisayar programları da girmiş olmaktadır.[374] İkinci değişiklik ise 23.01.2008 tarihinde 5728 sayılı yasa ile yapılmıştır. Bu yasayla, FSEK'in 71. 72. ve 73. maddelerinde yer verilen manevi

[371]Yazıcıoğlu, 2009, a.g.k., 57.
[372] Y. Kaplan (2004). *İnternet Ortamında Fikri Hakların Korunmasına Uygulanacak Hukuk.* Ankara: Seçkin Yayınevi, s. 73
[373]G. Öngören (2006). *İnternet Hukuku.* İstanbul: Öngören Hukuk Yayınları, s. 55.
[374]Dülger, 2013, a.g.k., 629.; Topaloğlu, 2005, a.g.k., 49-51.

haklara tecavüz, mali haklara tecavüz ve diğer suçlar, 71. maddede manevi, mali veya bağlantılı haklara tecavüz başlığı altında toplanmış, 72. maddede koruyucu programları etkisiz kılmaya yönelik hazırlık hareketleri başlıklı yeni bir suç tipi oluşturulmuş ve doktrinde eleştirilen[375] diğer suçlar başlıklı 73. madde ile fail başlıklı 74. maddeler ilga edilmiştir. Ayrıca, yine bu yasayla 75. maddenin başlığı kovuşturma ve tekerrür iken soruşturma ve kovuşturma şeklinde değiştirilmiştir. Bunun sonucunda FSEK'te yer alan suçlar köklü bir değişikliğe uğramıştır.[376]

Kanunda fikir ve sanat eserlerine yönelik suç olarak, 71/1-1. maddede eser sahibinin manevi mali ve bağlantılı haklarına ilişkin suçlar, 71/1-2. maddede başkasının eserini sahiplenmek suçu, 71/1-3. ve 71/5. maddede intihal suçları, 71/1-4. maddede eser içeriğini ifşa suçu, 71/1-6. maddede başkasının adından istifade suçu, 72. maddede koruyucu programları etkisiz kılmaya yönelik hazırlık hareketleri suçu düzenlenmiştir.[377] Görüldüğü üzere, kanunda sadece 2 maddede düzenlenmiş bulunan suçlar, aslında kendi içerisinde suçun konusu, suçla korunan hukuki değer ve hareket unsuru açısından bakıldığında 6 farklı suç tipine vücut vermektedir. Kanun koyucunun bu şekilde farklı suçları tek bir maddede toplaması yanlış bir yöntemdir. Çünkü, burada yer verilen suçların unsurları farklılık arz etmektedir. Nitekim, burada mağdur da manevi, mali ve bağlantılı hakları olmak üzere 3 farklı hakka sahiptir ve suçu oluşturan fiiller 3 farklı hakka yönelik olarak çeşitli yöntemlerle gerçekleştirilebilir.[378] Kanun koyucunun her ne kadar hatalı da olsa birbirinden farklı suçları sadece 2 maddede düzenlemiş olmasından dolayı suç tiplerini unsurları yönünden açıklarken özellikle 71. maddeyi tek bir başlık altında incelemek isabetli olacaktır.

2.3.2.2. Manevi, mali veya bağlantılı haklara tecavüz suçu (m. 71)

2.3.2.2.1. Genel olarak

5846 sayılı FSEK'in, Hukuk ve Ceza Davaları başlıklı beşinci bölümünde ceza davalarını düzenleyen B kısmının Manevi, Mali ve Bağlantılı Haklara Tecavüz başlıklı 71. maddesi manevi, mali ve bunlarla bağlantılı diğer hakları koruma altına almıştır. Manevi haklar esasen eser sahibine, eserinin özelliğine ve bütünlüğüne saygı

[375]Hafızoğulları, 1999, a.g.k., 4-5, 11.
[376]Yazıcıoğlu, 2009, a.g.k., 161-162.
[377]Yazıcıoğlu, 2009, a.g.k., 163-164.
[378]Ayrıntılı bilgi için bkz. Yazıcıoğlu, 2009, a.g.k., 167-169.

gösterilmesini talep etme hakkı verir.[379] Eser sahibinin manevi hakları, eseri topluma sunma hakkı (m.14), adın belirtilmesi hakkı (m.15), eserde değişiklik yapılmasını engelleme hakkı (m.16), eser sahibinin zilyet ve malike karşı hakları (m.17) dır. Manevi haklar, eser ile onu meydana getiren arasındaki ilişkiyi ifade eden ve gayrı maddi niteliği haiz olan, eser sahibinin doğrudan doğruya kişiliğine bağlı , devredilemeyen ölüme bağlı ya da sağlararası yapılacak hiçbir işleme konu olamayan ve herhangi bir süreyle de sınırlanmamış FSEK'de öngörülen haklardır. Ancak, bu haklar eser sahibinin ölümünden itibaren FSEK 19/2. maddesine göre 70 yıl süreyle mirasçıları tarafından kendi adlarına kullanılabilir.[380]

Eser sahibinin mali hakları, manevi haklarla birlikte eser sahibinin telif haklarını oluşturur. Mali haklar, eser sahibinin ortaya koymuş olduğu fikir ve sanat eseri üzerindeki her türlü ekonomik menfaatidir ve eser sahibi hukukun öngördüğü ölçüde bu haklardan dilediği gibi yararlanma yetkisine sahiptir. 3. kişiler ise sadece eser sahibinin rızası ölçüsünde bu haklardan yararlanabilirler. Manevi hakların aksine mali haklar, maddi bir nitelik taşıdığından dolayı devredilebilir, miras yoluyla mirasçılara geçebilir.[381] Eser sahibinin mali hakları, işleme hakkı (m.21), çoğaltma hakkı (m.22), yayma hakkı (m.23), temsil hakkı (m.24), İşaret, ses ve/veya görüntü nakline yarayan araçlarla umuma iletim hakkı (m.25) olmak üzere 5 tanedir. Bunların yanı sıra, eser sahibinin internet ortamında sahip olduğu mali haklarından bir diğeri ise eserini dijital olarak iletebilme hakkıdır. Dijital iletim hakkı, çoğaltma ve yayma hakkının bir görünümüdür. Eser sahibinin dijital iletim hakkına sahip olması eserini istediği şekilde çoğaltabilmesi ve internetin sınır ötesi karakterini de kullanarak geniş kitlelere eserini yayabilmesi anlamına gelir.[382]

Nihayet, eser sahibinin bağlantılı hakları ise FSEK'in 1/B-j maddesine göre, eser sahibinin manevi ve mali haklarına zarar vermemek kaydıyla, komşu hak[383] sahipleri ile

[379]Acun, 2000, a.g.k., 8.
[380]Yazıcıoğlu, 2009, a.g.k., 178-182; Bozbel, 2012, a.g.k., 152-153.
[381]Yazıcıoğlu, 2009, a.g.k., 297-299; Bozbel, 2012, a.g.k., 98.
[382]Özdilek, 2002, a.g.k., 70-71.
[383] Komşu Hak, Eser Sahibinin Haklarına Komşu Haklar Yönetmeliği'nin 4/a maddesine göre, eser sahibinin haklarına zarar vermeden ve onun rızası ile bir eseri özgün biçimde icra eden veya icrasına katılan bir icrayı ya da sesleri ilk defa tespit eden, yayınlayan gerçek ve tüzel kişilerin münhasıran sahip oldukları icrayı tespit etme, çoğaltma, kiralama, telli-telsiz her türlü araçla yayınlama ve kamuya açık yerlerde temsil suretiyle bundan yararlanma hakkıdır.

filmlerin ilk tespitini gerçekleştiren film yapımcılarının sahip oldukları haklardır. Bağlantılı haklar kavramıyla, bir fikir veya sanat eserinin halka ulaşmasında çeşitli şekillerde katkısı bulunan kişilerin sahip olduğu haklar kastedilmektedir. Bağlantılı hak sahibi olan kimseler, esasen bir eser sahibi olmayıp mevcut bir eserin toplum nezdinde tanınmasına yaygınlaşmasına popülerlik kazanmasına daha geniş kitlelere hitap etmesine imkan sağlayan kişilerdir.[384] Bağlantılı haklara yönelik gerçekleşecek ihlal hareketleri, esasen bağlantılı hak sahiplerinin mali haklarını zedelediğinden ötürü, mali haklara yönelik ihlal hareketlerinin başka bir şeklini oluşturmaktadır. Dolayısıyla, mali haklara tecavüz suçları için yapılmış olan açıklamalar burada da aynen geçerlidir. Ancak, diğer bağlantılı hak sahiplerinden farklı olarak FSEK'in 80. maddesinde, icracı sanatçılara[385] ayrıca icra sahibi olarak tanıtılma, icralarının kendi şeref ve itibarlarını zedeleyecek şekilde bozulması ve tahrif edilmesini önleme hakkı tanınmıştır.[386]

5728 sayılı Kanun'la değişiklik yapılmadan önce 71. maddede düzenlenmiş bulunan suç tipi, kanunun 71. maddesindeki manevi haklara tecavüz suçu, 72. maddesindeki mali haklara tecavüz suçu, 80. maddede düzenlenen bağlantılı haklara tecavüz suçu, ek 4/4. maddede düzenlenen eserin kimlik bilgilerinin yanlış verilmesi ile bilgi içerik sağlayıcıların eser sahiplerinin haklarını ihlal suçu şeklinde 4 farklı maddede düzenlenmekteydi. Fakat, yapılan bu değişiklik neticesinde mevcut 71. madde artık bir torba madde haline getirilmiş ve bahsedilen suç tipleri bu maddede bir araya getirilmiştir. Bunun yanı sıra, kanun koyucu 71. maddede suçla daha etkin mücadele edebilmek adına maddenin son kısmında bu hüküm bakımından özel bir etkin pişmanlık öngörmüştür. [387] Bu düzenlemeye göre, hukuka aykırı olarak üretilmiş, işlenmiş, çoğaltılmış, dağıtılmış veya yayımlanmış bir eseri, icrayı, fonogramı[388] veya yapımı satışa arz eden, satan veya satın alan kişi, kovuşturma evresinden önce bunları kimden temin ettiğini bildirerek yakalanmalarını sağladığı takdirde, hakkında verilecek cezadan indirim yapılabileceği gibi ceza vermekten de vazgeçilebilir.

[384]Yazıcıoğlu, 2009, a.g.k., 363-364; Bozbel, 2012, a.g.k., 377.
[385]İcracı Sanatçı, Eser Sahibinin Haklarına Komşu Haklar Yönetmeliği'nin 4/b maddesine göre, sanat eserleri ile folklor eserlerini özgün biçimde yorumlayan tanıtan anlatan söyleyen çalan ve çeşitli biçimlerde icra eden oyuncular ses sanatçıları müzisyenler dansçılar vb. diğer kişilerdir.
[386]Yazıcıoğlu, 2009, a.g.k., 367.
[387]Yazıcıoğlu, 2009, a.g.k., 176.
[388]Fonogram FSEK'in 1/B-f maddesine göre, sinema eseri gibi görsel-işitsel eserler içindeki ses tespitleri hariç olmak üzere bir icrada yer alan seslerin veya diğer seslerin veya ses temsillerinin tespit edildiği ses taşıyıcısı fiziki ortamdır.

2.3.2.2.2. Korunan hukuki yarar

71. maddedeki suç tipini koruduğu hukuki yarar açısından incelerken, mali, manevi ve bağlantılı haklara yönelik gerçekleşecek ihlal fiillerine göre ayrı ayrı değerlendirmek gerekmektedir. Çünkü, bu haklara yönelik suçlar mağdurun birbirinden farklı hukuki menfaatlerini zedeleyecektir.

Fikir ve sanat eseri sahibinin manevi haklarına yönelik tecavüz suçlarında korunan hukuki yarar, eser sahibinin eseri yaratarak duymuş olduğu hazzın, yaratmasının neticesi olarak hissettiği sahiplenme olgusunun ve manevi duygularının ihlal edilmemesi hakkıdır. Çünkü, eser sahibi, bir eser yaratma yeteneği ve insanlığa sunduğu katkısı sonucunda, toplumdan hem bir saygı hem de takdir edilme olgusu beklemektedir. Bu beklenti, eser sahibi için bir motivasyon unsuru oluşturur.[389]

Eser sahibinin mali haklarına yönelik tecavüz suçlarında korunan hukuki yarar, manevi haklardakinin aksine, eserin ekonomik getirisi ile ilgilidir. Fikir ve sanat eseri sahibi her ne kadar eserini estetik kaygıyla ve duygusal anlamda tatmin olmak için insanlığa katkı amacıyla meydana getirse de eserin ekonomik anlamda bir getirisi olacaktır. Hatta, çoğu zaman eser sahibi geçimini eserinden elde ettiği bu ekonomik getiri sayesinde sürdürebilmektedir. Bundan dolayı, hem eser sahibinin hem de eserinin mali anlamda da korunması sayesinde yeni eserler üretilmesi sağlanarak insanlığın ilerlemesine katkı sunulacaktır. FSEK'in 71/1-1. maddesinde düzenlenmiş bulunan mali haklara tecavüz suçuyla korunan hukuki yarar da eser sahibinin yarattığı eser sonucu elde edeceği ekonomik ve ticari haklarıdır. Eser sahibinin mali hakları, onun malvarlığı ile doğrudan ilişkili olduğu için bu suç tipiyle korunan hukuki yararın, eser sahibinin malvarlığı olduğu, hatta ekonomik düzenin dahi korunmaya çalışıldığı söylenebilir.[390]

Bağlantılı haklara yönelik tecavüz suçlarıyla korunan hukuki yarar ise bağlantılı hak sahibinin hakları, eser sahibinin mali haklarının başka bir şeklini oluşturmasından dolayı, mali haklara yönelik tecavüz suçlarında korunan hukuki değerin aynısıdır. Ancak, icracı sanatçılar için bahsedilen hukuki yararların yanı sıra, icra sahibi olarak tanıtılma ve icralarının kendi şeref ve itibarlarını zedeleyecek şekilde bozulması ve

[389]Yazıcıoğlu, 2009, a.g.k., 185-186.
[390]S. Bayındır (2014). Eser Sahibinin İzni Olmaksızın Eseri Umuma İletim Suçu. *TBB Dergisi*, (113), s. 307-338.; Yazıcıoğlu, 2009, a.g.k., 308-309.

tahrif edilmesini önlemek hakkı da korunan hukuki yararlardandır.[391]

2.3.2.2.3. Maddi unsur

2.3.2.2.3.1. Fiil

71. maddede yukarıda da belirtildiği üzere birden fazla suç tipi düzenlenmiştir. Madde metni incelendiğinde, her bir fıkrada aslında farklı bir suça yer verildiği ve bu suçların maddi unsurunu oluşturan hareket unsurlarının da çeşitlilik gösterdiği görülmektedir. Dolayısıyla, bu maddede yer verilen suç tiplerini maddi unsur açısından müstakil olarak incelemek daha doğru olacaktır.

71. maddenin birinci fıkrası açısından suçun maddi unsurunu oluşturan hareketler, izinsiz olarak bir eseri, icrayı, fonogramı veya yapımı işlemek, temsil etmek, çoğaltmak, değiştirmek, dağıtmak, her türlü işaret, ses veya görüntü nakline yarayan araçlarla umuma iletmek, yayımlamak ya da hukuka aykırı olarak işlemek veya çoğaltılan eserleri satışa arz etmek, satmak, kiralamak veya ödünç vermek suretiyle ya da sair şekilde yaymak, ticarî amaçla satın almak, ithal veya ihraç etmek, kişisel kullanım amacı dışında elinde bulundurmak ve depolamak fiilleridir. Suç, seçimlik hareketli bir suçtur ve sadece icrai hareketlerle işlenebilir.[392] Madde metninde sayılan fiillerden herhangi birinin gerçekleştirilmesiyle suç tamamlanmış olacaktır. Birden fazla fiilin işlenmesi durumunda da tek bir suç oluşacaktır. Yukarıda sayılan seçimlik hareketlerle yasanın 22, 23, 24 ve 25. maddelerinde düzenlenen eser sahibinin çoğaltma, yayma, temsil ve umuma iletim hakları koruma altına alınmıştır.[393]

71. maddenin 2. fıkrasında düzenlenen suçun maddi unsurunu, başkasına ait esere kendi eseri olarak ad koymak fiili oluşturur. Bu suç tipinde, fail, eser sahibinin fikri çabası sonucu ortaya koymuş olduğu eseri sanki kendi eseriymiş gibi sahiplenmektedir.[394] Yine bu fıkrada, fiilin dağıtmak veya yayımlamak suretiyle işlenmesi hali nitelikli hal olarak öngörülmüştür. Bu suçlar, başkasının eserini kendi eseriymiş gibi göstermenin yanı sıra 15. maddenin 2. fıkrasında düzenlenen hükme aykırı hareket ederek de işlenebilir.[395] 71/2. maddede, ad koyma suçunun ne şekilde

[391]Yazıcıoğlu, 2009, a.g.k., 368.
[392]Yazıcıoğlu, 2009, a.g.k., 203.
[393]Pallı, 2008, a.g.k., 226.
[394]Yazıcıoğlu, 2009, a.g.k., 245.
[395]Pallı, 2008, a.g.k., 228.

olacağı belirtilmediğinden suç, serbest hareketli bir suçtur.[396] Yani hukuka aykırı olan herhangi bir fiille bu suç işlenebilir. Ancak, burada öngörülmüş olan nitelikli halin gerçekleşebilmesi için suçun dağıtmak veya yayımlamak suretiyle işlenmiş olması gerekmektedir.[397]

71. maddenin 3. fıkrasında düzenlenen suçun maddi unsurunu bir eserden kaynak göstermeksizin iktibasta bulunmak fiili oluşturur. Diğer bir ifadeyle, eser sahibinin üretmiş olduğu fikir ve sanat eserinin bazı kısımlarının bir başka kişi tarafından sahiplenilmesi durumunda bu suç oluşacaktır. Eserin bazı kısımları değil de tamamı eser sahibi dışındaki biri tarafından sahiplenilecek olursa artık bu fıkradaki değil, 2. fıkradaki başkasına ait esere kendi eseri olarak ad koyma suçu oluşacaktır.[398] Kanunda suçun ne şekilde işlenebileceği belirtilmediğinden suç, serbest hareketli bir suçtur. FSEK'te düzenlenmiş olan 71/1-2, 71/1-3 ve 71/1-5 maddeleri genellikle intihal suçu[399] olarak bilinen suçları oluşturan fiilleri yaptırıma bağlamaktadır. İktibasın nasıl yapılması gerektiği FSEK'in 31. ve devamı maddelerinde ayrıntılı olarak belirtilmiştir. Bunlara aykırı olarak yapılacak iktibaslar suç oluşturacaktır. İktibas yaparken kaynak göstermemek, yanlış kaynak göstermek, kifayetsiz ya da aldatıcı kaynak göstermek suretiyle bu suçlar işlenebilir.[400] Kanun koyucunun intihal suçlarını 3 farklı suç tipiyle düzenlemiş olmasının sebebi, eserin usulsüz olarak tamamen iktibas edilmesinin yanı sıra bir kısmının iktibas edilmesini de yasaklayarak fikir ve sanat eseri sahibinin haklarını etkin olarak koruma isteğidir.

71. maddenin 4. fıkrasında düzenlenen suçun maddi unsurunu, hak sahibi kişilerin izni olmaksızın, alenileşmemiş bir eserin muhtevası hakkında kamuya açıklamada bulunmak fiili oluşturur. Eseri kamuya sunma hakkı, eserin varlığı ve içeriği ile ilgili kamuya bilgi vermek, eseri tanıtmak ve topluma sunmak yani kısacası, eseri alenileştirmek hakkı eser sahibine ait mutlak haklardandır.[401] Bu hakka yönelik gerçekleştirilecek ihlal fiilleri 71/4. maddede düzenlenen suçu oluşturacaktır. Kanunda

[396]Suçun bağlı hareketli olduğuna dair görüş için bkz. L.Yavuz, T.Alıca ve F. Merdivan (2013). *Fikir ve Sanat Eserleri Kanunu Yorumu Cilt -II- (48-91. maddeler).* Ankara: Seçkin Yayınevi, s. 2197.
[397]Yazıcıoğlu, 2009, a.g.k., 246.
[398]D. Yaman (2010). Fikir ve Sanat Eserleri Kanununda Düzenlenen Bir Eserden Kaynak Göstermeksizin İktibasta Bulunma Suçu (m. 71/1-III). *DEÜHFD,* 12 (Özel Sayı), s. 1561.
[399]İntihal: bir kişinin eserinde başka kişilerin ifade, buluş veya düşüncelerini kaynak göstermeksizin kendisine aitmiş gibi kullanması. İntihal, bir sahtekârlık veya hırsızlık türüdür. İntihal ile ilgili ayrıntılı bilgi için bkz. Yaman, 2010, a.g.k., 1556-1558; Ayrıca bkz. Bozbel, 2012, a.g.k., 165-166.
[400]Pallı, 2008, a.g.k., 228; ayrıca bkz. Hafızoğulları, 1999, a.g.k., 6-8.
[401]Yazıcıoğlu, 2009, a.g.k., 219.

suçun ne şekilde işlenebileceği açıkça belirtilmediğinden dolayı suç, serbest hareketli bir suçtur ve icrai hareketlerle işlenebilir.

71. maddenin 5. fıkrasında düzenlenen suçun maddi unsurunu, bir eserle ilgili olarak yetersiz, yanlış veya aldatıcı mahiyette kaynak göstermek fiili oluşturur. Yukarıda da belirtildiği gibi, bu suç, bir intihal suçudur. FSEK'in 31. ve devamı maddelerinde düzenlenmiş olan yöntemler dışında yapılan usulsüz iktibaslar bu suçu oluşturacaktır. Suç, serbest hareketli bir suçtur ve icrai hareketlerle gerçekleştirilebilir.

71. maddenin 6. fıkrasında düzenlenen suçun maddi unsurunu, bir eseri, icrayı, fonogramı veya yapımı, tanınmış bir başkasının adını kullanarak çoğaltmak, dağıtmak, yaymak veya yayımlamak fiilleri oluşturur. Fail, bu fiilleri neticesinde başka bir kişinin adından ve namından yararlanarak aslında hak etmediği bir değer sahibi olmakta ya da adını ve namını kullandığı kişinin şöhretini lekelemektedir.[402] Aslında, bu suç tipinde fikri haklara yönelik bir ihlal değil, ünlü şahsiyetlerin kişiliğine yapılan bir saldırı söz konusu olmaktadır. [403] Suç seçimlik hareketli bir suçtur ve icrai hareketlerle gerçekleştirilebilir.

2.3.2.2.3.2. Fail ve mağdur

FSEK'in 71. maddesinde düzenlenen suçlarda fail için herhangi bir özellik aranmamıştır. Kanun koyucu bu suçlarda herhangi bir kişiden bahsetmeyip, suç failinin kimler olabileceğine yönelik de hiçbir kısıtlama getirmemiştir. Dolayısıyla, bu suçun faili herkes olabilir.[404]

Eser sahibi bizzat bu suçun faili olamaz. Ancak, herhangi bir eserin sahibi bir başka esere yönelik manevi, mali ya da bağlantılı haklara tecavüz edecek olursa, elbette bu kişi suçun faili olabilecektir.[405]

FSEK'in fail başlığını taşıyan 74. maddesi, manevi, mali ve bağlantılı suçlara yönelik suçlara iştirak edenlerin kanunda belirtilen durumlar gerçekleştiğinde fail ya da yardım eden gibi cezalandırılacağını, bu suçların işlenmesinde tüzel kişilerin masraf ve para cezasından diğer suçlularla birlikte müteselsilen sorumlu olacağını düzenlemekteydi. Fakat, bu hüküm 23.01.2008 tarih ve 5728 sayılı yasa ile yürürlükten

[402]Dülger, 2013, a.g.k., 639.
[403]Bozbel, 2012, a.g.k., 588.
[404]Yazıcıoğlu, 2009, a.g.k., 187-188.; Yavuz, Alıca ve Merdivan, 2013, a.g.k., 2184.
[405]Yazıcıoğlu, 2009, a.g.k., 188.

kaldırılmıştır.

Manevi ve mali haklara tecavüz suçlarında mağdur, özellik gösterir, çünkü, bu suçun mağduru herkes değil ancak belirli kişiler olabilir. 71. maddede suçun mağdurunun hak sahibi olduğu açıkça belirtilmiştir. Fikir ve sanat eseri üzerinde hak sahibi kanunun 19. maddesinde belirtildiği üzere eser sahibidir. Eser sahibi de 8. maddeye göre eseri meydana getiren kişidir. Buradan da anlaşılacağı üzere bu suçlarda mağdur sadece gerçek kişiler olabilir. Tüzel kişilerin suçun mağduru olması mümkün değildir. Tüzel kişilerin eser sahibi sayıldığı durumlarda ise eser sahibi olan tüzel kişiler, suçtan zarar gören sıfatını kazanırlar.[406]

Bağlantılı haklara tecavüz suçlarında mağdur, herhangi bir kimse değildir. 71. maddede bağlantılı haklara tecavüz suçlarının mağdurunun, bağlantılı hak sahibi kişiler olduğu belirtilmiştir. Bağlantılı hak sahibi kişiler ise 80. maddeye göre, icracı sanatçılar, bir icra ürünü olan veya sair sesleri ilk defa tespit eden fonogram yapımcıları, radyo ve televizyon kuruluşları ve filmlerin ilk tespitini gerçekleştiren film yapımcılarıdır.[407]

2.3.2.2.3.3. Netice

FSEK'in 71. maddesinde düzenlenmiş olan suç tiplerinin tamamı tehlike suçudur. Kanun koyucu suçun oluşması için bir zararın meydana gelmiş olması şartını aramamıştır. Madde metninde düzenlenmiş maddi unsuru oluşturan fiillerin gerçekleştirilmesi durumunda suç oluşacaktır. Dolayısıyla, manevi, mali ve bağlantılı haklara yönelik tecavüz suçları tehlike suçlarındandır.[408]

2.3.2.2.4. Manevi unsur

FSEK'in 71. maddesinde düzenlenmiş olan suçlar ancak kasten işlenebilir. Failde hukuka aykırı olarak işlenen özel kast aranmamıştır.[409] Failin fiilini gerçekleştirirken, 71. maddede öngörülmüş fiilleri bilerek ve isteyerek işlemiş olması şeklindeki genel kastı suçun oluşumu için yeterlidir. Kanun koyucu suçun taksirli halini açıkça

[406]Yazıcıoğlu, 2009, a.g.k., 190-193, 313-316.; Bayındır, 2014, a.g.k., 319.; Yavuz, Alıca ve Merdivan, 2013, a.g.k., 2184-2185.
[407]Yazıcıoğlu, 2009, a.g.k., 372.
[408]Dülger, 2013, a.g.k., 643-644.
[409]Yavuz, Alıca ve Merdivan'a göre, hukuka aykırı olarak işlenmiş veya çoğaltılmış eserleri ticari amaçla satın almak, kişisel kullanım amacı dışında elinde bulundurmak ya da depolamak suçları yönünden failde özel kast aranır. bkz. Yavuz, Alıca ve Merdivan, 2013, a.g.k., 2180.

düzenlemediğinden dolayı bu suçların taksirle işlenmesi mümkün değildir.[410]

2.3.2.2.5. Hukuka aykırılık unsuru

Manevi, mali ve bağlantılı haklara tecavüz suçlarında mağdurun rızası, bir hukuka uygunluk sebebi olarak kabul edilmiştir. Rızanın varlığı halinde hukuka aykırılık ortadan kalkacağı için 71. maddede düzenlenmiş suçlar oluşmayacaktır. Fakat, kanun koyucu FSEK'in 71. maddesinin sadece 1. fıkrasındaki suç tipi açısından fiili hukuka uygun hale getiren rızanın yazılı olması şartını aramıştır. Bu maddede yer verilen diğer suçlar için ise rızanın, yazılı olmasının yanı sıra, sözlü olması ya da imzalı olmayan bir yazı ile verilmiş olması durumunda hukuka aykırılık ortadan kalkacaktır.[411]

Yazılı izin, hak sahibinin rıza göstereceği kişiye, kendisinden elde edilmiş ıslak imzalı bir belge vermesi anlamına gelir. Yazılı izin, hukuka uygunluk bakımından önemli bir şekil şartıdır. Doktrinde, böyle bir şekil şartı aranması isabetli görülmekte, aksi halde "şüpheden sanık yararlanır (in dubio pro reo)" kuralı gereğince hak sahibinin izin vermediğini ispatlamak zorunda kalacağı belirtilmektedir.[412]

FSEK'in 52. maddesinde mali haklara dair sözleşme ve tasarrufların yazılılık şartına uygun olması ve konuları olacak hakların ayrı ayrı gösterilmesi gerektiği belirtilmiştir. Buna göre, 71. maddenin 1. fıkrasında suç olarak belirtilen fiiller açısından verilen yazılı rızanın fiilleri hukuka uygun hale getirebilmesi için, yazılı rızanın hangi tür fiillere ya da hangi haklara yönelik olduğu açıkça belirtilmelidir.[413]

Yazılı iznin, suç teşkil eden fiillerin işlenmesinden önce ya da fiilin işlendiği esnada hak sahibince verilmiş olması gerekmektedir. Suç oluştuktan sonra verilen rıza (icazet) fiili hukuka uygun hale getirmez. Ancak, böyle bir durumda gösterilen rıza suçun oluşumuna engel olmasa da kanunun 75. maddesine göre bu suçların soruşturma ve kovuşturması şikayete bağlı olduğu için şikayet hakkından feragat anlamına gelecektir ve fail fiilinden dolayı sorumlu tutulamayacaktır.[414]

71. maddede düzenlenmiş suçlar açısından genel bir hukuka uygunluk nedeni olan yazılı iznin yanı sıra, bu maddede düzenlenmiş bazı suçlar için kanun koyucu başka

[410]Pallı, 2008, a.g.k., 229-230.
[411]Dülger, 2013, a.g.k., 644.
[412]Yazıcıoğlu, 2009, a.g.k., 355.; Yavuz, Alıca ve Merdivan, 2013, a.g.k., 2182-2183.
[413]Yazıcıoğlu, 2009, a.g.k., 355-356.
[414]Yazıcıoğlu, 2009, a.g.k., 356.

birtakım hukuka uygunluk sebepleri öngörmüştür. Örneğin, eser sahibinin izni olmaksızın eseri umuma iletim suçu açısından, FSEK'in 32., 33., 34., 35. maddelerinde yer verilen genel menfaat düşüncesi, eğitim öğretim amaçlı fiiller, eğitim öğretim amaçlı olarak seçme ve toplama eserlerin meydana getirilmesi ve eser sahibinin ismi belirtilmek suretiyle gerçekleştirilen fiiller hukuka uygun olarak kabul edilebilir.[415] Ayrıca, maddenin 2. fıkrasındaki başkasına ait esere kendi eseri olarak ad koymak suçu, 3. fıkrasındaki bir eserden kaynak göstermeksizin iktibasta bulunmak suçu, 5. fıkrasındaki bir eserle ilgili olarak yetersiz, yanlış veya aldatıcı mahiyette kaynak göstermek suçu açısından, FSEK'in 35. ve 36. maddelerine uygun olarak yapılacak iktibaslar hukuka uygunluk sebebi olarak kabul edilecektir. Burada kanun koyucu kendi deyimiyle, kişilere iktibas serbestisi sağlamış ve bu maddelere uygun olarak yapılan iktibasların intihal suçunu oluşturmayacağını belirtmiştir.[416]

Bilgisayar programları için kanundan kaynaklanan başka bir hukuka uygunluk sebebi daha vardır. FSEK'in 38. maddesinin 2. fıkrasına göre hukuka uygun yollardan elde edilmiş olması koşulunu sağlayan kişi tarafından, bilgisayar programının hata düzeltme de dahil olmak üzere çoğaltılması ve işlenmesi serbesttir. Fakat, yine aynı maddeye göre, bilgisayar programının düşünüldüğü amaca uygun kullanımı için gerekli olduğu durumda bahsedilen fiiller hukuka uygun olacaktır.

2.3.2.2.6. Suçun özel görünüş şekilleri

2.3.2.2.6.1. Teşebbüs

Manevi, mali veya bağlantılı haklara tecavüz suçuna teşebbüs mümkündür**.** Yukarıda da belirttiğimiz gibi suç, neticesiz bir suç olduğu için fail tarafından elverişli vasıtalarla icra hareketlerinin yapılmış olması suçun oluşumu için yeterlidir. Ayrıca, bir zarar meydana gelmiş olması gerekmez. Bu suç açısından icra hareketlerinin parçalara bölünebildiği durumlarda, teşebbüs failin, elverişli vasıtalarla suçun icra hareketlerine başlanması fakat elinde olmayan sebeplerle icra hareketlerini tamamlayamaması halinde mümkündür. Failin elinde olmayan sebeplerle elektrik kesilmesi ya da eseri çoğaltmak için baskı yapıldığı esnada zabıta tarafından kopyalama araçlarına el konulması suça

[415]Bayındır, 2014, a.g.k., 327.
[416]Yaman, 2010, a.g.k., 1557-1558.

teşebbüse örnek olarak verilebilir.[417] Yine, failin internet ortamında bir bilgisayar programını hukuka aykırı olarak kişisel bilgisayarına indirmek suretiyle çoğaltırken internet bağlantısında bir arıza meydana gelmesi halinde suç teşebbüs aşamasında kalmış olacaktır.[418]

2.3.2.2.6.2. İştirak

Manevi, mali veya bağlantılı haklara tecavüz suçu iştirak açısından bir özellik göstermez.

2.3.2.2.6.3. İçtima

Manevi mali veya bağlantılı haklara tecavüz suçu zincirleme şekilde işlenebilir. failin aynı suç işleme kararının icrası kapsamında farklı zamanlarda aynı mağdura karşı 71. maddedeki suçu işlemesi halinde zincirleme suç hükümleri uygulanacaktır. Ancak, örneğin, aynı suç işleme kararından bahsedilemeyecek kadar uzun aralıklarla yazılımların çoğaltılması halinde faiel, her fiili için ayrı ceza verilmelidir.[419]

2.3.2.2.7. Yaptırım, soruşturma ve kovuşturma

Kanun koyucu, FSEK'in *71. maddesinin 1. fıkrasındaki* suç tipi için seçimlik ceza öngörmüştür. Buna göre, hapis cezasına hükmedilmesi durumunda cezanın alt sınırı bir yıl, üst sınırı ise beş yıldır. Aynı şekilde adli para cezasının da alt sınırı bir yıl, üst sınırı ise beş yıl olacaktır. Hapis ya da adli para cezasına hükmedilmesi hakimin takdirindedir.

71. maddenin 2. fıkrasında düzenlenen başkasına ait esere kendi eseri gibi ad koyma suçunda da seçimlik ceza öngörülmüştür. Hapis cezasına hükmedilmesi durumunda cezanın alt sınırı altı ay, üst sınırı ise iki yıldır. Aynı şekilde adli para cezasının da alt sınırı altı ay, üst sınırı ise iki yıl olacaktır. Hapis ya da adli para cezasına hükmedilmesi hakimin takdirindedir. Bu fıkranın ikinci cümlesinde fiilin dağıtmak veya yayımlamak suretiyle işlenmesi şeklinde düzenlenmiş nitelikli hal için hapis cezasının üst sınırı beş yıl olarak düzenlenmiştir. Ayrıca, bu durumda artık adli para cezasına hükmedilemeyecektir.

71. maddesinin 3. fıkrasında düzenlenen bir eserden kaynak göstermeksizin iktibasta bulunmak suçunda da seçimlik ceza öngörülmüştür. Hapis cezasına

[417]Yazıcıoğlu, 2009,a.g.k., 212.
[418]Yavuz, Alıca ve Merdivan, 2013, a.g.k., 2187-2188.
[419]Dülger, 2013, a.g.k., 647.

hükmedilmesi durumunda cezanın alt sınırı altı ay, üst sınırı ise iki yıldır. Aynı şekilde adli para cezasının da alt sınırı altı ay, üst sınırı ise iki yıl olacaktır. Hapis ya da adli para cezasına hükmedilmesi hakimin takdirindedir.

71. maddenin 4. fıkrasında düzenlenen bir eserin içeriği hakkında kamuya açıklamada bulunma suçunun alt sınırı burada açıkça düzenlenmemiştir. Dolayısıyla, hapis cezasının alt sınırı genel hükümlere göre belirlenecektir. Üst sınır ise altı ay olarak düzenlenmiştir. Kanun koyucu bu suç tipinde adli para cezası öngörmemiştir.

71. maddenin 5. fıkrasında düzenlenen bir eserle ilgili olarak yetersiz, yanlış veya aldatıcı mahiyette kaynak göstermek suçunun da bir üst fıkradaki suç tipinde olduğu gibi alt sınırı burada açıkça düzenlenmemiştir. Dolayısıyla, hapis cezasının alt sınırı genel hükümlere göre belirlenecektir. Üst sınır ise altı ay olarak düzenlenmiştir. Kanun koyucu bu suç tipinde adli para cezası öngörmemiştir.

71. maddenin 6. fıkrasında düzenlenen bir fikir veya sanat eserini tanınmış bir başkasının adını kullanarak çoğaltmak, dağıtmak, yaymak veya yayımlamak suçunda da seçimlik ceza öngörülmüştür. Hapis cezasına hükmedilmesi durumunda cezanın alt sınırı üç ay, üst sınırı ise bir yıldır. Aynı şekilde adli para cezasının da alt sınırı üç ay, üst sınırı ise bir yıl olacaktır. Hapis ya da adli para cezasına hükmedilmesi hakimin takdirindedir.

Nihayet, *71. maddenin son kısmında* düzenlenen suç için hapis cezası öngörülmüştür. Hapis cezasının alt sınırı üç ay, üst sınırı ise iki yıldır. Kanun koyucu bu suç tipinde adli para cezası öngörmemiştir. Faile, bu suçtan dolayı ceza verilebilmesi için fiilinin daha ağır cezayı gerektiren başka bir suçu oluşturmaması gerekir.

Ayrıca, 71. maddenin son kısmında etkin pişmanlık hükmüne yer verilmiştir. Bu hükme göre, hukuka aykırı olarak üretilmiş, işlenmiş, çoğaltılmış, dağıtılmış veya yayımlanmış bir eseri, icrayı, fonogramı veya yapımı satışa arz eden, satan veya satın alan kişi, kovuşturma evresinden önce bunları kimden temin ettiğini bildirerek yakalanmalarını sağlarsa, hakkında verilecek cezadan indirim yapılabileceği gibi ceza vermekten de vazgeçilebilecektir.

FSEK'in 75. maddesine göre, 71. maddede yer verilen suçlar açısından soruşturma ve kovuşturma yapılabilmesi şikayete bağlıdır. Şikayette bulunabilecek kişi, eser

üzerindeki hakları tecavüze uğrayan kimsedir. Dolayısıyla, Eser sahibi, onun kanuni halefleri ve eser üzerindeki mali hakları bu kişilerden iktisap edenler ile meslek birlikleri şikayette bulunabilirler.[420] Şikayetin geçerli olabilmesi için, yine aynı maddeye göre, hak sahiplerinin veya üyesi oldukları meslek birliklerinin haklarını kanıtlayan belge veya sair delilleri cumhuriyet başsavcılığına vermeleri gerekmektedir.

FSEK'in 76. maddesine göre, 71. maddede düzenlenmiş suçlara bakmaya yetkili ve görevli mahkeme kanunda gösterilen ceza miktarına bakılmaksızın Adalet Bakanlığı tarafından kurulacak fikri ve sınai haklar ceza mahkemeleridir.

2.3.2.3. Koruyucu programları etkisiz kılma suçu (m. 72)

2.3.2.3.1. Genel olarak

5846 sayılı FSEK'in Hukuk ve Ceza Davaları başlıklı beşinci bölümünde ceza davalarını düzenleyen B kısmının Koruyucu Programları Etkisiz Kılmaya Yönelik Hazırlık Hareketleri başlıklı 72. maddesinde bilgisayar programlarını korumak amacıyla birtakım hazırlık hareketleri suç olarak düzenlenmiştir.

Bu hüküm, mevzuata 1995 yılında 4110 sayılı Kanun'la girmiştir. Daha sonra 2004 yılında 5101 sayılı Kanun'la hükümde değişiklik yapılmış, nihayet 2008 yılında 5728 sayılı Kanun'la yapılan son değişiklikle birlikte 72. madde bugünkü halini almıştır.[421]

Kanun koyucu 72. maddede korsan yazılımların üretimine karşı alınan birtakım önlemlerin yok edilmesine veya işlevsiz kılınmasına yönelik hareketleri cezalandırmaktadır. Çünkü, korsan yazılımların çoğaltılması ya da yayılması eser sahibinin mali haklarına zarar vermektedir. Aslında burada suç sayılan mali haklara yönelik tecavüz hareketleridir.[422]

2.3.2.3.2. Korunan hukuki yarar

FSEK'in 72. maddesinde düzenlenen suç tipiyle, dolaylı yoldan da olsa fikir ve sanat eseri olarak kabul edilen bilgisayar programları ve bu programlara sahip olanların çoğaltma ve kamuya sunma hakkı korunmaktadır. Kanun koyucu burada, daha ortada

[420]Bozbel, 2012, a.g.k., 597.
[421]Yazıcıoğlu, 2009, a.g.k., 419.
[422]Dülger, 2013, a.g.k., 650.

bir zarar olmamasına rağmen, bazı hazırlık hareketlerini suç olarak düzenlemiştir.

Korsanla mücadele edebilmek amacıyla, bilgisayar programlarını korumak için oluşturulmuş ilave programlara yönelik hazırlık hareketlerinin suç olarak düzenlenmesiyle, fikir ve sanat eseri sahibinin ve bağlantılı hak sahibinin, öncelikle mali olmak üzere, manevi hakları da koruma altına alınmıştır.[423]

2.3.2.3.3. Maddi unsur

2.3.2.3.3.1. Fiil

72. maddede düzenlenen suçun maddi unsurunu, bir bilgisayar programının hukuka aykırı olarak çoğaltılmasının önüne geçmek amacıyla oluşturulmuş ilave programları etkisiz kılmaya yönelik program veya teknik donanımları üretmek, satışa arz etmek, satmak veya kişisel kullanım amacı dışında elinde bulundurmak hareketleri oluşturur. Suç, seçimlik hareketli bir suçtur. Maddede sayılan fiillerin en az birinin gerçekleşmesiyle suç oluşacaktır.[424]

Bilgisayar programlarının hukuka aykırı olarak çoğaltılmasının önüne geçmek amacıyla üretilen programları kısıtlayan programlardan en çok kullanılanlar, crack programlar[425] ile çeşitli kopyalama programlarıdır.[426]

2.3.2.3.3.2. Fail ve mağdur

Kanun koyucu bu suç açısından failde herhangi bir özellik aramadığından dolayı suçun faili herkes olabilir. 72. maddede düzenlenen koruyucu programları etkisiz kılmaya yönelik hazırlık hareketlerini yapan herhangi bir kişi suçun faili olabilir.

Suç, mağdur açısından özellik gösterir. Mağdur herkes değil, sadece hak sahibidir. Bu sebeple suç mağdurun sıfatı bakımından özgü suçtur. Fikir ve sanat eseri üzerinde hak sahibi, Kanunun 19. maddesinde belirtildiği üzere eser sahibidir. Eser sahibi de 8. maddeye göre, eseri meydana getiren kişidir. Buradan da anlaşılacağı üzere, bu suçlarda mağdur sadece gerçek kişiler olabilir. Tüzel kişilerin suçun mağduru olması mümkün değildir. Tüzel kişilerin eser sahibi sayıldığı durumlarda ise eser sahibi olan tüzel kişiler

[423]Yazıcıoğlu, 2009, a.g.k., 423.
[424]Yavuz, Alıca ve Merdivan, 2013, a.g.k., 2252.
[425]Kendisine veya başkasına çıkar sağlamak için kötü niyetle web sayfalarının veya sistemlerin güvenlik duvarlarının ya da şifrelerinin kırılması suretiyle web sayfasına veya sistemlere zarar verilmesine crack, bu fiilleri gerçekleştirenlere de cracker denir. bkz. Özdilek, 2002, a.g.k., 166.
[426]Yazıcıoğlu, 2009, a.g.k., 427.

suçtan zarar gören sıfatını kazanırlar.[427]

2.3.2.3.3.3. Netice

Suçun oluşması için zararlı bir sonucun ortaya çıkmış olması şart değildir. Failin, madde metninde sayılan fiilleri gerçekleştirmesiyle suç oluşacaktır. Dolayısıyla, 72. maddede düzenlenen suç bir soyut tehlike suçudur.[428]

2.3.2.3.4. Manevi unsur

Bu suç, ancak kast ile işlenebilir. Suçun oluşumu için genel kast yeterlidir. Kanun koyucu failde ayrıca özel bir kast aramamıştır. Kanunda suçun taksirli haline yer verilmediğinden dolayı bu suçun taksirle işlenebilmesi mümkün değildir.

2.3.2.3.5. Hukuka aykırılık unsuru

Kanun koyucu, 72. maddede düzenlediği suç tipi için hiçbir hukuka uygunluk sebebi öngörmemiştir.

2.3.2.3.6. Suçun özel görünüş şekilleri

2.3.2.3.6.1. Teşebbüs

Koruyucu programları etkisiz kılma suçuna teşebbüs mümkündür. Yukarıda da belirttiğimiz gibi suç, neticesiz bir suç olduğu için fail tarafından elverişli vasıtalarla icra hareketlerinin yapılmış olması suçun oluşumu için yeterlidir. Ayrıca, bir zarar meydana gelmiş olması gerekmez. Bu suç açısından icra hareketlerinin parçalara bölünebildiği durumlarda, teşebbüs failin, elverişli vasıtalarla suçun icra hareketlerine başlaması fakat elinde olmayan sebeplerle icra hareketlerini tamamlayamaması halinde mümkündür.

2.3.2.3.6.2. İştirak

Koruyucu programları etkisiz kılma suçu, iştirak açısından bir özellik göstermez.

2.3.2.3.6.3. İçtima

Koruyucu programları etkisiz kılma suçu zincirleme şekilde işlenebilir. Failin, aynı suç işleme kararının icrası kapsamında farklı zamanlarda aynı mağdura karşı 72.

[427]Yazıcıoğlu, 2009, a.g.k., 425.
[428]Yazıcıoğlu, 2009, a.g.k., 430.

maddedeki suçu işlemesi halinde zincirleme suç hükümleri uygulanacaktır. Ancak, fiillerin aynı suç işleme kararından bahsedilemeyecek kadar uzun aralıklarla gerçekleştirilmesi halinde faile, her fiili için ayrı ceza verilmelidir.

2.3.2.3.7. Yaptırım, soruşturma ve kovuşturma

Kanun koyucu 72. maddede düzenlenen suç tipi için hapis cezası öngörmüştür. Bu hapis cezasının alt sınırı altı ay, üst sınırı ise iki yıldır.

FSEK'in 75. maddesine göre, 72. maddede yer verilen suç açısından soruşturma ve kovuşturma yapılabilmesi şikayete bağlıdır. Şikayette bulunabilecek kişi eser üzerindeki hakları tecavüze uğrayan kimsedir. Dolayısıyla, Eser sahibi, onun kanuni halefleri ve eser üzerindeki mali hakları bu kişilerden iktisap edenler ile meslek birlikleri şikayette bulunabilirler.[429] Şikayetin geçerli olabilmesi için, yine aynı maddeye göre hak sahiplerinin veya üyesi oldukları meslek birliklerinin haklarını kanıtlayan belge veya sair delilleri cumhuriyet başsavcılığına vermeleri gerekmektedir.

FSEK'in 76. maddesine göre, 72. maddede düzenlenen suça bakmaya yetkili ve görevli mahkeme, kanunda gösterilen ceza miktarına bakılmaksızın Adalet Bakanlığı tarafından kurulacak fikri ve sınai haklar ceza mahkemeleridir.

2.3.3. Elektronik İmza Kanunu'nda yer alan bilişim suçları

2.3.3.1. Genel olarak

Bakanlar Kurulu'nun 28.4.2003 tarihinde karara bağladığı Elektronik İmza Kanunu Tasarısı'nın genel gerekçesinde kanunun amacının, elektronik ticaretin gelişmesi ve elektronik imzanın kullanıcılar tarafından benimsenmesi için gerekli olan açık ağ sistemine güven duyulmasının sağlanması, güvenin sağlanabilmesi için de taraflar arasında karşılıklı olarak iletilen bilgilerin gizliliğinin ve bütünlüğünün korunması, tarafların kimliklerinin doğruluğunun güvence altına alınması olduğu belirtilmiştir. Bilgisayar ve internetin her geçen gün daha fazla sosyal yaşama girişini ve teknolojinin hızla gelişimini vurgulayan tasarı metni, ayrıca elektronik imzanın uluslararası düzeyde etkin olarak kullanılması dolayısıyla bu alanda çeşitli düzenlemeler yapıldığını, 13 Aralık 1999 tarihli Avrupa Parlamentosu ve Konseyi Elektronik İmza Direktifi ile Birleşmiş Milletlerin 14 Haziran 1996 tarihli Elektronik Ticarete İlişkin

[429] Bozbel, 2012, a.g.k., 597.

Model Kanunu'nun bu düzenlemelere örnek olduğunu belirtmiştir.[430] Yine gerekçede, hukuki ve ticari işlemlerde zaman, yer ve işgücü tasarrufu için elektronik imzanın çok yaygın olacağı öngörüldüğünden bu alanda hukuki düzenlemelerin yapılması gerekliliği vurgulanmış olup bunun ilk adımının Elektronik İmza Kanunu'nu çıkarmak olduğu belirtilmiştir.[431]

Bahsedilen Tasarı 15.01.2004 tarihinde 5070 sayılı Elektronik İmza Kanunu olarak TBMM'de kabul edildikten sonra, 23.01. 2004 tarihinde Resmi Gazete'de yayımlanmış ve kanunun 25. maddesi uyarınca altı ay sonra yürürlüğe girmiştir. EİK, elektronik imzaya ilişkin ilk yasal düzenlemedir. Ayrıca, kanunun 20. maddesinde belirtilmiş olan kanun maddelerinin uygulanmasına ilişkin usul ve esasların düzenlenmesi için Kurum[432] tarafından altı ay içinde ikincil düzenlemeler yapılacağı belirtilmiştir. Öngörülen süre içerisinde kurum gerekli ikincil yasal düzenlemeleri yapmıştır.[433]

EİK'nın en önemli özelliği, ıslak imza olarak tabir edilen geleneksel yöntemin karşılığı olarak elektronik imzayı hukuk dünyasına kazandırmasıdır. Bu yasa ile tüm kamu kurum ve kuruluşlarında ve elektronik ticaret olarak adlandırılan internet yoluyla ticarette büyük bir dönüşüm sağlanmıştır. Özellikle, elektronik ticarette önemli olan taraflar arası haberleşmede bilginin gizliliği, bütünlüğü ve tarafların kimliklerinin doğruluğu elektronik imza yolu ile garanti edilmiştir.[434] Kamu kurumlarında ise elektronik imza, işleri hızlandırmakta, kırtasiye masraflarını düşürmekte, kişiler ve kurumlar arası güveni artırmakta ve olası bazı hataları engelleyebilmektedir.

Burada belirtmek gerekir ki EİK'da sadece elektronik imza ile ilgili hususlar düzenlenmiştir. Elektronik imza ile doğrudan ilgisi olmayan örneğin, elektronik sözleşmeler konusuna hiç değinilmemiştir. Kanun tasarısının genel gerekçesinde, bu kanunla elektronik ticaretin bütünüyle düzenlenmesinin değil, elektronik ticaretin temel unsuru olan elektronik imzanın düzenlenmesinin hedeflendiği belirtilmiştir.[435]

---

[430]Dünyada elektronik imza alanında yapılan düzenlemelerle ilgili ayrıntılı bilgi için bkz. Orer, 2011, a.g.k., 34-35.; Topaloğlu, 2005, a.g.k., 122-126.

[431]https://www.tbmm.gov.tr/sirasayi/donem22/yil01/ss333m.htm (Erişim Tarihi: 22.07.2016)

[432]Bahsedilen kurum, EİK'nın 3/j maddesine göre, Telekomünikasyon Kurumu'dur. Fakat, bu Kurum'un adı daha sonra Bilgi Teknolojileri ve İletişim Kurumu olarak değiştirilmiştir.

[433]Yapılan ikincil yasal düzenlemelerin neler olduğuna dair ayrıntılı bilgi için bkz. T.K. Bensghir ve F. Topcan (2010). *E- imza Türkiye'de Kamu Kurumlarında Uygulanması*. Ankara: Öncü Basımevi, 112-118.

[434]M. Orta (2005). *Elektronik İmza ve Uygulaması*. Ankara: Seçkin Yayınevi, s. 92.

[435]Orta, 2005, a.g.k., 93.

Günümüzde teknolojinin hızlı gelişiminin bir sonucu olarak elektronik ortamda yapılan işlemler çoğalmaktadır. Posta ile mektup yollamak veya sözleşme yapmak yakında nostalji olacaktır. İletişim alanındaki ilerlemeler sayesinde sadece bilgi transferi değil bunun da ötesinde büyük sözleşmeler yapılmaktadır. Hatta, tapu sicili gibi kamu kurumlarına ait kayıtlar bile yakın zamanda elektronik olarak yürütülebilecektir.[436]

EİK'da denetim ve ceza hükümleri başlığı altında iki suç tipine yer verilmiştir. Kanun, elektronik imza ve onu oluşturan elektronik sertifikalara yönelik gerçekleştirilecek ihlal ve sahtekarlık fiillerini suç olarak düzenlemektedir. Kanunda yer verilmiş olan bu suçlar, elektronik imzanın yapısı gereği bilişim suçu olarak nitelendirilmektedir.[437]

2.3.3.2. Elektronik imza ve elektronik sertifika

EİK'nın 3-b maddesinde, elektronik imza, "başka bir elektronik veriye eklenen veya elektronik veriyle mantıksal bağlantısı bulunan ve kimlik doğrulama amacıyla kullanılan elektronik veri" şeklinde tanımlanmıştır. Kişinin elinin ürünü olan ıslak imza, sadece kağıt ve benzeri materyal üzerine atılabilir. Dijital (elektronik) imza ise kişinin duyu organlarıyla algılayamayacağı bir ortamda evrensel bir ağ vasıtasıyla iletilen imza türüdür. Kişinin bir metnin altına elle attığı imzası metnin içeriğini kabul ettiğini ve kendisi için artık, o metnin bağlayıcı olduğunu ifade eder. Elektronik ortamda yapılan işlemlerde ise, bu kabul ve bağlayıcılık beyanını ifade etme yöntemi elektronik imzadır.[438]

Elektronik imza, bilgilerin elektronik olarak taşındığı, kopyalandığı, işlendiği, internetteki iş ilişkilerinde, fikri hakların korunmasında (copyright) yazılımlardaki manipülasyonların kontrolünde kimlik tespitinde kullanılabilir.[439] Ayrıca, teknolojinin gelişimine bağlı olarak elektronik imzanın yakın zamanda kamu kurum ve kuruluşları, özel şirketler, üniversiteler, bilgi güvenliğinin önem arz ettiği organizasyonlar başta olmak üzere birçok yerde yaygın olarak kullanılacağı tahmin edilmektedir.[440]

---

[436]L.K. Berber (2002). *İnternet Üzerinden Yapılan İşlemlerde Elektronik Para ve Dijital İmza.* Ankara: Yetkin Yayınları, s. 125.
[437]Pallı, 2008, a.g.k., 233.
[438]Berber, 2002, a.g.k., 135.; G. Orer (2011). *Elektronik İmza ve Elektronik Sertifika Hizmet Sağlayıcısının Hukuki ve Cezai Sorumluluğu.* Ankara: Adalet Yayınevi, s. 32.
[439]Berber, 2002, a.g.k., 177.
[440]Orer, 2011, a.g.k., 70.

EİK'nın 5. maddesinde, güvenli elektronik imzanın elle atılan ıslak imza ile aynı hukuki sonucu doğuracağı belirtilmiştir. Kanun koyucunun elle atılan imzaya eşdeğer gördüğü herhangi bir elektronik imza değil, güvenli elektronik imzadır. Güvenli elektronik imzanın taşıması gereken özellikler kanunun 4. maddesinde belirtilmiştir. Buna göre, güvenli elektronik imza, münhasıran imza sahibine bağlı olan, sadece imza sahibinin tasarrufunda bulunan, güvenli elektronik imza oluşturma aracı ile oluşturulan, nitelikli elektronik sertifikaya dayanarak imza sahibinin kimliğinin tespitini ve imzalanmış elektronik veride sonradan herhangi bir değişiklik yapılıp yapılmadığının tespitini sağlayan elektronik imzadır.[441]

Güvenli elektronik imza, elle atılan imza ile aynı hukuki sonucu doğurmasına rağmen, bazı hukuki işlemler güvenli elektronik imzayla yapılamaz. EİK'nın 5/2. maddesine göre, kanunların resmî şekle veya özel bir merasime tabi tuttuğu hukukî işlemler ile teminat sözleşmeleri güvenli elektronik imza ile yapılamayacaktır. Bu kısıtlamanın getirilmesinin sebebinin hukuki işlem güvenliğinin tesis edilmesi ve tarafların bir hukuki işlem yaparken bunun sonuçlarını daha iyi düşünerek karar vermesini sağlamak olduğu söylenebilir. Benzer kısıtlamalar, Avrupa Birliği ülkelerinde de mevcuttur.[442]

Elektronik sertifika ise, kanunun 3/ı maddesinde "imza sahibinin, imza doğrulama verisini ve kimlik bilgilerini birbirine bağlayan elektronik kaydı" olarak tanımlanmıştır. Elektronik sertifikalar, sahibinin kişisel bilgilerini ve bu kişisel bilgilere ait açık anahtar bilgisini taşıyan ve taşıdığı açık anahtar bilgisinin belirtilen kişiye ait olduğunu garanti eden elektronik dosyalardır. Bu elektronik sertifikaları, elektronik sertifika hizmet sağlayıcısı[443] olarak adlandırılan güvenilir ve yetkilendirilmiş kuruluşlar verebilir.[444] Kanunun 8. maddesinde, kimlerin elektronik sertifika hizmet sağlayıcısı olabileceği düzenlenmiştir. Buna göre, elektronik sertifika, zaman damgası ve elektronik imzalarla ilgili hizmetleri sağlayan kamu kurum ve kuruluşları ile gerçek veya özel hukuk tüzel kişiler elektronik sertifika hizmet sağlayıcısı olabilirler. Bu kişilerin taşıması gereken şartlarda yine 8. maddede belirtilmiştir.

[441] Ayrıntılı bilgi için bkz. Bensghir ve Topcan, 2010, a.g.k., 118-121.; Orer, 2011, a.g.k., 43-45.
[442] Orta, 2005, a.g.k., 139-140.
[443] EİK'nın 8. maddesine göre, elektronik sertifika hizmet sağlayıcısı, elektronik sertifika, zaman damgası ve elektronik imzalarla ilgili hizmetleri sağlayan kamu kurum ve kuruluşları ile gerçek veya özel hukuk tüzel kişilerdir.
[444] Ayrıntılı bilgi için bkz. Bensghir ve Topcan, 2010, a.g.k., 18-19.; Orer, 2011, a.g.k., 93-95.

Geçerli bir elektronik imzanın, nitelikli elektronik sertifikaya dayanarak oluşturulması gerekmektedir.[445] Elektronik imzanın imkanlarından faydalanmak isteyenlerin, elektronik sertifika hizmet sağlayıcılarından elektronik sertifika temin etmeleri gerekmektedir.[446] Bu şarta aykırı olarak elde edilmiş olan elektronik imzalar, güvenli elektronik imza olarak değerlendirilemeyecektir.

2.3.3.3. İmza oluşturma verilerini izinsiz kullanma suçu (m. 16)

2.3.3.3.1. Genel olarak

Suç, EİK'nın Denetim ve Ceza Hükümleri başlıklı üçüncü kısmının 16. maddesinde İmza Oluşturma Verilerinin İzinsiz Kullanımı başlığı altında iki fıkra halinde düzenlenmiştir. Birinci fıkrada, suçun konusunu oluşturan imza oluşturma verisi ve imza oluşturma aracının izinsiz kullanımı yaptırıma bağlanmıştır. Madde metninde geçen imza oluşturma verisi, kanunun 3/d maddesinde, imza sahibine ait olan imza sahibi tarafından elektronik imza oluşturma amacıyla kullanılan ve bir eşi daha olmayan şifreler kriptografik gizli anahtarlar gibi veriler olarak, imza oluşturma aracı ise kanunun 3/e maddesinde elektronik imza oluşturmak üzere imza oluşturma verisini kullanan yazılım veya donanım aracı olarak tanımlanmıştır. İkinci fıkrada ise suçu ağırlaştıran bir hal öngörülmüştür. Bu fıkraya göre, birinci fıkrada belirtilen suçlar elektronik sertifika hizmet sağlayıcısı çalışanları tarafından işlenirse verilecek ceza yarı oranına kadar artırılacaktır.

2.3.3.3.2. Korunan hukuki yarar

Maddede düzenlenmiş olan suç tipiyle korunmak istenen hukuki yarar, elektronik imzaya duyulan güven ve ispat aracı olarak imzanın güvenliği ve bütünlüğüdür.[447] Yani korunan hukuki değer, evrakta sahtecilik suçlarıyla korunan değerin aynısıdır.[448] Bunun yanı sıra, korunan bir başka hukuki yarar elektronik ticaretin güvenliğidir. Çünkü, elektronik imza, elektronik ticaretin temel unsurunu oluşturduğundan imza oluşturma verilerinin izinsiz kullanımı, elektronik ticarette yapılan işlemlerde taraflar arasında güvenilirliği zedeleyecektir. Ayrıca, elektronik imza kamu kurum ve kuruluşları tarafından da kullanıldığından suçla korunan hukuki değerin, elektronik ticaretin

[445]Bensghir ve Topcan, 2010, a.g.k., 121.; Orer, 2011, a.g.k., 43-44.
[446]Orta, 2005, a.g.k., 108.
[447]Orer, 2011, a.g.k., 160.
[448]E. Yaycı (2007). *Bilişim Suçları*. Yayımlanmamış Yüksek Lisans Tezi. Ankara: Gazi Üniversitesi, s. 150-151.

güvenliği olmasının yanı sıra, elektronik ortamda gerçekleştirilen kamusal faaliyetler olduğu da söylenebilir.[449]

2.3.3.3.3. Maddi unsur

2.3.3.3.3.1. Fiil

Suçun hareket unsurunu, imza oluşturma verisi veya imza oluşturma aracını ilgili kişinin rızası dışında elde etmek, kopyalamak ve bu araçları yeniden oluşturmak veya izinsiz elde edilen imza oluşturma araçlarını kullanarak izinsiz elektronik imza oluşturmak fiilleri oluşturur. Görüldüğü üzere, suç, seçimlik hareketli bir suçtur. Suçun oluşması için failin madde metninde belirtilen fiillerden herhangi birini gerçekleştirmiş olması gerekmektedir.[450] Birden fazla fiil gerçekleşmiş olsa bile, fail tek bir suçtan cezalandırılır.

Suçun konusunu elektronik imza verisi veya aracı oluşturduğundan bunlar dışında kalan, imza doğrulama verisi veya aracına yönelik olarak gerçekleşecek fiiller, bu suç kapsamında değerlendirilemeyecektir. Fakat, mahiyetine uygun düştüğü ölçüde, bu fiiller TCK'da düzenlenen genel nitelikteki bilişim suçlarını oluşturabilir.[451]

2.3.3.3.3.2. Fail ve mağdur

Kanun koyucu imza oluşturma verilerinin izinsiz kullanımı suçu için failde herhangi bir özellik aramamıştır. Dolayısıyla, bu suçun faili herkes olabilir. Ancak, 16. maddenin 2. fıkrasında düzenlenen ağırlaştırılmış hal, suçun herkes tarafından değil, sadece elektronik sertifika hizmet sağlayıcısı çalışanları tarafından işlenmesi durumunda söz konusu olabilir.

Suçun mağduru, imza oluşturma verisi veya imza oluşturma aracı kendisinin izni dışında kullanılmış herhangi bir kişidir. Suçun mağduru, sadece gerçek kişiler olabilir. Tüzel kişiler ancak suçtan zarar gören olabilirler. Bir görüşe göre, bu suçun mağduru daima devlettir ve bu madde kapsamındaki fiiller dolayısıyla zarar görenler mağdur olmazlar, ancak kamu davasına katılmak suretiyle katılan sıfatını alabilirler.[452] Fakat, tüm suçların dolaylı mağduru devlettir. Bunun yanı sıra, hemen her suçun bir de fiil

[449]Pallı, 2008, a.g.k., 238.
[450]Orer, 2011, a.g.k., 161.
[451]Pallı, 2008, a.g.k., 239-240.
[452]Yaycı, 2007, a.g.k., 151.; Orer, 2011, a.g.k., 163.

neticesinde zarara uğramış kişisi yani doğrudan mağduru vardır. Bundan ötürü, bu suç tipinde tek mağdurun daima devlet olduğu görüşüne katılmak mümkün değildir.

2.3.3.3.3.3. Netice

Maddede sayılmış olan fiillerin işlenmesiyle suç tamamlanmış sayılır. Kanun koyucu suçun oluşması için herhangi bir neticenin meydana gelmesi şartı aramamıştır. bu suç, bir zarar suçudur.

2.3.3.3.4. Manevi unsur

Suç, ancak kastla işlenebilir. Genel kast, suçun oluşumu için yeterlidir. Failde, özel bir kastı olmasına gerek yoktur. Taksirli hali kanunda düzenlenmediğinden suçun taksirli hali cezalandırılmaz.

Failin suçu işlerken hangi saikle hareket ettiğinin tam olarak tespiti zor olduğundan dolayı, bu durum uygulamada sıkıntılara sebep olacaktır. Örneğin, failin elektronik imza oluşturma verisini, sıradan bir kredi kartı şifresi ya da bilgisayar giriş şifresi olduğunu düşünerek elde etmesi durumunda kişisel verileri elde etme suçu oluşabilir ya da bir hırsızın eve girerek, elektronik imza oluşturma verisinin CD ya da benzeri depolama cihazında olması durumunda herhangi bir taşınır eşya gibi bunu çalmış olması öncelikle hırsızlık suçu olarak değerlendirilebilir.

2.3.3.3.5. Hukuka aykırılık unsuru

Madde metninde belirtilen tek hukuka uygunluk sebebi, ilgilinin rızasıdır. Elektronik imza oluşturma verisi veya imza oluşturma aracının sahibi olan kişinin rızası, fiili hukuka uygun hale getirir. Bunun haricinde, herhangi bir hukuka uygunluk sebebi yoktur.

2.3.3.3.6. Suçun nitelikli hali

EİK'nın 16. maddesinin 2. fıkrasına göre, suçun failinin elektronik sertifika hizmet sağlayıcısı olması durumunda 1. fıkraya göre verilecek cezalar yarısına kadar artırılacaktır.

2.3.3.3.7. Suçun özel görünüş şekilleri

2.3.3.3.7.1. Teşebbüs

İmza oluşturma verilerini izinsiz kullanma suçuna teşebbüs mümkündür. Yukarıda da belirttiğimiz gibi suç neticesiz bir suç olduğu için fail tarafından elverişli vasıtalarla icra hareketlerinin yapılmış olması suçun oluşumu için yeterlidir. Ayrıca bir zarar meydana gelmiş olması gerekmez. Bu suç açısından icra hareketlerinin parçalara bölünebildiği durumlarda, teşebbüs failin, elverişli vasıtalarla suçun icra hareketlerine başlaması fakat elinde olmayan sebeplerle icra hareketlerini tamamlayamaması halinde mümkündür.

2.3.3.3.7.2. İştirak

İmza oluşturma verilerini izinsiz kullanma suçu, iştirak açısından bir özellik göstermez.

2.3.3.3.7.3. İçtima

İmza oluşturma verilerini izinsiz kullanma suçu zincirleme şekilde işlenebilir. Failin aynı suç işleme kararının icrası kapsamında farklı zamanlarda aynı mağdura karşı 16. maddedeki suçu işlemesi halinde zincirleme suç hükümleri uygulanacaktır. Ancak, fiillerin aynı suç işleme kararından bahsedilemeyecek kadar uzun aralıklarla gerçekleştirilmesi halinde faile, her fiili için ayrı ceza verilmelidir.

2.3.3.3.8. Yaptırım, soruşturma ve kovuşturma

Bu suç için öngörülen yaptırım hem hapis cezası hem de adli para cezasıdır. Hakim imza verilerini izinsiz kullanma suçunda her iki cezayı da vermek zorundadır. Sadece hapis ya da sadece adli para cezasını seçmek gibi bir takdir hakkı yoktur. Hapis cezasının alt sınırı bir yıl, üst sınırı ise üç yıldır. Adli para cezasının alt sınırı elli gündür, üst sınırı ise maddede belirtilmediğinden genel hükümlere göre belirlenecektir. İkinci fıkrada düzenlenen ağırlaştırılmış halin gerçekleşmesi durumunda birinci fıkraya göre verilmiş olan cezalar yarı oranına kadar artırılacaktır.

Görevli mahkeme, 5235 sayılı Adli Yargı İlk Derece Mahkemeleri ile Bölge Adliye Mahkemelerinin Kuruluş, Görev ve Yetkileri Hakkında Kanun'un 11. ve 12. maddelerine göre asliye ceza mahkemeleridir. 2. fıkradaki suçun nitelikli halinde de asliye ceza mahkemeleri görevlidir. Suçun takibi şikayete bağlı değildir, resen

soruşturulur.

2.3.3.4. Elektronik sertifikalarda sahtekarlık suçu (m. 17)

2.3.3.4.1. Genel olarak

Suç, EİK'nın Denetim ve Ceza Hükümleri başlıklı üçüncü kısmının 17. maddesinde Elektronik Sertifikalarda Sahtekarlık başlığı altında iki fıkra halinde düzenlenmiştir. Birinci fıkrada, suçun konusunu oluşturan elektronik sertifikaların tamamen veya kısmen sahte oluşturulması, geçerli olan elektronik sertifikayı geçersiz hale getirmek ve geçersiz olan elektronik sertifikayı kullanmak yaptırıma bağlanmıştır. Elektronik sertifika, kanunun 3/ı maddesinde, İmza sahibinin, imza doğrulama verisini ve kimlik bilgilerini birbirine bağlayan elektronik kaydı olarak tanımlanmıştır. Bu suç, geleneksel sahtecilik suçunun güvenli elektronik imza oluşturmaya yarayan elektronik sertifika üzerinde işlenmesi anlamına gelmektedir.[453] Fakat, burada suçun işleniş tarzı ve maddi unsuru bazı farklılık göstermektedir. 17. maddenin ikinci fıkrasında suçu ağırlaştıran bir hal öngörülmüştür. Bu fıkraya göre, birinci fıkrada belirtilen suçlar elektronik sertifika hizmet sağlayıcısı tarafından işlenirse verilecek ceza yarı oranına kadar artırılacaktır.

2.3.3.4.2. Korunan hukuki yarar

Suçla korunan hukuki yarar, elektronik imzaya duyulan güven ve ispat aracı olarak imzanın güvenliği ve bütünlüğüdür.[454] Yani korunan hukuki değer, evrakta sahtecilik suçlarıyla korunan değerin aynısıdır.[455] Bunun yanı sıra, korunan bir başka hukuki değer, elektronik ticaretin güvenliğidir. Elektronik imza, kamu kurum ve kuruluşları tarafından da kullanılmakta olduğu için korunan hukuki değerin, elektronik ticaretin güvenliğinin yanı sıra elektronik ortamda yürütülen kamusal faaliyetler olduğu söylenebilir.[456]

2.3.3.4.3. Maddi unsur

2.3.3.4.3.1. Fiil

Suçun maddi unsurunu, tamamen veya kısmen sahte elektronik sertifika

[453]Pallı, 2008, a.g.k., 241.
[454]Orer, 2011, a.g.k., 167.
[455]Yaycı, 2007, a.g.k., 150-151.
[456]Pallı, 2008, a.g.k., 241.

oluşturmak veya geçerli olarak oluşturulan elektronik sertifikaları taklit etmek veya tahrif etmek, sahte oluşturulmuş, taklit veya tahrif edilmiş olan elektronik sertifikaları kullanmak fiilleri oluşturur. Suç, seçimlik hareketli bir suçtur. Maddede belirtilen fiillerin herhangi birinin işlenmesi halinde suç oluşacaktır, birden fazla fiil bir arada gerçekleştiğinde de tek bir suç oluşur ve fail bu maddedeki suçtan bir kez cezalandırılır. Tahrif, bir şeyin aslını bozmak, kalem oynatmak ya da değiştirmek[457]; taklit ise, benzeterek yapmak, benzemeye veya benzetmeye çalışmak, imitasyon anlamlarına gelir.[458] Elektronik sertifikalarda yapılacak sahtecilik, suçun işlenme tarzına göre maddi ya da fikri sahtecilik şeklinde olabilir.

2.3.3.4.3.2. Fail ve mağdur

Kanun koyucu, elektronik sertifikalarda sahtecilik suçu için failde herhangi bir özellik aramamıştır. Dolayısıyla, bu suçun faili herkes olabilir. Ancak, 17. maddenin 2. fıkrasında düzenlenen ağırlaştırılmış hal, suçun, herkes tarafından değil, sadece elektronik sertifika hizmet sağlayıcısı çalışanları tarafından işlenmesi durumunda söz konusu olabilir. Suçun mağduru, herhangi bir gerçek kişidir. Tüzel kişiler ancak suçtan zarar gören olabilirler. Bir görüşe göre, bu suçun mağduru daima devlettir ve bu madde kapsamındaki fiiller dolayısıyla zarar görenler mağdur olmazlar ancak kamu davasına katılmak suretiyle katılan sıfatını alabilirler.[459] Fakat, tüm suçların dolaylı mağduru devlettir. Bunun yanı sıra, hemen her suçun bir de fiil neticesinde zarara uğramış kişisi yani doğrudan mağduru vardır. Bundan ötürü, bu suç tipinde tek mağdurun daima devlet olduğu görüşüne katılmak mümkün değildir.

2.3.3.4.3.3. Netice

Maddede sayılmış olan fiillerin işlenmesiyle suç tamamlanmış sayılır. Kanun koyucu suçun oluşması için herhangi bir neticenin meydana gelmesi şartı aramamıştır. Suç, neticesi harekete bitişik bir suçtur.

2.3.3.4.4. Manevi unsur

Suç, ancak kastla işlenebilir. Failin genel kastı suçun oluşumu için yeterlidir, özel

[457] http://tdk.gov.tr/index.php?option=com_bts&arama=kelime&guid=TDK.GTS.5887ba402a8c24.09321679 (Erişim Tarihi: 24.01.2017)
[458] http://tdk.gov.tr/index.php?option=com_bts&arama=kelime&guid=TDK.GTS.5887b987b91361.91400854 (Erişim Tarihi: 24.01.2017)
[459] Yaycı, 2007, a.g.k., 151.; Orer, 2011, a.g.k., 170.

bir kastı olmasına gerek yoktur. Suçun taksirli hali kanunda düzenlenmediğinden suçun taksirle işlenmesi mümkün değildir.

Klasik sahtecilik suçlarında failde aranan zarar verme kastı bu suç açısından geçerli değildir. Çünkü, bilişim suçlarının büyük bir kısmında failin menfaat elde etmek veya başkasına zarar vermek kastını taşıması gerekmekle birlikte, bu suçların fail tarafından sırf merak ya da kendini test etme kastıyla işlenmesi de mümkündür.[460]

2.3.3.4.5. Hukuka aykırılık unsuru

Bu suç için 17. maddede herhangi bir hukuka uygunluk sebebi öngörülmemiştir. Suçun maddi unsurunun, elektronik sertifikaların sahte üretimi, taklidi veya tahrifi gibi hukuk düzeninin korumayacağı fiiller olmasından dolayı genel hukuka uygunluk sebeplerinin de burada uygulama alanı bulmayacağı söylenebilir.

2.3.3.4.6. Suçun nitelikli hali

EİK'nın 17. maddesinin 2. fıkrasına göre, suçun failinin elektronik sertifika hizmet sağlayıcısı olması durumunda 1. fıkraya göre verilecek cezalar yarısına kadar artırılacaktır.

2.3.3.4.7. Suçun özel görünüş şekilleri

2.3.3.4.7.1. Teşebbüs

Elektronik sertifikalarda sahtekarlık suçuna teşebbüs mümkündür. Yukarıda da belirttiğimiz gibi suç neticesiz bir suç olduğu için fail tarafından elverişli vasıtalarla icra hareketlerinin yapılmış olması suçun oluşumu için yeterlidir. Ayrıca bir zarar meydana gelmiş olması gerekmez. Bu suç açısından icra hareketlerinin parçalara bölünebildiği durumlarda, teşebbüs failin, elverişli vasıtalarla suçun icra hareketlerine başlaması fakat elinde olmayan sebeplerle icra hareketlerini tamamlayamaması halinde mümkündür.

2.3.3.4.7.2. İştirak

Elektronik sertifikalarda sahtekarlık suçu iştirak açısından bir özellik göstermez.

[460]Pallı, 2008, a.g.k., 243.

2.3.3.4.7.3. İçtima

Elektronik sertifikalarda sahtekarlık suçu zincirleme şekilde işlenebilir. Failin aynı suç işleme kararının icrası kapsamında farklı zamanlarda aynı mağdura karşı 17. maddedeki suçu işlemesi halinde zincirleme suç hükümleri uygulanacaktır. Ancak, fiillerin aynı suç işleme kararından bahsedilemeyecek kadar uzun aralıklarla gerçekleştirilmesi halinde her fiil için ayrı ceza verilmelidir.

2.3.3.4.8. Yaptırım, soruşturma ve kovuşturma

Bu suç için öngörülen yaptırım hem hapis cezası hem de adli para cezasıdır. Hakim, elektronik sertifikalarda sahtekarlık yapılması suçunda her iki cezayı da vermek zorundadır. Sadece hapis ya da sadece adli para cezasını seçmek gibi bir takdir hakkı yoktur. Hapis cezasının alt sınırı iki yıl, üst sınırı ise beş yıldır. Adli para cezasının alt sınırı yüz gündür, üst sınırı ise genel hükümlere göre belirlenecektir. İkinci fıkrada düzenlenen ağırlaştırılmış halin gerçekleşmesi durumunda, birinci fıkraya göre verilmiş olan cezalar yarı oranına kadar artırılacaktır.

Görevli mahkeme, 5235 sayılı Adli Yargı İlk Derece Mahkemeleri ile Bölge Adliye Mahkemelerinin Kuruluş, Görev ve Yetkileri Hakkında Kanun'un 11. ve 12. maddelerine göre asliye ceza mahkemeleridir. 2. fıkradaki suçun nitelikli halinde de asliye ceza mahkemeleri görevlidir. Suçun takibi şikayete bağlı değildir, resen soruşturulur.

SONUÇ

Bilişim teknolojisinin gelişmesi, yeni suç tiplerini ortaya çıkarmıştır. Teknolojik alanda yaşanan bu ilerleme, bilişim araçlarının sosyal yaşamda yaygın olarak kullanılması ve insan hayatını kolaylaştırmasının yanı sıra kötü niyetli kişilere de birçok imkan sunmaktadır. Gelişen bilişim teknolojilerinin kendilerine sağladığı avantajı kullanan suç failleri, zararlı yazılım ve programlarla ya da bilişim sistemlerindeki açıkları kullanmak suretiyle, çoğu zaman sadece bilgisayar klavyesini kullanmaktan öte geçmeyen hareketleri ile insanların haklarını ihlal etmektedirler. İlk bakışta, basit ve sıradan fiiller olarak görülüp önemsenmeyen bu tarz ihlaller, kimi zaman tahminlerin çok ötesinde zararlara sebebiyet vermektedir.

Meydana gelebilecek zararlarla ilgili örnek vermek gerekirse; geçtiğimiz günlerde henüz kim tarafından gerçekleştirildiği tespit edilemeyen bir siber saldırı sonucu dünya üzerinde yüzbinlerce bilgisayar çalışamaz hale geldi. Buna benzer ve tüm dünya çapında etkisini hissettiren bir başka olay da, Amerikan Diplomasisine ait gizli bilgileri içeren Wikileaks belgelerinin hackerlar tarafından ele geçirilerek yayımlanması oldu. Yine yakın zamanda ülkemizde, 50 milyon kişinin kimlik bilgileri hackerların eline geçti. Çeşitli zamanlarda, birçok devlet kurumunun resmi internet siteleri, farklı teknikler kullanılarak yapılan siber saldırılar sonucu kısa süreli de olsa devre dışı bırakıldı. Çok sayıda kişinin sosyal medya hesapları ele geçirilerek onlara ait gizli bilgiler ifşa edildi. Ayrıca, hesaba giriş şifreleri değiştirildi, kişiler kendi hesaplarına giremedi. Bankacılık sistemi açısından ise örneğin, faillerin banka müşterilerinin kart ve hesap bilgilerini, bilişim araçlarını kullanarak elde etmesi sonucu faillerin, çok yüksek miktardaki parayı kendi hesaplarına geçirmeleri, hatta belki de kart ya da hesap sahiplerinin tüm mal varlıklarını elde etmeleri söz konusu olabilir.

Günümüz dünyasında, bilişim sistemlerinin hemen her alanda kullanılması, kamu kurumları ve özel sektör için hayati öneme sahip bilgi ve belgelerin bilgisayar sistemiyle muhafaza ediliyor olması, bilişim alanındaki tehlikeyi daha da artırmaktadır. Bilişim suçlularının, diğer suçların faillerine göre çok daha nitelikli olmaları, onları suç işlemeye iten sebeplerin klasik suçlardaki gibi sadece maddi menfaat elde etmek, intikam almak ya da cinsel haz duymak gibi saiklerle ya da merak, arzu, kendini

kanıtlama, yeteneğini gösterme vb. dürtüler ve motivasyonla hareket etmeleri, bilişim suçlarıyla mücadeleyi zorlaştıran faktörlerdir. Bunların yanı sıra, mücadeleyi zorlaştıran bir başka faktörde bilişim suçlarının herhangi bir ülke ya da bölgeyle sınırlı kalmaması, tüm dünyada etkisini hissettirerek çok sayıda devleti ve kişiyi mağdur etmesidir.

Bilişim alanındaki ihlallerle mücadele edebilmenin en etkili yolu, uluslararası işbirliğini artırmaktır. Çünkü, siber saldırılar, hacker faaliyetleri vb. şeklindeki bilişim suçları bütün devletleri tehdit etmektedir. Bu durum, suçla mücadelede uluslararası düzenlemeler yapma ihtiyacını doğurmaktadır. Uluslararası metinlerle, tarafların yapacakları düzenlemelerde birtakım asgari standartları tesis etmeleri gerekmektedir. Örneğin, bilişim sistemlerine haksız erişim öncelikle suç olarak düzenlenmelidir. Çünkü, haksız erişim çoğu zaman bilişim alanında işlenen diğer suçlar için bir araç suç olup, adeta daha sonra gerçekleştirilecek fiiller için geçiş yolu oluşturmaktadır. Ayrıca, bilişim sistemlerinin işleyişine ve güvenilirliğine yönelen her türlü hareket suç olarak tanımlanmalıdır. Bunların yanı sıra, bilişim sistemlerinin araç olarak kullanılması suretiyle işlenen suçlar da dolaylı bilişim suçları olarak kabul edilmelidir.

Uluslararası düzeyde bilişim suçlarına yönelik en etkili düzenlemenin Avrupa Siber Suçlar Sözleşmesi olduğu kabul edilmektedir. Sözleşme, yetkisiz erişim başta olmak üzere, bilişim suçlarının tamamına yer veren çok kapsamlı bir metin olarak değerlendirilmektedir. Ayrıca, sözleşmede meydana gelebilecek yetki ve usul sorunlarına çözüm getiren hükümler yer almaktadır. Türkiye, 2010 yılında imzaladığı bu sözleşmeyi, 2014 yılında yürürlüğe sokmuştur.

Suçla mücadelede ikinci aşamayı ise devletlerin kendi iç hukuk metinlerindeki ceza normlarının, uluslararası standartlara uyumu oluşturmaktadır. Her devlet, bilişim alanındaki ihlal hareketlerini önleyebilmek için uluslararası sisteme entegre olmalıdır. Sözleşmelerde suç olarak düzenlenmesi tavsiye edilen başta, bilişim sistemlerine yetkisiz erişim olmak üzere, sistemlere tecavüz niteliği taşıyan her türlü hareket ceza normu olarak kabul edilmelidir. Bir başka deyişle, ulusal ve uluslararası düzenlemeler mümkün olduğunca yeknesak olmalı, iç hukuk metinlerindeki eksiklikler ve hatalar giderilerek uluslararası standartlar yakalanmalıdır.

Türkiye'de bilişim suçlarına yönelik ilk düzenlemeye 1989 yılındaki kanun tasarısında yer verilmiş 1991 yılında da bu suçlar ilk kez mevzuata girmiştir. Bilişim

sistemlerindeki birtakım ihlalleri suç olarak tanımlayan eski kanun döneminde özellikle, bilişim sistemlerine yetkisiz erişim fiili cezalandırılmamaktaydı. 2005 yılında yürürlüğe giren 5237 sayılı TCK ile birlikte bilişim suçlarının ilk aşamasını oluşturan yetkisiz erişim suç haline getirildi. Ancak, yetkisiz erişimin cezalandırılmasının failin bilişim sistemine girdikten sonra orada bir süre kalmış olması şartına bağlanması eleştirilmekteydi. Yine bu kanunda ilk kez banka ve kredi kartlarının kötüye kullanılması ilk kez münhasıran suç olarak düzenlendi. Ayrıca, yeni kanunla ilk kez klasik suçlar olarak kabul edilen hırsızlık, dolandırıcılık gibi suçların bilişim sistemlerinin kullanılması suretiyle işlenmesi suçun nitelikli hali olarak kabul edildi. Böylece, dolaylı bilişim suçları ceza kanununa girmiş oldu. Sonraki yıllarda kanunda yapılan değişiklikle, bilişim sistemlerine yetkisiz erişim sistemde bir süre kalmış olma şartı aranmaksızın münhasıran suç olarak tanımlandı. Ayrıca, bilişim sistemine girmeksizin teknik araçlarla sistemdeki veri nakillerini izlemek suç olarak düzenlendi. Kanuna bir madde eklenerek, bilişim suçlarını işlemek amacıyla cihaz ya da program oluşturma fiilleri suç olarak düzenlendi.

Türk Hukukunda, bilişim suçlarına yönelik düzenlemeler sadece ceza kanunuyla sınırlı kalmadı. Bunun yanı sıra, Fikir ve Sanat Eserleri Kanunu'nda ve Elektronik İmza Kanunu'nda da birtakım düzenlemeler yapıldı. Ayrıca, başka bazı kanunlarda da bilişim suçu sayılan düzenlemelere yer verildi. Bu düzenlemelerden en dikkat çekici olanlara değinmek gerekirse, örneğin, Fikir ve Sanat Eserleri Kanunu'nda, eklenen bir hükümle bilgisayar programları bu kanun kapsamında eser kabul edildi. Böylece, bilgisayar programları oluşturanların hakları etkin bir şekilde korunmak istendi. Yine kanunda, 3 farklı maddede düzenlenmiş fikir ve sanat eserlerine yönelik tecavüz fiilleri, manevi, mali ve bağlantılı haklara yönelik tecavüz başlığı altında tek bir maddede toplandı. Elektronik İmza Kanunu'nda yapılan değişiklikle, imza oluşturma verilerini izinsiz kullanma ve elektronik sertifikalarda sahtekarlık yapma fiili suç olarak tanımlandı. Elektronik imza, teknolojinin sosyal yaşamın her alanına girmesiyle birlikte önemini artırmaktadır. Kanunda tanımlanmış olan güvenli elektronik imza, bazı istisnalar dışında, kişinin elinin ürünü olan ıslak imzayla aynı hüküm ve sonuçları doğurmakta ve kişiyi borç ve sorumluluk altına sokabilmektedir. Böylesine önemli bir işleve sahip olan güvenli elektronik imzayı oluşturma yetkisini haiz olan elektronik sertifika hizmet

sağlayıcıları başta olmak üzere, diğer kişi ve kurumların bu yetkiyi kötüye kullanmasını önlemeye yönelik düzenlemeler yapılması isabetli olmuştur.

Türk Hukukunda, bilişim suçlarına yönelik bahsetmiş olduğumuz düzenlemeler, genel itibariyle olumlu olmakla birlikte birtakım eksiklikler ve hatalar barındırmaktadır. Suçla mücadelenin ilk şartının etkili hukuk kurallarının tesisi olması gerçeği karşısında, kanun koyucunun mevzuatın aksayan yönlerini gidermesi gerekmektedir. Çalışmamızda yeri geldikçe değindiğimiz, doktrinde eleştiri konusu olan ve uygulamada sorun teşkil eden hükümler gözden geçirilmelidir.

Bilişim suçlarıyla mücadelede etkili hukuk kuralları oluşturulması ilk faktör olmakla beraber tek başına yeterli değildir. Bunun yanı sıra, bilişim sistemlerinin teknik bir alan olması sebebiyle, teknik bilgiye sahip uzmanlaşmış personelin bu alanda istihdam edilmesi gerekmektedir. Özellikle, ethical hackerların suçla mücadelede aktif rol alması gerekir. Ayrıca, suçla mücadele kapsamında, suç faillerinin takip edilebilmeleri ve yakalanmaları, yargılanmaları ve cezalandırılabilmeleri açısından teknik cihazlara ihtiyaç duyulmaktadır. Ülkemizde, bilişim uzmanları başta olmak üzere, bilişim alanında yetişmiş insan gücünün azlığı, suçla mücadelede en büyük zaaflardan birisidir. Yeterli teknik bilgiye sahip personelin yetiştirilmesi ve gerekli olan teknik cihazların temini, devlet tarafından bu işe kaynak aktarılmasına, gerekli teşviklerin sağlanmasına ve bilişim sistemlerine ilgi duyan bireylerin bu alanda eğitilmelerine bağlıdır.

Bilişim suçlarıyla mücadelede münhasıran bilişim suçlarına bakan ihtisas mahkemeleri kurulması da düşünülebilir. Bilişim suçları kanunda öngörülen cezalar itibariyle asliye ceza mahkemelerinin görev alanına girmektedir. Ceza hukuku sistemimizde, asıl mahkemelerin asliye ceza mahkemeleri olması ve bu mahkemelerin, Türk Ceza Kanunu'ndaki ve özel ceza yasalarındaki birbirinden çok farklı olan suç tiplerine bakması sebebiyle, bilişim suçları bu mahkeme hakimleri tarafından doğal olarak, sıradan bir suç tipi olarak görülmektedir. Ancak, bahsettiğimiz gibi bilişim sistemlerinin teknik bilgi ve konu üzerinde özel çalışma gerektiren bir alan olması ve bilişim suçlarının çok vahim sonuçlar doğurabilmesi ihtimali nazara alınarak ihtisas mahkemeleri kurulması görüşü değerlendirilmelidir.

Son olarak, bilişim suçlarıyla mücadelede bir başka tedbir de bireyleri bilişim sistemlerinde yaşayabilecekleri mağduriyetlere karşı bilinçlendirmektir. Bilişim alanında, bireylerin bilgisini artırabilmek açısından kamu spotları, eğitim faaliyetleri, uyarı mesajları, reklam ve tanıtım organizasyonları etkili olabilecek yöntemlerdir. Bunun yanı sıra, siber alanda kişilerin kendilerini saldırılara karşı koruyabilmeleri için özellikle internet kullanımında dikkatli olmaları ve sorumlu davranmaları gerekmektedir. Gelecekte bilişim sistemlerinin sosyal yaşamda çok daha fazla yer edinmesi ihtimali karşısında, meydana gelebilecek zararları asgari düzeye indirilebilmek için bilişim suçlarıyla mücadelede geç kalınmamalıdır.

KAYNAKÇA

Acun, R. (2000). İnternet ve Telif hakları. *Bilgi Dünyası*, 1 (1), 5-25.

Akarslan, H. (2012). *Bilişim Suçları*. Ankara: Seçkin Yayınevi.

Akbulut, B.B. (2000). Bilişim Suçları. *SÜHFD*, 7 (1-2), 545-555.

Akbulut, B. (2016). *Ceza Hukuku Genel Hükümler*. (3. Baskı). Ankara: Adalet Yayınevi.

Artuk, M.E. ve Çınar, A.R. (2004). Yeni Bir Ceza Kanunu Arayışları ve Adalet Alt Komisyonu Tasarısı Üzerine Düşünceler. T. Ergül (Ed.), *Türk Ceza Kanunu Reformu İkinci Kitap Makaleler, Görüşler, Raporlar* içinde (s. 37-84). Ankara: Türkiye Barolar Birliği Yayınları.

Artuk, M.E., Gökçen, A. ve Yenidünya, A.C. (2009). *TCK Şerhi Özel Hükümler Madde 235-345 5. Cilt.* Ankara: Turhan Kitabevi.

Artuk, M.E., Gökçen, A. ve Yenidünya, A.C. (2011). *Ceza Hukuku Özel Hükümler*. (11. Baskı). Ankara: Adalet Yayınevi.

Artuk, M.E., Gökçen, A. ve Yenidünya, A.C. (2015). *Ceza Hukuku Özel Hükümler*. (15. Baskı). Ankara: Adalet Yayınevi.

Artuk, M.E., Gökçen, A. ve Yenidünya, A.C. (2016). *Ceza Hukuku Genel Hükümler*. (10. Baskı). Ankara: Adalet Yayınevi.

Avşar, B.Z. ve Öngören, G. (2010). *Bilişim Hukuku*. İstanbul: Türkiye Bankalar Birliği.

Aydın, E.D. (1992). Bilişim Sistemlerinde Güvenlik, Güvenirlik, Mahremiyet ve Bilişim Suçları. *Marmara İletişim Dergisi*, (1), 109-137.

Aydın, E.D. (1992). *Bilişim Suçları ve Hukukuna Giriş*. Ankara: Doruk Yayınevi.

Aydın, E.D. (1999). *Bilişim ve Telekomünikasyon Terimler Sözlüğü*. İstanbul: Telsim Yayınları.

Bayındır, S. (2014). Eser Sahibinin İzni Olmaksızın Eseri Umuma İletim Suçu. *TBB Dergisi*, (113), 307-338.

Bensghir, T.K. ve Topcan, F. (2010). *E- imza Türkiye'de Kamu Kurumlarında*

Uygulanması. Ankara: Öncü Basımevi.

Berber, L.K. (2002). *İnternet Üzerinden Yapılan İşlemlerde Elektronik Para ve Dijital İmza*. Ankara: Yetkin Yayınları.

Biçkin, İ. (2006). Siber Suç Sözleşmesi ve 5237 Sayılı Türk Ceza Kanununda Bilişim Suçları. *Yargıtay Dergisi*, 32 (1-2), 145-168.

Bozbel, S. (2012). *Fikir ve Sanat Eserleri Hukuku*. İstanbul: On İki Levha Yayınları.

Casey, E. (2011). *Digital Evidence and Computer Crime Forensic Science, Computers and Internet*. Cambridge, Massachusetts: Academic Press.

Değirmenci, O. (2005). 2004 Türk Ceza Kanunu'nun Bilişim Suçları Bakımından Değerlendirilmesi. *TBB Dergisi*, (58), 195-208.

Değirmenci, O. (2014). *Ceza Muhakemesinde Sayısal (Dijital) Delil*. Ankara: Seçkin Yayınevi.

Demirbaş, T. (2016). *Ceza Hukuku Genel Hükümler*. (11. Baskı). Ankara: Seçkin Yayınevi.

Doğan, K. (2005). Bilişim Suçları ve Yeni Türk Ceza Kanunu. *Hukuk ve Adalet Eleştirel Hukuk Dergisi*. (6-7), 290-319.

Dönmezer, S. (1995). *Kişilere ve Mala Karşı Cürümler*. (14. Bası). İstanbul: Beta Yayınevi.

Dursun, H. (1998). Bilgisayar İle İlgili Suçlar, *Yargıtay Dergisi*, 24 (3), 334-339.

Dülger, M.V. (2004). *Bilişim Suçları*. Ankara: Seçkin Yayınevi.

Dülger, M.V. (2013). *Bilişim Suçları ve İnternet İletişim Hukuku*. (3. Baskı). Ankara: Seçkin Yayınevi.

Eker, Ö.U. (2006). "Türk Ceza Hukuku'nda Bilişim Suçları" Eski TCK Bağlamında Hukukumuzda Yer Alan İlk Düzenlemeler ve 5237 Sayılı Yeni Türk Ceza Kanunu'nun İlgili Hükümlerinin Yorumu. *TBB Dergisi,* (62), 101-131.

Ekinci, M. ve Esen, S. (2003). *Açıklamalı ve İçtihatlı Sahtecilik Hırsızlık Gasp Dolandırıcılık Emniyeti Suistimal Bilişim Alanında Suçlar ile Müşterek Hükümler*. Ankara: Adalet Yayınevi.

Erdağ, A.İ. (2010). Bilişim Alanında Suçlar (Türk ve Alman Ceza Hukukunda). *GÜHFD*, 14 (2), 275-303.

Erdoğan, Y. (2012). Bilişim Sistemine Girme ve Kalma Suçu. *Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi*, 10 (Özel Sayı), 1363-1433.

Erem, F. (1991). Bilgisayar Suçları ve Türk Ceza Kanunu. *Yargıtay Dergisi*, 17 (4), 436-444.

Erol, H. (2010). *Türk Ceza Kanunu Gerekçeli ve Açıklamalı*. Ankara: Yayın Matbaacılık ve Ticaret İşletmesi.

Ersoy, Y. (1994). Genel Hukuki Koruma Çerçevesinde Bilişim Suçları. *AÜSBFD*, 49 (3-4), 149-183.

Esen, S. (2007). *Anlatımlı ve İçtihatlı Malvarlığına Karşı Suçlar Belgelerde Sahtecilik ve Bilişim Alanında Suçlar*. Ankara: Adalet Yayınevi.

Gözler, K. (2007). *İdare Hukukuna Giriş*. (7. Baskı). Bursa: Ekin Yayınevi.

Gül, A. (2016). *Doğrudan, Dolaylı Bilişim Suçları*. Ankara: Seçkin Yayınevi.

Hafızoğulları, Z. (1999). Fikir ve Sanat Eserlerinin Cezai Himayesi. *AÜHFD*, 48 (1), 1-14.

Hakeri, H. (2014). *Ceza Hukuku Genel Hükümler*. (17. Baskı). Ankara: Adalet Yayınevi.

Kaplan, Y. (2004). *İnternet Ortamında Fikri Hakların Korunmasına Uygulanacak Hukuk*. Ankara: Seçkin Yayınevi.

Karagülmez, A. (2009). *Bilişim Suçları ve Soruşturma - Kovuşturma Evreleri.* (2. Baskı). Ankara: Seçkin Yayınevi.

Karagülmez, A. (2010). Olması Gereken Hukuk Açısından Türk Ceza Kanununda Bilişim Sistemine Haksız Erişim Suçu. *TAAD,* 1 (3), 235-258.

Karakehya, H. (2009). Türk Ceza Kanunu'nda Bilişim Sistemine Girme Suçu. *TBB Dergisi*, (81), 1-24.

Katyal, N.K. (2001). Criminal Law in Cyberspace. *University Of Pennsylvania Law Review*, (149). 1003-1114.

Kaylan, K. (2004). Belgelerde Sahtecilik Suçları. T. Ergül (Ed.), *Türk Ceza Kanunu Reformu İkinci Kitap Makaleler, Görüşler, Raporlar* içinde (s. 163-184). Ankara: Türkiye Barolar Birliği Yayınları.

Ketizmen, M. (2008). *Türk Ceza Hukukunda Bilişim Suçları*. Ankara: Adalet Yayınevi.

Keyser**,** M. (2003). The Council Of Europe Convention On Cybercrıme. *Journal Transnational Law & Policy*, 12 (2), 287-326.

Koca, M. (2010). Yargıtay Kararları Işığında Bilişim Sistemleri Kullanılması Suretiyle Haksız Yarar Sağlama Suçları. *Prof. Dr. Ali Güzel'e Armağan,* 2. Cilt, 1651-1660.

Koca, M. ve Üzülmez, İ. (2016). *Türk Ceza Hukuku Özel Hükümler*. (3. Baskı). Ankara: Adalet Yayınevi.

Kurt, L. (2005). *Açıklamalı - İçtihatlı Tüm Yönleriyle Bilişim Suçları ve Türk Ceza Kanunundaki Uygulaması*. Ankara: Seçkin Yayınevi.

Mahmutoğlu, F.S. (2013). Türk Ceza Kanunu'nda Yer Alan Bilişim Alanındaki Suçlar ve Karşılaşılan Sorunların Yargı Kararları Işığında Değerlendirilmesi. *İÜHFM*. 71 (1), 855-889.

Oğuz, H. (2010). *İnternet Ortamında Kişilik Haklarının İhlali ve Korunması*. Ankara: Adalet Yayınevi.

Orer, G. (2011). *Elektronik İmza ve Elektronik Sertifika Hizmet Sağlayıcısının Hukuki ve Cezai Sorumluluğu*. Ankara: Adalet Yayınevi.

Orta, M. (2005). *Elektronik İmza ve Uygulaması*. Ankara: Seçkin Yayınevi.

Öngören, G. (2006). *İnternet Hukuku*. İstanbul: Öngören Hukuk Yayınları.

Özbek, V.Ö. (2007). Banka veya Kredi Kartlarının Kötüye Kullanılması Suçu (TCK m.245). *Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi*, 9 (Özel Sayı), 1019-1063.

Özbek, V.Ö., Doğan, K., Bacaksız, P. ve Tepe, İ. (2016). *Türk Ceza Hukuku Özel Hükümler*. (10. Baskı) Ankara: Seçkin Yayınevi.

Özdilek, A.O. (2002). *İnternet ve Hukuk*. İstanbul: Papatya Yayıncılık.

Özen, M. ve Baştürk, İ. (2011). *Bilişim - İnternet ve Ceza Hukuku*. Ankara: Adalet Yayınevi.

Öztürk, B. (2015). *Nazari ve Uygulamalı Ceza Muhakemesi Hukuku*. (9. Baskı). Ankara: Seçkin Yayınevi.

Pallı, H. (2008). *Türk Hukukunda ve Mukayeseli Hukukta Bilişim Suçları*. Yayımlanmamış Yüksek Lisans Tezi. Kayseri: Erciyes Üniversitesi.

Parlar, A. (2011). *Türk Ceza Hukukunda Bilişim Suçları*. Ankara: Bilge Yayınevi.

Sınar, H. (2001). *İnternet ve Ceza Hukuku*. İstanbul: Beta Yayınevi.

Sieber, U. (2013). Bilgisayar Suçluluğu. Y. Ünver (Ed.), *İnternet Hukuku*. (Çev: Y. Ünver), içinde (s. 13-57). Ankara: Seçkin Yayınevi.

Sieber, U. (2014). *İnternetteki Suçlar ve Suçun İnternette Takibi*. Y. Ünver (Ed.), Ankara: Seçkin Yayınevi.

Sokullu Akıncı, F. (2001). Avrupa Konseyi Siber Suç Sözleşmesinde Yer Alan Maddi Ceza Hukukuna İlişkin Düzenlemeler ve Özellikle İnternette Çocuk Pornografisi. *İÜHFM*. 59 (1-2), 11-38.

Soyaslan, D. (2012). *Ceza Hukuku Genel Hükümler*. (5. Baskı). Ankara: Yetkin Yayınevi.

Taner, F.G. (2007). Banka veya Kredi Kartlarının Kötüye Kullanılması Suçu Bileşik Suç mudur?. *AÜHFD*, 56 (2), 75-81.

Taşkın, Ş.C. (2008). *Bilişim Suçları*. İstanbul: Beta Yayınevi.

Tezcan, D., Erdem, M.R. ve Önok, R.M. (2017). *Teorik ve Pratik Ceza Özel Hukuku*. (14. Baskı). Ankara: Seçkin Yayınevi.

Topaloğlu, M. (2005). *Bilişim Hukuku*. Adana: Karahan Kitabevi.

Topaloğlu, N. (2014). Bilgisayar Mimarisi. H. Çakır ve M.S. Kılıç (Ed.), *Adli Bilişim ve Elektronik Deliller*. içinde (25-93). Ankara: Seçkin Yayınevi.

Toraman, C. (2002). Bankacılık Sektöründe İnternetin Yeri ve Türk Bankacılık Sistemi Uygulaması, *Kamu İş Hukuku ve İktisat Dergisi*, 6 (3),s. 1-13.

Toroslu, N. ve Ersoy, Y. (2004). Kanunlaşmaması Gereken Bir Tasarı. T. Ergül (Ed.),

Türk Ceza Kanunu Reformu İkinci Kitap Makaleler, Görüşler, Raporlar içinde (s. 1-20). Ankara: Türkiye Barolar Birliği Yayınları.

Ünver, Y. (2001). Türk Ceza Kanunu'nun ve Ceza Kanunu Tasarısının İnternet Açısından Değerlendirilmesi. *İÜHFM*, 59 (1-2), 51-153.

Ünver, Y. ve Hakeri, H. (2015). *Ceza Muhakemesi Hukuku*.(10. Baskı). Ankara: Adalet Yayınevi.

Yaman, D. (2010). Fikir ve Sanat Eserleri Kanununda Düzenlenen Bir Eserden Kaynak Göstermeksizin İktibasta Bulunma Suçu (m. 71/1-III). *DEÜHFD,* 12 (Özel Sayı), 1551- 1566.

Yaşar, O., Gökcan H.T. ve Artuç, M. (2010). *Yorumlu - Uygulamalı Türk Ceza Kanunu Cilt V Madde 205-256.* Ankara: Adalet Yayınevi.

Yavuz, L., Alıca, T. ve Merdivan, F. (2013). *Fikir ve Sanat Eserleri Kanunu Yorumu Cilt -II- (48-91. maddeler).* Ankara: Seçkin Yayınevi.

Yaycı, E. (2007). *Bilişim Suçları*. Yayımlanmamış Yüksek Lisans Tezi. Ankara: Gazi Üniversitesi.

Yazıcıoğlu, R.Y. (1997). *Bilgisayar Suçları Kriminolojik, Sosyolojik ve Hukuki Boyutları İle*. (1. Baskı). İstanbul: Alfa Yayınevi.

Yazıcıoğlu, R.Y. (2009). *Fikri Mülkiyet Hukukundan Kaynaklanan Suçlar*. İstanbul: XII Levha Yayıncılık.

Yenidünya, A.C. ve Değirmenci, O. (2003) *Mukayeseli Hukukta ve Türk Hukukunda Bilişim Suçları*. İstanbul: Legal Yayıncılık.

Yıldırım, M. F. ve Memiş, T. (2005). Elektronik Posta Kutusu Kullanımı ile İlgili Karşılaşılan Hukuki Sorunlar ve Çözüm Önerileri. *AÜEHFD*, 9 (3-4), 331-353.

Yıldız, M.E. (2011). *Banka veya Kredi Kartlarının Kötüye Kullanılması Suçu.* Yayımlanmamış Yüksek Lisans Tezi. İzmir: Dokuz Eylül Üniversitesi.

Yılmaz, S. (2010). Banka veya Kredi Kartlarının Kötüye Kullanılması Suçu. *TBB*

Dergisi, (87), 262-298.

Yılmaz, S. (2016). *Türk Ceza Hukuku Sisteminde Siber Suçlar*. Ankara: Adalet Yayınevi.

Yücel, M.T. (1992), Bilişim Suçları, *Ankara Barosu Dergisi*, (4), 505-512.

İnternet Kaynakları

http://www.tdk.gov.tr/index.php?option=com_gts&kelime=B%C4%B0L%C4%B0%C5%9E%C4%B0M (Erişim Tarihi: 05.04.2016)

http://www.ozgureralp.av.tr/web/makaleler/bilisim-suclari-turk-ceza-kanunu-madde-243-bilisim-sistemine-girme-2/ (Erişim Tarihi: 10.04.2016)

http://teknolojibilimmerkezi.tr.gg/dokuman-tr.htm (Erişim Tarihi: 18.05.2016)

http://www.mynet.com/haber/guncel/redhack-asti-ve-osmanlisporun-sitelerini-hackledi-1631129-1 (Erişim Tarihi: 01.06.2016)

http://www.milliyet.com.tr/50-milyon-kimlik-bilgisi-calindi--teknoloji-2221019/) (Erişim Tarihi: 01.06.2016)

http://arsiv.ntv.com.tr/news/263321.asp#BODY (Erişim Tarihi: 01.06.2016)

http://bilisim-kulubu.com/makale/ (Erişim Tarihi: 03.06.2016)

http://bidb.itu.edu.tr/seyirdefteri/blog/2013/09/07/vir%C3%BCs-solucan-ve-truva-at%C4%B1 (Erişim Tarihi: 03.06.2016)

https://www.itu.int/osg/spu/visions/papers/securitypaper.pdf(Erişim Tarihi: 03.07.2016)

http://www.emreeren.com/2005/10/bilgisayar-program-nedir.html (Erişim Tarihi: 03.07.2016)

http://stockton.usnwc.edu/ils/vol76/iss1/10/ (Erişim Tarihi: 03.07.2016)

https://www.tbmm.gov.tr/sirasayi/donem22/yil01/ss333m.htm (Erişim Tarihi: 22.07.2016)

https://tr.wikipedia.org/wiki/Veri (Erişim 15.12.2016)

http://tdk.gov.tr/index.php?option=com_bts&arama=kelime&guid=TDK.GTS.5887ba402a8c24.09321679 (Erişim Tarihi: 24.01.2017)

http://tdk.gov.tr/index.php?option=com_bts&arama=kelime&guid=TDK.GTS.5887b987b91361.91400854 (Erişim Tarihi: 24.01.2017)

http://bidb.itu.edu.tr/seyirdefteri/blog/2013/09/07/internet'in-tarih%C3%A7esi (Erişim Tarihi: 26.01.2017)

http://kelimeler.net/BİLİŞİM-kelimesinin-anlami-nedir (Erişim Tarihi: 15.05.2017)

http://novellaqalive2.mhhe.com/sites/dl/free/0073195553/462568/Chapter14.pdf (Erişim Tarihi: 16.05.2017)

http://www.sertels.av.tr/avukat/hukuk/bilişim-hukuku/yeni-bilişim-suçları-zararli-yazilim-veri-izleme.html (Erişim Tarihi: 10/07/2017)

http://arsiv.ntv.com.tr/news/195214.asp#BODY (Erişim Tarihi: 06.08.2017)

Mahkeme Kararları

Yargıtay Ceza Genel Kurulu'nun 17.11.2009 tarih ve 2009/11-193 Esas ve 2009/268 Karar sayılı kararı.

Yargıtay Ceza Genel Kurulu'nun 30.03.2010 Tarih ve 2010/11-17 Esas ve 2010/65 Karar Sayılı Kararı

Yargıtay Ceza Genel Kurulu'nun 18.10.2011 tarih ve 2011/6-166 Esas ve 2011/213 Karar sayılı kararı.

Yargıtay 8. Ceza Dairesi'nin 31.03.2014 tarih ve 2014/2161 Esas ve 2014/8038 Karar sayılı kararı.

Yargıtay 8. Ceza Dairesi'nin 07.04.2014 tarih ve 2013/3214 Esas ve 2014/8845 Karar sayılı kararı.

Yargıtay 8. Ceza Dairesi'nin 08.04.2014 tarih ve 2014/33371 Esas ve 2015/15859 Karar sayılı kararı.

Yargıtay 8. Ceza Dairesi'nin 16.04.2014 tarih ve 2013/11662 Esas ve 2014/9785 Karar sayılı kararı.

Yargıtay 8. Ceza Dairesi'nin 14.05.2014 tarih ve 2013/4675 Esas ve 2014/12406 Karar sayılı kararı.

Yargıtay 8. Ceza Dairesi'nin 09.06.2014 tarih ve 2014/5592 Esas ve 2014/14132 Karar sayılı kararı.

Yargıtay 8. Ceza Dairesi'nin 22.09.2014 tarih ve 2014/6182 Esas ve 2014/20376 Karar sayılı kararı

Yargıtay 8. Ceza Dairesi'nin 16.10.2014 tarih ve 2013/12964 Esas ve 2014/22580 Karar sayılı kararı.

Yargıtay 8. Ceza Dairesi'nin 13.11.2014 tarih ve 2014/20966 Esas ve 2014/26063 Karar sayılı kararı.

Yargıtay 8. Ceza Dairesi'nin 18.03.2015 tarih ve 2014/30051 Esas ve 2015/13973 Karar sayılı kararı.

Yargıtay 8. Ceza Dairesi'nin 02.06.2015 tarih ve 2014/37839 Esas ve 2015/18101 Karar sayılı kararı.

Yargıtay 8. Ceza Dairesi'nin 10.09.2015 tarih ve 2014/35013 Esas ve 2015/21341 Karar sayılı kararı.

Yargıtay 8. Ceza Dairesi'nin 14.10.2015 tarih ve 2015/3445 Esas ve 2015/22717 Karar sayılı kararı.

Yargıtay 8. Ceza Dairesi'nin 18.11.2015 tarih ve 2015/7531 Esas ve 2015/24704 Karar sayılı kararı.

Yargıtay 8. Ceza Dairesi'nin 18.11.2015 tarih ve 2015/11682 Esas ve 2015/24706 Karar sayılı kararı.

Yargıtay 8. Ceza Dairesi'nin 11.12.2015 tarih ve 2015/9842 Esas ve 2015/25682 Karar sayılı kararı.

Yargıtay 8. Ceza Dairesi'nin 08.02.2016 tarih ve 2015/12565 Esas ve 2016/1121 Karar sayılı kararı.

Yargıtay 8. Ceza Dairesi'nin 29.03.2016 tarih ve 2016/1881 Esas ve 2016/4107 Karar sayılı kararı.

Yargıtay 8. Ceza Dairesi'nin 04.04.2016 tarih ve 2016/1781 Esas ve 2016/4371 Karar sayılı kararı.

Yargıtay 8. Ceza Dairesi'nin 12.04.2016 tarih ve 2015/14782 Esas ve 2016/4928 Karar Sayılı kararı.

Yargıtay 8. Ceza Dairesi'nin 19.04.2016 tarih ve 2015/9501 Esas ve 2016/5237 Karar sayılı kararı.

Yargıtay 8. Ceza Dairesi'nin 21.06.2016 tarih ve 2016/3802 Esas ve 2016/8259 Karar sayılı kararı.
Yargıtay 8. Ceza Dairesi'nin 23.06.2016 Tarih ve 2016/4589 Esas ve 2016/8439 Karar Sayılı kararı.
Yargıtay 8. Ceza Dairesi'nin 23.11.2016 tarih ve 2016/6436 Esas ve 2016/ 10698 Karar sayılı kararı.
Yargıtay 8. Ceza Dairesi'nin 21.02.2017 tarih ve 2016/10914 Esas ve 2017/1618 Karar sayılı kararı.
Yargıtay 11. Ceza Dairesi'nin 20.02.2008 tarih ve 2007/8458 Esas ve 2008/915 Karar sayılı kararı.
Yargıtay 11. Ceza Dairesi'nin 28.05.2009 tarih ve 2009/3019 Esas ve 2009/6644 Karar sayılı kararı.
Yargıtay 11. Ceza Dairesi'nin 19.11.2015 tarih ve 2013/25561 Esas ve 2015/31099 karar sayılı kararı.
Yargıtay 11. Ceza Dairesi'nin 18.04.2016 tarih ve 2016/1332 Esas ve 2016/3310 Karar sayılı kararı.
Yargıtay 13. Ceza Dairesi'nin 06.06.2016 tarih ve 2015/2174 Esas ve 2016/10469 Karar Sayılı kararı.