

# TÜRK CEZA KANUNUNDA YER ALAN BİLİŞİM ALANINDAKİ SUÇLAR VE KARŞILAŞILAN SORUNLARIN YARGI KARARLARI İŞİĞİNDA DEĞERLENDİRİLMESİ

Prof. Dr. Fatih Selami Mahmutođlu\*

## I. GENEL OLARAK

Teknolojik gelişmeler birçok alanı olduđu gibi bilişim alanını da etkilemiş özellikle de bu ortamda ya da yolla işlenen suçların niteliđi geređi yeniden gözden geçirilmesine neden olmuştur. Kanunlarımızda anılan deđişimlere paralel olarak gerek 765 sayılı Türk Ceza Kanunu döneminde, gerekse 5237 sayılı Türk Ceza Kanunu'nun hazırlanmasında, bilişim sistemlerine karşı veya bilişim sistemlerinin araç olarak kullanıldıđı suç tiplerini düzenleyen bazı maddelere yer verilmiştir.

Kısaca göz atacak olursak, bilişim alanındaki suçlara ilişkin ilk düzenlemenin, 1991 yılında<sup>1</sup>, 3756 sayılı Kanun ile 765 sayılı Ceza Kanununun 11. babına ilave edilen "Bilişim Alanında Suçlar" başlıklı 525/a, b, c ve d maddeleri olduđu görölmektedir. Devamında ise 01.06.2005 tarihli 5237 sayılı yeni Türk Ceza Kanununda bilişim suçları ile ilgili olarak birtakım suçlara yer vermiştir<sup>2</sup>.

---

\* İstanbul Üniversitesi Hukuk Fakültesi Ceza ve Ceza Usul Hukuku A. B. D.Öğretim Üyesi

<sup>1</sup> Bu dönem hakkında bilgi için bkz: DÖNMEZER Sulhi, **Kişilere ve Mala Karşı Cürümler**, İstanbul, 1998, s.520 vd.; ÖNDER Ayhan, **Şahıslara ve Mala Karşı Cürümler ve Bilişim Alanında Suçlar**, İstanbul, 1994, s.506 vd.; ÜNVER Yener, **Türk Ceza Kanunu'nun ve Ceza Kanunu Tasarısının İnternet Açısından Deđerlendirilmesi**, İÜHF, C.LIX, S.1-2, 2001, s.51 vd., 126.

<sup>2</sup> Bu tür suçlar mukayeseli hukukta da karşımıza çıkmaktadır. Örneđin, İngiltere'de bilişim suçları ayrı bir düzenleme ile ihdas edilmiştir. Bilgisayarın Kötüye Kullanılması Kanunu bu konudaki özel kanundur. 29 Haziran 1990 tarihli ve Computer Misuse Act (CMA) adlı kanun ile yetkisiz şekilde bilgisayarlara girmek, sistem içerisinde deđişiklik yapmak veya benzeri müdahalelerde bulunmak, bilişim sistemini kasten veya taksirle bozma, zarar verme suç olarak öngörölmüştür. Söz konusu kanunda bilişime ilişkin diđer bir suç tipi, amaç suçları işlemek amacıyla bilişim sistemine girmek olarak belirtilmiştir. Bunun dışında devlet kamu kurumlarına ya da askeri kuruluşlara ait bilişim sistemlerine zarar veren failin, İngiltere'de terör şüpheli statüsünde izlemeye alındıđı ve bu eylemlere karıştıđı belirlenirse Terörle Mücadele Kanunu'ndan yargılandıđı ifade edilmektedir. ERALP Özgür, "Bilişim Suçları," [http://www.ozgureralp.av.tr/makaleler/bilimsuclari\\_sistemi\\_engelleme\\_244.html](http://www.ozgureralp.av.tr/makaleler/bilimsuclari_sistemi_engelleme_244.html), (Erişim Tarihi: 16. 03. 2012). Alman Hukuku'nda ise, bilişim suçları ayrı bir kanunla deđil, Alman Ceza Kanunu/Strafgesetzbuch (StGB) içerisinde düzenlenmiştir. Alman Ceza Kanunu bilişim suçlarına deđişik bölümlerde şu başlıklarla yer vermiştir. §202 a Veri Casusluđu, § 202 b Verilerin İletirken Ele Geçirilmesi, § 202 c Veri Casusluđunun ve Verilerin İletirken Ele Geçirilmesinin Hazırlıđı, § 263 a Bilgisayar Dolandırıcılıđı, § 266 b Çek Kartının ve Kredi Kartının Kötüye Kullanılması, § 268 Teknik Kayıtlarda Sahtecilik, § 269 İspat Açısından Önemli Verilerde Sahtecilik, § 270 Bilgi İşlem Alanında Hukuki İşlemlerde Aldatma, § 303 a Verilerin Deđiştirilmesi, § 303 b Bilgisayara Sabotaj, § 303 c Şikâyet. § 01.03.2003 tarihli Fransız Ceza Kanunu ile bilişim suçları düzenleme altına

Bu suçları; **1-** Sadece bilişim sisteminin kullanılmasıyla işlenebilen suçlar (doğrudan ya da dar anlamda veyahut gerçek bilişim suçları), **2-** Bilişim sisteminin kullanılması zorunlu olmamakla birlikte, bazı suçların nitelikli hali olan suçlar ve **3-** Kanunda bu sistemin kullanılması zorunlu olmamakla birlikte, söz konusu sistemin suçta vasıta olarak kullanıldığı suçlar, şeklinde ayrımlara tabi tutabiliriz.

Buna göre; **sadece bilişim sisteminin kullanılmasıyla işlenebilenler;** Bilişim Sistemine Girme (TCK md.243), Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme (TCK md.244), Banka ve Kredi Kartlarının Kötüye Kullanılması (TCK md.245), **bilişim sisteminin kullanılması zorunlu olmamakla birlikte, bazı suçların nitelikli hali olanlar;** Hırsızlık (TCK md. 142/2-e) ve Dolandırıcılık (TCK md. 158/1-f), **bu sistemin kullanılması zorunlu olmakla birlikte söz konusu sistemin suçta vasıta olabileceği suçlar ise;** Haberleşmenin Gizliliğini İhlal (TCK md. 132), Haberleşmenin Engellenmesi (md. 124), Eğitim ve Öğretimin Engellenmesi (md. 112), Kamu Kurumu veya Kamu Kurumu Niteliğindeki Meslek Kuruluşlarının Faaliyetlerinin Engellenmesi (TCK md. 113), Hakaret ve Sövme (TCK md. 125), Müstehcenlik (TCK md. 226), Kumar Oynanması İçin Yer ve İmkân Sağlanması (TCK md. 228), Suç İşlemeye Tahrik (TCK md. 214), Cinsel Taciz (TCK md. 105) gibi suçlardır.

Çalışmamızda sadece bilişim sisteminin kullanılmasıyla işlenen suçlar incelenecektir. Ancak yeri geldiği zaman diğer suçlarla olan ilişkisine de değinilecektir. Bu kapsamda, önce yasada kullanılan birtakım temel kavramların

---

alınmış ve yeni suç tipleri oluşturulmuştur. Bu kanunun II. babında III. faslı içindeki 323/1 ile 323/7 maddeleri arasında bilişim suçları düzenlenmektedir. Fransa Ceza Kanunu 323. maddesine göre; **1-** Verileri otomatik işleme tabi tutmuş sistemin bir kısmına kanuna aykırı olarak giren veya orada kalmaya devam eden 1 yıl'ı geçmemek üzere hapis ve 100.000 Frank'a kadar para cezasına çarptırılır. Eğer sistemdeki veri veya sistemin fonksiyonları değiştirilirse, 2 yıl'ı geçmemek üzere hapis cezası ve 200.000 Frank'a kadar para cezası verilir. **2-** Verileri otomatik işleme tabi tutmuş sistemin fonksiyonlarını bozan veya bunların işlemlerini zorlaştıranlar 3 yıl'ı geçmemek üzere hapis ve 300.000 Frank'a kadar para cezasına çarptırılırlar. **3-** Verileri otomatik işleme tabi tutan bir sisteme hile ile veriler sokan veya sistemin içerdiği verileri hile ile imha eden veya değiştiren kişiye 3 yıl hapis ve 300.000 Frank para cezası verilir. **4-** Oluşturulan bir gruba veya manevi hazırlık anlaşmasına katılımla 323/1 ile 323/2 fıkralarında düzenlenen bir veya daha fazla suçun işlenmesi halinde ceza en ağırından verilir. Fransız Ceza Kanunu'nun da 226/16 ile 226-24 maddelerinde bilişim sistemleri aracılığı ile kişilik haklarına yapılan saldırılar düzenlenmiştir. Bu Kanun'un 277/3 Maddesi ile küçüklerin resminin pornografik amaçla kullanılması, 227/24 maddesi ile ise küçükler tarafından erişilebilecek şiddet ya da pornografi içeren mesaj yayınlanması suç haline getirilmiştir. Bilişim suçları konusunda önem arz eden kanunlardan en önemlilerinden biri 05.01.1988 tarihli 88-19 sayılı Kanun olup, bu kanun ile bilişim suçları ceza kanunu içinde değerlendirilmeye başlanmıştır, bilişim suçlarıyla mücadele amacıyla devletin birden fazla kurumunda özel birimler kurulmuştur. Bunlar; a. Başbakan'a bağlı Milli Savunma Genel Sekreterliği (SGDN)bünyesinde kurulan Haberleşme Sistemleri Güvenliği Merkez Birimi (DCSSI) b. Haberleşme Teknolojisi kullanılarak yapılan dolandırıcılıkların soruşturulması birimi (SEFTI) c. Bilgisayar ortamında işlenen suçların bastırılması birimi (BCRCI) d. Jandarma Genel Komutanlığı Seç Araştırmaları Enstitüsü (IRCGN) e. Fransız İstihbarat Örgütü (DST) f. İletişim ve Enformasyon ve Teknolojilerinin Kullanımı Suretiyle İşlenen Suçlarla Mücadele Bürosu'dur. Schjolberg, Stein, <http://www.mosstingrett.no/info/legal.html>, 31.08.2006; Aktaran: DEMİRCAN Tunç, **Bilişim Alanında Suçlar**, yayınlanmamış yüksek lisans tezi, Konya, 2007, s.38.

açıklanmasından sonra, bilişim suçları tüm unsurlarıyla ele alınacaktır. Devamında ise Yargıtay kararları ışığında bunların benzer diğer suç tipleriyle karşılaştırması yapılacaktır.

## II. KANUNDA YER VERİLEN BAZI KAVRAMLAR

Türk Ceza Kanunu'ndaki bilişim suçlarına geçmeden Türk Ceza Kanunu'nda yer almayan ya da yer alan ancak tanımlanmayan bazı kavramları ortaya koymak gerekir.

**Veri;** Avrupa Konseyi Siber Suç Sözleşmesi md. 1' de; *“bir bilgisayar sisteminin belli bir işlevi yerine getirmesini sağlayan yazılımlar da dâhil olmak üzere, bir bilgisayar sisteminde işlenmeye uygun nitelikteki her türlü bilgi”*, 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun'un tanımlar başlıklı 2. maddesinde ise; *“bilgisayar tarafından üzerinde işlem yapılabilen her türlü değer”* olarak tanımlanmaktadır<sup>3</sup>. Bilişim sistemi veri üzerine işlem yapmaktadır. Amacı ise verileri işlemek, saklamak ve bu verilerden sonuç çıkarmaktır<sup>4</sup>. Kısaca verinin bilişim sisteminin temelini oluşturan ve bu sistemde kullanılan her şey olduğu söylenebilir<sup>5</sup>.

**Bilişim sistemi;** verileri toplayıp yerleştirdikten sonra bunları otomatik olarak işleme tabi tutma olanağı veren manyetik sistemlerdir.

**Banka Kartı;** 5464 sayılı Banka ve Kredi Kartları Kanunu md.3'te kartın hamiline ait mevduat hesabı ile özel cari hesapların kullanımı dâhil bankacılık hizmetlerinden yararlanmayı sağlamak üzerine çıkarılan kart olarak tanımlanmıştır. Buna göre banka kartı bankada bulunan bir mevduat veya cari hesaba bağlı olarak çıkarılan ve bu hesapların kullanımını da kapsayan bankacılık faaliyetlerinin yapılabilmesini sağlayan bir araçtır.

**Kredi Kartı;** Banka kartı gibi kredi kartı da 5464 sayılı Banka ve Kredi Kartları Kanunu'nun 3. maddesinde tanımlanmıştır. Bu maddeye göre, nakit kullanımı gerekmeksizin mal ve hizmet alımı veya nakit çekme olanağı sağlayan basılı kartı veya fiziki varlığı bulunmayan kart numarasını ifade eder. Kart hamili nakit kullanmaksızın alışveriş yapabilmektedir. Banka kartı ile bu yönde benzeşmektedir. Zira artık gelişen teknoloji ile birlikte banka kartları ile de alışveriş yapılmaktadır. Ancak kredi kartında önemli olan kart numarasıdır. Basılı fiziki varlığının olmasına gerek yoktur. Bu yönüyle de banka kartından ayrılmaktadır.

**Kartlı sistem kuruluşu;** Banka kartı veya kredi kartı sistemi kuran ve bu sisteme göre kart çıkarma veya üye işyeri anlaşması yapma yetkisi veren kuruluşlardır.

**Kart çıkaran kuruluş;** Banka kartı veya kredi kartı düzenleme yetkisine sahip bankalar ile diğer kuruluşlardır.

<sup>3</sup> Kavram hakkında bilgi için bakınız; DÜLGER Murat Volkan, **Bilişim Suçları**, Ankara, 2004; s.45-48; ÖNGÖREN Gürsel, **İnternet Hukuku**, İstanbul, 2006, s.49

<sup>4</sup> YENİDÜNYA Caner, DEĞİRMENCİ Olgun, **Mukayeseli Hukukta ve Türk Hukukunda Bilişim Suçları**, İstanbul, 2003, s.47

<sup>5</sup> *“Bilişim sisteminde saklanan her şey (bir yazı, bir resim, bir program) veridir.”* YENİDÜNYA/DEĞİRMENCİ, Mukayeseli Hukukta..., s.48

**Kart hamili;** Banka kartı veya kredi kartı hizmetlerinden yararlanan gerçek veya tüzel kişiyi ifade eder.

### III. TÜRK CEZA KANUNUNDAKİ BİLİŞİM SUÇLARI

#### A. BİLİŞİM SİSTEMİNE GİRME (TCK md.243)

Bilişim Sistemine Girme Suçu, 5237 sayılı TCK'nın ikinci kitabının, topluma karşı suçlara yer veren üçüncü kısmının, "*Bilişim Alanında Suçlar*"<sup>6</sup> başlıklı onuncu bölümünde, md.243'te düzenlenmiştir<sup>7</sup>. Temel olarak bu hükümlerle, bir bilişim sisteminin bütününe veya bir kısmına hukuka aykırı olarak girme ve<sup>8</sup> orada kalmaya devam etme fiili, yaptırım altına alınmıştır.

#### 1. Suçla Korunan Hukuksal Yarar

Gelişen teknolojiyle bağlantılı olarak, bilişim sistemleri aracılığıyla yapılan işlemlerin sayısı her geçen gün artmaktadır. Ancak söz konusu sistemlerin tercih edilebilmesi için kişilerde bunlara yönelik güven fikrinin tam olması gerekmektedir. Yasa koyucu da, bilişim sistemine girme suçu ile bunu esas alarak, bilişim sisteminin güvenliğini<sup>9</sup> koruma altına almıştır<sup>10</sup>. Aslında güvenliğin

<sup>6</sup> Bu bölüm başlığı, TBMM Adalet Komisyonunda "Bilişim Sistemlerine Karşı Suçlar" olarak kabul edilmiştir. Ancak, TBMM Genel Kurulunda verilen bir önerge üzerine, bölüm başlığı, Hükümet Tasarısında olduğu gibi, "Bilişim Alanında Suçlar" olarak değiştirilmiştir.

"*Bilişim Sistemlerine Karşı Suçlar*" başlığı, bilişim suçlarının sadece bilişim sistemlerine karşı suçları ihtiva ettiğini düşündürmesi bakımından yerinde değildir. Nitekim bilişim suçları hem bilişim sistemlerine karşı suçları, hem de bilişim sistemleri kullanılarak işlenen suçları ifade etmektedir. Bu bakımdan kanun tasarısından ayrılmasını yerinde bulmaktayız." DEĞİRMENCİ Olgun, **2004 Türk Ceza Kanunu'nun Bilişim Suçları Bakımından Değerlendirilmesi**, TBB Dergisi, Sayı:58, Mayıs/Haziran 2005 s.198; Aynı görüş için ayrıca bkz, YAZICIOĞLU Yılmaz, **Bilişim Suçları**, HPD Hukuki Yorum ve Haber Dergisi, Sayı:2, 2004, s.142-143.

<sup>7</sup> Alman Ceza Kanunu StGB'de bizdeki 243'e yakın suç, 292a ve 292b maddeleriyle "özel hayat ve sır alanının ihlali" bölümünde ve yazışarak haberleşme sırlarının ihlali (m.202 Verletzung des Briefgeheimnisse) kapsamında yaptırım altına alınmıştır. "Alm. CK'nın bizdeki 243. madde düzenlemesine karşılık gelen ve

Bilgisayar Ceza Hukuku'nun çekirdek hükmü olan 202a maddesi düzenlemesinin 243'e göre özellik arz eden farkları, bilişim sistemine girme veya erişim yerine verilere ulaşım veya erişimin yolunu açmaktan bahsetmesi ve suçun meydana gelmesi için orada kalmayı aramayı sadece verilere erişimin önünün açılmasını yeterli saymasıdır." ERDAĞ Ali İhsan, **Bilişim Alanında Suçlar (Türk ve Alman Ceza Hukukunda)**, Gazi Üniversitesi Hukuk Fakültesi Dergisi, C.XIV, Y:2010, Sayı:2, s.287.

<sup>8</sup> TCK 243. maddenin ilk halinde, buradaki "ve" bağlacı "veya" şeklindeydi. TBMM Genel Kurulunda yapılan görüşmeler ile değiştirilerek "ve" halini almıştır.

<sup>9</sup> Doktrinde bir görüşe göre, suçun maddi unsurlarından olan bilişim sisteminde kalmaya devam etme gerekçe gösterilerek korunan hukuki değer in sistem güvenliğinden ziyade bilişim sistemini kullananların belirli bir süreden sonra rahatsız edilmemesi olduğu ifade edilmiştir. (KARAGÜLMEZ Ali, **Bilişim Suçları ve Soruşturma-Kovuşturma Evreleri**, 2.bası, Ankara, 2011, s.179-180). Kanaatimizce salt rahatsız edilmeme suçla korunan hukuki değer bakımından oldukça dar bir anlam ifade eder. Bu suçla birden fazla hukuki değer korunduğu için bilişim sistemini kullanan kişilerin rahatsız edilmemesi korunan hukuki değerlerden sadece bir tanesini oluşturmaktadır.

<sup>10</sup> AKINCI Füsun Sokullu, **Avrupa Konseyi Siber Suç Sözleşmesinde Yer Alan Maddi Ceza Hukukuna İlişkin Düzenlemeler ve Özellikle İnternette Çocuk Pornografisi**, ÜHFMC., Cilt:LIX, Sayı:1-2, 2001, s.14; DÜLGER, Bilişim Suçları, s.214; MERAN Ne-

sağlanmasına yönelik amacın yanı sıra daha sonra oluşabilecek hırsızlık ve dolandırıcılık suçlarının da engellenmesi hedeflenmektedir<sup>11</sup>.

Diğer taraftan bir sisteme hukuka aykırı olarak girilmesi ve orada kalınması ile sistem maliki veya kullanıcısının özel hayatının gizliliği veya dokunulmazlığı<sup>12</sup>, sırlarının masumiyeti<sup>13</sup>, haberleşme hürriyeti<sup>14</sup> gibi farklı türdeki birçok hakkının da ihlali gündeme gelebilir. Söz konusu yasal düzenlemeyle, kişilerin hak ihlallerinin de önüne geçilmek istenmiştir<sup>15</sup>. Bu verilerden hareketle anılan suç tipi ile birden fazla hukuki degerin korunmakta olduğunu söyleyebiliriz.

## **2. Maddi Unsurlar**

### **a. Fail**

Kanuni düzenlemede suç işleyecek kişiyle ilgili “kimse” sözcüğü kullanılarak, herhangi bir özellik belirtilmemiştir. Bu nedenle anılan suç herkes tarafından işlenebilir<sup>16</sup>.

Söz konusu suç gerçek kişilerin yanı sıra, bir tüzel kişi yararına haksız menfaat sağlamak için de işlenebilir. Böyle bir durumda, TCK md.60’a göre bunlar bakımından güvenlik tedbirlerinin uygulanması mümkün olabilecektir<sup>17</sup>.

### **b. Mağdur**

Bilişim Sistemine Girme Suçu, mağduru bakımından bir özellik göstermemektedir. Bu nedenle bu suçun mağduru hukuka aykırı şekilde kısmen veya tamamen girilen ve kalınmaya devam edilen sistemin maliki veya kullanıcısı olan herkes olabilir. Suç dolayısıyla birden fazla kişinin hakkı ihlal edildiğinde, hakları ihlal edilen kişilerin her biri mağdurdur<sup>18</sup>.

---

cati, **Yeni Türk Ceza Kanununda Sahtecilik - Malvarlığı Bilişim Suçları İle Ekonomi Ve Ticaret Alanında Suçlar**, Ankara, 2005, s.363

<sup>11</sup> ARTUK Mehmet Emin, GÖKCEN Ahmet, YENİDÜNYA Caner, **Türk Ceza Kanunu Şerhi, Özel Hükümler**, Ankara, 2009, s.4630

<sup>12</sup> PARLAR Ali, **Türk Ceza Hukukunda Bilişim Suçları**, Ankara, 2011, s.15

<sup>13</sup> ARTUK/GÖKCEN/YENİDÜNYA, **Türk Ceza...**, s. 4630

<sup>14</sup> YAŞAR Osman, GÖKCEN Hasan Tahsin, ARTUÇ Mustafa, **Yorumlu Uygulamalı Türk Ceza Kanunu**, Ankara, 2010, s.6738.

<sup>15</sup> Aksi görüş için bkz:KETİZMEN Muammer, **Türk Ceza Hukukunda Bilişim Suçları**, Ankara, 2008, s.99

<sup>16</sup> Ancak profesyonellik bahis konusu olduğunda, uygulamaya yansıdığı yabancı terminolojiyle akla ilk gelen hacker ve cracker kavramlarıdır. Bunları kısaca açıklamak gerekirse; hacker “bölmek, kesip atmak, yontmak, becermek” anlamlarına gelen İngilizce “hack” fiilinden türetilmiştir. Hackerlar “sahip bulunduğu teknolojik aygıtlarla bir bilişim sistemine kişisel verileri elde etmek veya sahtecilik, dolandırıcılık gibi çeşitli suçları işlemek için hukuka aykırı olarak erişebilen kimselerdir”. Cracker ise Türkçede “kırmak, açmak” manasına gelen crack fiilinden türetilmiştir. Crackerların teknolojik bilgi seviyeleri hackerlara oranla daha üst seviyededir. Bu nedenle, bunların faaliyetleri hackerlara göre daha tahrip edicidir. Ayrıca temel olarak hackerlar ilkeli, crackerler ise ilkesiz davranışlar içerisindeyler. ARTUK/GÖKCEN/YENİDÜNYA, **Türk Ceza...**, s.4638-4639.

<sup>17</sup> Tüzel Kişilerin cezai sorumluluğu hakkında genel bilgi için bkz; KANGAL Zeynel, **Tüzel Kişilerin Ceza Sorumluluğu**, Ankara, 2003

<sup>18</sup> “Bir bankanın bilişim sistemine girerek, müşteri bilgilerinin incelenmesi durumunda, bilgileri incelenen her bir müşteri suçun mağduru olduğu gibi, bankanın tüzel kişiliği de suçtan zarar gören durumdadır.” Bunların dışında bir kimse, kişisel dosyasını arkadaşının bilgisayarında muhafaza ettiğinde ve bu sisteme hukuka aykırı şekilde

Tüzel kişiler bakımından hak ihlalleri oluştuğunda ise, bunlar hakkında suçtan zarar gören sıfatını kullanmak gerekecektir<sup>19</sup>.

### c. Fil

Suçun maddi unsuru, hangi yolla olursa olsun bir bilişim sisteminin bütününe veya bir kısmına hukuka aykırı şekilde girmek ve<sup>20</sup> orada kalmaya devam etmektir<sup>21</sup>. Bu nedenle suçun oluşması için sadece bilişim sistemine girmek yeterli değildir. Belirli bir süre sistemde kalmaya devam etmek de gerekir<sup>22</sup>. Görüldüğü üzere, girmek ve kalmak şeklinde biri icrai, diğeri ise ihmali iki hareketin bir arada oluşması gerekliliği nedeniyle bu suç, çok hareketli bir suçtur. Ayrıca fiilin icrası sürdüğü için kesintisiz (mütemadi) niteliktedir<sup>23</sup>.

Maddede bahsi geçen "girmek" fiilinden kastedilen; bir bilişim sisteminin tamamına ya da bir parçasına ulaşmak, içeriğine dâhil olmaktır<sup>24</sup>. Daha teknik

---

ulaşılıp giriş yapıldığında, hem bilgisayar sahibi hem de veri sahibi suçun mağduru olacaktır. ARTUK/GÖKCEN/YENİDÜNYA, Türk Ceza..., s.4639, 4640; YAŞAR/GÖKCAN/ARTUÇ, Yorumlu Uygulamalı..., s.6739

<sup>19</sup> Ancak *Meran*, tüzel kişinin bu suçun mağduru olabileceğini kabul etmektedir. (MERAN, Yeni Türk Ceza..., s.364)

<sup>20</sup> "Avrupa Konseyi Siber Suç Sözleşmesinin 2. maddesinde, bilişim sistemine hukuka aykırı erişim, suçun oluşması için yeterli sayılmış, failin ayrıca burada kalmaya devam etmesi aranmamıştır. Mukayeseli hukukta genel eğilim bu yöndedir. Bu itibarla TCK'nın "hukuka aykırı erişimi" suçun oluşması bakımından yeterli saymaması yerinde olmamıştır. Bilişim sistemlerinden haksız kazanç elde etmek isteyen kişiler, bu düzenleme sayesinde hiçbir yaptırma maruz kalmaksızın istedikleri kadar bilişim sistemlerine girecek, amaç suçları gerçekleştirmek konusunda daha elverişli imkân ve ortama sahip olacaklardır. Örneğin, bankaların güvenlik kodlarını, şifrelerini kırmak suretiyle bilişim sistemlerine girmek suç teşkil etmeyecektir." (ARTUK/GÖKCEN/ YENİDÜNYA, Türk Ceza..., s, 4632-4633; MAHMUTOĞLU Fatih Selami, Karşılaştırmalı Hukuk Bakımından İnternet Sujelerinin Ceza Sorumluluğu, ÜHFM, Cilt:LIX, Sayı:1-2, İstanbul, 2001, s.39-51)

<sup>21</sup> 765 sayılı TCK ile bir karşılaştırma yaptığımızda, TCK md. 525/a ilgili düzenlemeyle benzer gibi gözüktüğü, ancak birtakım farklılıklar içerdiği, bu nedenle de aslında söz konusu suçun eski yasada tam bir karşılığının olmadığı anlaşılmaktadır. Çünkü 765 sayılı TCK md. 525/a'da düzenlenen suçun oluşabilmesi için, verilerin ele geçirilmesi<sup>21</sup> gerekmektedir. TCK md. 243 bakımından ise eski yasadaki -verileri ele geçirme- şartı aranmaksızın, sisteme hukuka aykırı girme ve orada kalmaya devam etme hareketleri suçun oluşması açısından yeterlidir. Bu suretle de, diyebiliriz ki, bilişim sistemine girme ve orada kalmaya devam etme, 5237 sayılı TCK ile getirilen yeni bir suç tipidir.

<sup>22</sup> ÖNGÖREN, İnternet Hukuku, s.46

<sup>23</sup> Suçun işlendiği yerin tespiti ise bazı ihtimallerde oldukça karmaşık gözükmektedir. Ortada fiziksel temasla bilişim sistemine girme varsa eylem nerede yapılmışsa, suç orada işlenmiş sayılacaktır. Ancak, bilişim sistemine bir ağ aracılığı ile girilmesi durumunda, suçun araç bilişim sisteminin bulunduğu yerde mi, yoksa hedef bilişim sisteminin bulunduğu yerde mi işlenmiş sayılacağı noktasında ortaya çıkacaktır. Hatta bunlardan birinin yurtiçinde, diğerinin yurtdışında olması halinde, tartışma daha da farklı boyutlara sürüklenecektir. Bizce bu tür suçlarda hem sisteme girilen araç bilişim sisteminin olduğu yer hem de hedef sistemin bulunduğu yer suçun işlendiği yer olarak kabul edilebilir.

Ayrıca hedef ile araç bilişim sisteminin farklı ülkelerde bulunması, suçun işlendiği yer dışında, yetki sorunlarını da beraberinde getirecektir. Bu konuda da yine suçun işlendiği yerin tespitine ilişkin getirmiş olduğumuz çözüm kabul edilebilir. Bu durumda birden fazla yetki söz konusu olacaktır.

<sup>24</sup> "Hareketin gerçekleştirilmesi bakımından herhangi bir sınırlama da söz konusu değildir. Bu konuda çeşitli ihtimaller düşünülebilir. İlk olarak, bilişim sistemine ağ üzerinden ulaşılarak veri, program veya diğer unsurlar ele geçirilebilir. İkinci olarak, sisteme

bir anlatımla sanal bir alana erişmektir<sup>25</sup>. Bu erişim, bir kimsenin emanet ettiği bilgisayarın açılması ve içindeki verilerin gönderilmesi<sup>26</sup> şeklinde gerçekleşebileceği gibi kamusal veya yerel telekomünikasyon ağları yoluyla veya internet üzerinde bir bilgisayar sistemiyle de gerçekleşebilir<sup>27</sup>. Erişimde, bağlantının kablolulu-kablosuz olması, mesafenin yakınlığı-uzaklığı suçun oluşumunda etkili değildir. Sisteme e-posta mesajı ya da dosya gönderilmesi durumunda ise bilişim sistemine girme değil, veri gönderme söz konusu olduğundan, girmeden söz edilemeyecektir<sup>28</sup>. Ancak gönderilen dosyanın içinde yer alan programlar aracılığıyla bilişim sistemine girmek mümkün ise bu durumda da bilişim sistemine girmeden bahsedebiliriz. Bu durumda mail yoluyla gönderilen dosyayı alan kişinin bu dosyayı açmaması halinde ise teşebbüs tartışması yapılacaktır.

“Kalmaya devam etmek” ise, “bilişim sisteminin bütününe veya bir kısmına giren failin, bu sanal ortamda eylemin ciddiliğini ortaya koyabilecek ölçüde bulunmasıdır”<sup>29</sup>. Söz konusu kavramın bu şekildeki izahı, akla, suçun gerçekleşmesi için failin başkasına ait bir sanal ortamda en az ne kadar süre bulunması gerektiği sorusunu getirmektedir. Ancak mevcut düzenlemede bu sorunun cevabı yer almamaktadır. Bizce burada dikkat edilmesi gereken kıstas, failin başkasına ait bir alana girdiğini fark etmesinin ardından, bu fiilini sonlandırması için yetecek sürede buradan uzaklaşıp uzaklaşmadığıdır<sup>30</sup>. Başka bir ifadeyle fail girmiş olduğu sistemden çıkması için gerekli olan (çıkarmayı olanaklı hale getiren<sup>31</sup>) sürede çıkmamışsa kalmaya devam etmiş olacaktır.

Bu bağlamda mağdurun zarara uğrayıp uğramadığının bir önemi yoktur. Böylelikle fail bilişim sistemine girip orada kalmasına rağmen, hiçbir veri ve

---

manüel ulaşılabilir. Bu durumda sisteme sokulan, bir disket veya CD'ye kaydetmek suretiyle veri, program veya diğer unsur elde edilebilir. Hemen ifade edelim ki mağdur tarafından açılan bir dosyanın, başkaları tarafından görülmesi halinde (örneğin monitörden) bilişim sisteminden verilerin ele geçirilmesi söz konusu değildir. Çünkü fail tarafından sisteme herhangi bir müdahalede bulunulamamaktadır. Ancak mağdurun çalışır halde bıraktığı bilgisayarında kayıtlı bulunan bir dosyayı, klavye veya fareyi kullanarak açan ve içeriğine nüfuz eden kimsenin eylemi 525a/1 kapsamında değerlendirilir. Diğer bir ihtimalde sistemin dâhil bulunduğu ağa müdahale ederek, sistemin veri nakli sırasında ağa gönderdiği verilere ulaşılması söz konusudur. Son bir olasılık olarak özellikle bilgisayarın verileri işlemesi esnasında çeşitli unsurlarından yaydığı elektromanyetik dalgaların bir alıcı vasıtasıyla toplanarak tekrar verinin elde edilmesi durumu zikredilebilir.” (YENİDÜNYA/DEĞİRMENÇİ, Mukayeseli Hukukta..., s.64-65; MERAN, Yeni Türk Ceza..., s.365).

<sup>25</sup> “Bilişim sistemine girmek suçuyla kastedilen bilişim sistemlerine yapılacak olan fiziki bir müdahale değildir. Sözgelimi, bilgisayarın kasasını açarak içindeki donanım zarar vermek bu suçu oluşturmaz; bu durumda ancak koşulları varsa “mala zarar verme” (TCK 151/1) suçu oluşur” (TAŞKIN Şaban Cankat, **Bilişim Suçları**, İstanbul, 2008, s.25). “O halde büyük bir bilgisayarın içine girip orada geceleleyen kimsenin eylemi bu suç kapsamında değerlendirilmeyecektir.” (YAŞAR/GÖKCAN/ARTUÇ, Yorumlu Uygulamalı..., s. 6742. Aynı görüş için bkz: DÜLGER, Bilişim Suçları, s.217).

<sup>26</sup> YAŞAR/GÖKCAN/ARTUÇ, Yorumlu Uygulamalı..., s.6744

<sup>27</sup> ARTUK/GÖKCEN/YENİDÜNYA, Türk Ceza..., s.4631

<sup>28</sup> ARTUK/GÖKCEN/YENİDÜNYA, Türk Ceza..., s.4631

<sup>29</sup> ARTUK/GÖKCEN/YENİDÜNYA, Türk Ceza..., s.4631

<sup>30</sup> Aynı konu hakkında ÖNGÖREN; “bu suç ile sistem sahibi ya da kullanıcısının özel hayatı, mülkiyeti ya da meslek sırları korunmaya çalışıldığından bu değerleri ihlal edecek kadar kalınmış olması yeterlidir.” ifadelerine yer vermiştir (ÖNGÖREN, İnternet Hukuku, s.46).

<sup>31</sup> MERAN, Yeni Türk Ceza..., s. 365

bilgi edinmeden sistemden çıksa dahi, bu suç oluşacaktır. Bu suretle de bilişim sistemine girme bir tehlike suçu olarak nitelendirilebilecektir.

### 3. Manevi Unsur

Bilişim sistemine hukuka aykırı olarak girme suçunun manevi unsuru, kasttır. Suçun taksirli hali cezalandırılmamaktadır. Bu nedenle failin, bilerek ve isteyerek hareket etmiş olması gerekir. Yasada herhangi bir saike yer verilmediği için de failin suçu işleyiş amacının sistemin güvenliğini denemek, eğlenmek, merak veya oyun olması arasında bir fark yoktur. Öte yandan bu suçun olası kastla işlenmesi de mümkündür.

### 4. Hukuka Aykırılık

Bilindiği üzere hukuka aykırılıktan bahsedebilmek için öncelikle tipik eylemin gerçekleşmesi gerekmektedir. Tipikliğin gerçekleştiği durumlarda karine olarak hukuka

aykırılık da gerçekleşmiştir<sup>32</sup>. Bu karinenin çürütülebilmesi için ortada fiilin hukuk düzeni ile çatışmasını engelleyecek bir hukuka uygunluk nedeni olmalıdır.

Bilişim sistemine girme suçu bakımından suçun kanuni tanımında açıkça hukuka aykırılık vurgulanmış olduğundan doktrinde bu husus hukuka özel aykırılık olarak adlandırılmaktadır. Hukuka özel aykırılık halinin suç tipinde yer aldığı durumda hâkimin, failin kastı dışında ayrıca bu özel aykırılığı da bilip bilmediğini, buna göre hareket etmeyi isteyip istemediğini de araştırması gerektiği belirtilmektedir<sup>33</sup>.

Hukuka aykırılığa ilişkin bu kısa açıklamadan sonra inceleme konusuyla ilgili olarak 5237 sayılı TCK'da yer alan bazı hukuka uygunluk nedenleri üzerinde durmak gerekir. Bu kapsamda ilk planda ilgilinin rızası akla gelmektedir. Gerçekten de başkasına ait bir bilişim sistemine, sistem sahibinin rızası dâhilinde giriş yapıldığında, kişinin fiili hukuka uygun hale gelecektir. Ayrıca var sayılan (farazi) rızanın söz konusu olabileceği durumlarda da yine aynı sonuca ulaşılabacaktır.

5271 sayılı Ceza Muhakemesi Kanununda bilişim sistemleriyle ilgili olarak bazı koruma tedbirleri düzenlenmiştir. Buna göre, CMK md. 134'te düzenlenen "*Bilgisayarlarda, Bilgisayar Programlarında Ve Kütüklerinde Arama, Kopyalama ve Elkoyma*" ve md. 135'te düzenlenen "*Telekomünikasyon Yoluyla Yayımlanarak İletişimin Denetlenmesi İletişimin Tespiti, Dinlenmesi Ve Kayda Alınması*" koruma tedbirlerin koşullarına uygun olarak uygulanması halinde; kanun hükmünü icra, hukuka uygunluk nedeninden söz edilecektir<sup>34</sup>. Elbette ki günümüzde yaygın şekilde kullanılan ileri teknoloji ürünü cep telefonları da bilişim sistemlerini bünyesinde barındırdığından CMK 135. Madde kapsamındadır.

<sup>32</sup> İÇEL Kayıhan, Özgenç İzzet, SÖZÜER Adem, MAHMUTOĞLU Fatih S., ÜNVER Yener, **İçel Suç Teorisi, 2. Kitap**, İstanbul, 1999s.100

<sup>33</sup> ARTUK Mehmet Emin, GÖKCEN Ahmet, YENİDÜNYA Caner, **Ceza Hukuku Özel Hükümler**, 10. Bası, Ankara, 2010, s.714; MAHMUTOĞLU Fatih Selami, 5237 Sayılı Türk Ceza Kanunu'nda Hukuka Uygunluk Nedenleri, Hukuk ve Adalet Dergisi, Yıl:2, Sayı:5, Nisan 2005, s.42-60

<sup>34</sup> ARTUK/GÖKCEN/YENİDÜNYA, Ceza Hukuku Özel Hükümler, s.715



## 5. Nitelikli Unsurlar

TCK 243. Maddenin ikinci fıkrasında suçun, bedeli karşılığı yararlanılabilen sistemler hakkında işlenmesi, daha az cezayı gerektiren nitelikli bir hal olarak düzenlenmiş olup, böyle bir durumun varlığı halinde mevcut ceza, yarı oranında indirilecektir. Doktrinde bu bağlamda ücret karşılığında girilebilecek bir sisteme ücret ödemeksizin girilmesi halinde yapılan ceza indirimini eleştirilmektedir<sup>35</sup>. Bize göre ise, belirli bir bedel verilmesi karşılığında açık olan sisteme girilmesi durumunda cezanın azaltılması şeklindeki düzenleme isabetlidir.

Yasaya baktığımızda bedel karşılığında yararlanılabilen sistemlerin neler olabileceğinin açıklanmadığı görülmektedir. Burada söz konusu olan sistemler, ücret karşılığında içeriğine ulaşılabilen bilişim sistemleridir. Ücret karşılığı hizmet veren web siteleri ve internet kafeler bu kapsamdadır<sup>36</sup>. Yine ücret karşılığı kullanıcılarına açık olan elektronik arşiv merkezlerinin, elektronik kütüphanelerin, gazetelerin, dergilerin bu kapsamda olduğu söylenebilir<sup>37</sup>.

Doktrinde internet servisini sağlayan sistemler ve dekoderlerin bedel karşılığında yararlanılabilen sistemlerden olup olmadığı tartışma konusu olmuştur. Bir görüşe göre; internet servisini sağlayan sistemleri de bu hüküm kapsamında değerlendirirken, diğer görüş bunlara TCK md. 163/2'de yer verilen karşılıksız yararlanma suçunun uygulanması gerektiğini belirtmiştir<sup>38</sup>. Bize göre de internet servisi sağlayan sistemler TCK md.163/2 kapsamında telefon hatları ile frekanslarından veya elektromanyetik dalgalarla yapılan şifreli veya şifresiz yayınlardan sahibinin veya zilyedinin rızası olmadan yararlanma olarak değerlendirilmelidir.

## 6. Netice Sebebiyle Ağırlaşmış Hal

TCK md.243/3 uyarınca bilişim sistemine hukuka aykırı girmek ve orada kalmak fiili nedeniyle sistemin içerdiği verilerin yok olması veya değiştirilmesi halinde cezanın arttırılacağı hükme bağlanmıştır.

Burada suç işlenmesindeki irade önem taşımaktadır. Çünkü failin kastı, girdiği ve kalmaya devam ettiği sistemdeki verileri değiştirmek veya yok etmek olmamalıdır. Aksi halde, burada TCK md.243 değil, aşağıda açıklayacağımız md. 244'te düzenlenen Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme Suçu tartışma konusu yapılacaktır<sup>39</sup>.

## 7. Suçun Özel Görünüş Şekilleri

### a. Teşebbüs

Bilişim sistemine girme suçu, sisteme girmekle tamamlanmayan bir suçtur. Çok hareketli suç olması nedeniyle tipik hareketlerden yalnız birinin işlenmesi suçun gerçekleşmesi bakımından yeterli değildir. Failin, bilişim sistemine girdikten sonra orada kalması da gerekir. Bilişim sistemine girme suçuna, icra hareketleri yarıda kaldığında **teşebbüs**<sup>40</sup> mümkündür. Örneğin; bir

<sup>35</sup> TEZCAN Durmuş, ERDEM Mustafa R., ÖNOK R. Murat, **Teorik Ve Pratik Ceza Özel Hukuku**, 7.bası, Ankara, 2010 s.772-773

<sup>36</sup> DÜLGER, Bilişim Suçları, s.226-227

<sup>37</sup> KARAGÜLMEZ, Bilişim Suçları..., s.187

<sup>38</sup> YENİDÜNYA/DEĞİRMENCİ, Mukayeseli Hukukta..., s.19

<sup>39</sup> ARTUK/GÖKCEN/YENİDÜNYA, Ceza Hukuku Özel Hükümler, s.715

<sup>40</sup> Teşebbüs hakkında bilgi için bkz: SÖZÜER Adem, **Suçta Teşebbüs**, İstanbul, 1994; DEMİRBAŞ Timur, **Ceza Hukuku Genel Hükümler**, Ankara, 2011s.420-435, ÖZGENÇ İzzet, **Türk Ceza Hukuku Genel Hükümler**, Ankara, 2009, s.421-444

bilişim sistemine girdikten sonra bir engelin ortaya çıkması dolayısıyla fiiline devam edemeyen fail, teşebbüsten sorumlu olacaktır. Bu çerçevede elektrikle rin kesilmesi, sistemin kilitlenmesi<sup>41</sup> gibi durumlarda suç teşebbüs aşamasında kalacaktır. Diğer taraftan failin bilişim sistemine girdikten sonra kendi iradesiyle sistemden çıkması gönüllü vazgeçme teşkil edeceğinden bu suça ilişkin ceza sorumluluğu bulunmayacaktır.

### **b. İştirak**

Suçun bir diğer özel görünüş şekli olan **iştirak** bakımından ise, bu suç herhangi bir özellik arz etmemektedir. Genel iştirak kuralları burada da geçerli olacaktır<sup>42</sup>.

### **c. İçtima**

Bu suça ilgili olarak **ıçtima**<sup>43</sup> bahsinde; bilişim sistemine hukuka aykırı şekilde girme ve kalmaya devam etme fiilinin, bir kişiye karşı aynı suç işleme kararıyla değişik zamanlarda işlenip işlenmediğinin değerlendirilmesi gerekir. Eğer eylem aynı kişiye ait bilişim sistemine yönelik işlenmişse, zincirleme suç hükümleri uygulanacaktır. Farklı kimselere ait bilişim sistemine yönelik işlenmişse de mağdur sayısınınca suç olacaktır.

Zincirleme suça ilişkin başka bir husus, sisteme hukuka aykırı şekilde girilmesi hareketinin, hem bilgisayar sahibine hem de o bilgisayarda kişisel bir dosyasını muhafaza eden veri sahibi üçüncü kişiye karşı işlenmiş olmasıdır. Bu durumda aynı neviden fikri içtima söz konusu olacak TCK md. 43/2 atfı nedeniyle de zincirleme suç hükümleri uygulanacaktır<sup>44</sup>.

Bir bilişim sisteminde hattın kopması nedeniyle sistemde kalınamıyor olunması halinde faile, yapmış olduğu birden çok eylem nedeniyle TCK md. 43/1'e göre ceza verilmemesi gerektiği ileri sürülmüştür. Bizce de bu durumda failin hareketlerini hukuki anlamda tek bir hareket olarak kabul etmek, başka bir anlatımla tek bir suçun varlığını kabul etmek daha isabetlidir.

Bunların yanı sıra belirtmeliyiz ki anılan suçun, bilişim sistemlerine girilerek işlenmesi zorunlu bulunan başka bilişim suçunun işlenmesi bakımından araç suç niteliğinde olduğu yönünde doktrinde görüşler vardır. Örneğin, hırsızlık (TCK md.142/2-e) veya dolandırıcılık (TCK md.158/1-f) suçlarını işlemek kastıyla bilişim sistemine girilmesi halinde bu suçlara nazaran geçit suç niteliğinde (tüketen-tüketilen norm ilişkisi) olan TCK md. 243 uygulanmayacağı belirtilse de burada TCK md. 42'de düzenlenen **bileşik suç** söz konusudur. Bilindiği gibi bu maddeye göre, biri diğerinin unsurunu veya ağırlaştırıcı nedenini oluşturan fiillerin varlığı halinde içtima kuralları uygulanmayacaktır. Bu bağlamda TCK md. 243'te düzenlenen bilişim sistemine girme suçu, TCK md. 142/2-e ve md.158/1-f açısından cezanın artmasına neden olan nitelikli unsur olduğundan fail yerine göre nitelikli hırsızlık veya nitelikli dolandırıcılıktan sorumlu olacaktır<sup>45</sup>. Dolayısıyla bu hususa ilişkin olarak doktrinde ileri sürülen

<sup>41</sup> MERAN, Yeni Türk Ceza..., s.367

<sup>42</sup> Suça iştirak hakkında ayrıntılı bilgi için bkz: MAHMUTOĞLU Fatih Selami, **Kusurluluk Prensibi Açısından Azmettirenin Ceza Sorumluluğu**, ÜHFM, Cilt: LXIII, Sayı:1-2, 2005, s.57-113

<sup>43</sup> Gerek kavram gerekse sonuçları bakımından içtima hakkında ayrıntılı bilgi için bkz: İÇEL Kayıhan, **Suçların İçtimaı**, İstanbul, 1972

<sup>44</sup> YENİDÜNYA/DEĞİRMENÇİ, Mukayeseli Hukukta..., s.22

<sup>45</sup> KARAGÜLMEZ, Bilişim Suçları..., s.196

“fail sadece amaç suçlardan cezalandırılır<sup>46</sup>” görüşüne katılmamaktayız. Fakat sanığın, banka hesaplarına internet üzerinden giriş yapması, fakat hesapta herhangi bir oynama yapmaması halinde sadece TCK md. 243 uygulama alanı bulacaktır<sup>47</sup>. “Bu suçların bir bilişim sistemine hukuka uygun şekilde girildikten sonra gerçekleştirilmesi halinde, gerçek içtima kuralları uyarınca fail her iki suçtan da cezalandırılacaktır<sup>48</sup>” şeklindeki görüşe de yine aynı nedenlerle katılmadığımızı ifade etmek isteriz.

Diğer taraftan bu suç tipinin yapısal özellikleri nedeniyle fikri içtima hükümlerinin uygulanabilmesi olasılığı ile de karşılaşılabılır. Örneğin; TCK md. 136’da yer alan “Hukuka Aykırı Olarak Verileri Ele Geçirme Suçu”nun oluşması için TCK md. 243/1’deki sisteme hukuka aykırı olarak girmenin gerçekleşmesi gerekmektedir. Bu durumda fail tek bir fiil ile birden fazla suçun oluşmasına sebebiyet vermektedir ve en ağır cezayı gerektiren suçtan dolayı cezalandırılacaktır<sup>49</sup>. Teşebbüs aşamasında kalmış “Hukuka Aykırı Olarak Verileri Ele Geçirme Suçu” söz konusu olduğunda da sorun yine fikri içtima kuralları gereği çözümlenecektir.

## **B. SİSTEMİ ENGELLEME, BOZMA, VERİLERİ YOK ETME VEYA DEĞİŞTİRME SUÇU (TCK md.244)**

### **1. Genel Olarak**

Sistemi engelleme, bozma, verileri yok etme veya değiştirme suçu, 5237 sayılı TCK’nın ikinci kitabının, topluma karşı suçlara yer veren üçüncü kısmının, “*Bilişim Alanında Suçlar*” başlıklı onuncu bölümü altında, md. 244’te düzenlenmiştir<sup>50</sup>. Bu hükümlerle, bir bilişim sistemini engelleme, bozma, sistemdeki verileri bozma, yok etme, değiştirme veya erişilmez kılma, sisteme veri yerleştirme ve var olan veriyi başka yere gönderme fiilleri yaptırım altına alınmıştır.

### **2. Korunan Hukuksal Yarar**

Bu suçla korunan hukuksal yarar, bilişim sisteminin içerdiği veriler üzerinde tasarruf yetkisine sahip kişinin, verilerle oluşturulan (yazılım, ekonomik

<sup>46</sup> YENİDÜNYA/DEĞİRMENÇİ, *Mukayeseli Hukukta...*, s.22; TEZCAN/ERDEM/ÖNOK, *Teorik Ve Pratik...*, s.772; DÜLGER, *Bilişim Suçları*, s.226

<sup>47</sup> “Sanığın, katılanın yetkilisi olduğu İmalat Pazarlama Sanayi ve Ticaret Limited şirketinin Türkiye E. Bankası Denizli şubesinde bulunan hesabına internet üzerinden izinsiz giriş yaptığı, ancak şirkete ait hesaba girdikten sonra bu hesapta oynama yaparak başka bir hesaba havale yapmadığının iddia ve kabul olunması karşısında sanığın eyleminin 5237 sayılı TCK’nun 243/1.maddesinde düzenlenen suç oluşturduğu gözletilmektedir.” Yargıtay 11. CD, 26.03.2009 tarih, E.2008/18190, K. 2009/3058. Benzer şekilde bkz: Yargıtay 5. CD, 26.03.2009 tarih, E.18190, K.3058

<sup>48</sup> DÜLGER, *Bilişim Suçları*, s.225-226; PARLAR, *Türk Ceza...*, s. 18

<sup>49</sup> TAŞKIN, *Bilişim Suçları*, s. 34

<sup>50</sup> Alman Ceza Kanunu StGB’de, 244. maddeye yakın suç, §303a ve §303b maddeleriyle mala zarar verme kapsamında yaptırım altına alınmıştır. “Bilişim sistemlerinin işlevine uygun ve doğru bir şekilde faaliyetlerine devamının temini amacını güden §303a ve §303b maddeleriyle TCK md. 244’tekilere benzer düzenlemeler içeren Alman CK.’nın bu konuda bize göre özellik arz eden farklılıkları, genel olarak verileri değiştirmekten bahsetmesi ve bilgisayar sabotajı suçuna ismen yer vermiş olmasıdır. Ancak gerek bu düzenlemenin gerekse TCK md. 244 düzenlemesinin neticeten sistemi ve yazılımını yakın düzeyde ve yeterince koruyucu nitelikte olduğu söylenebilir.” (ERDAĞ, *İşleme ve Bilgiye...*, s.293, 294).

bilgiler, bilimsel çalışma gibi) değerlerine herhangi bir engel ya da gecikme yaşamadan ulaşması ve kullanmasıdır<sup>51</sup>.

### 3. Maddi Unsurlar

#### a. Fail

Kanun suçun faili olmak bakımından herhangi bir sınırlama getirmediğinden, herkes fail olabilir. Suçun işlenmesi suretiyle bir tüzel kişi yararına haksız menfaat sağlanması durumunda ise tüzel kişiler suç faili olamayacağından cezalandırılmayacaktır. Ancak TCK md. 246 atfıyla, TCK md. 60 uygulama alanı bularak tüzel kişi hakkında güvenlik tedbirine hükmolunacaktır.

#### b. Mağdur

Bu suç tipi mağduru bakımından da bir özellik göstermemektedir. İşleyişi engellenen, bozulan, yok edilen veya değiştirilen sistem üzerinde hak sahibi kimse, suçun mağduru. Failin eyleminin birden fazla kimsenin hakkını ihlal ettiği durumlarda, bu kişilerin hepsi mağdur sıfatını kazanacaktır.

#### c. Fiil

TCK 244'deki düzenlemeye genel olarak baktığımızda; *bilişim sisteminin işleyişini engelleme-bozma, verilere zarar verme ve bilişim sistemlerini kullanarak haksız menfaat sağlama* fiillerinin cezalandırıldığı görülmektedir.

Suçun maddi unsurunun izahı bakımından söz konusu düzenlemede bahsi geçen bu hareketlerin her birini ayrı ayrı açıklamakta yarar görmekteyiz. Buna göre;

#### i. Bilişim Sisteminin İşleyişini Engelleme veya Bozma (TCK md.244/1)

Bilişim sisteminin işleyişini engelleme veya bozma fiili, TCK 244/1'de yaptırım altına alınmıştır. Suç, "işleyişi engelleme" veya "bozma" fiillerinden birinin icrasıyla gerçekleşeceği için seçimlik hareketlidir.

Engelleme ve bozmadan ne anlaşılması gerektiğini kısaca izah edecek olursak; **engelleme**, "*sistemin gereği gibi çalışmasının önlenmesi, faaliyet ve kapasitesinin sınırlandırılması, sistemin işleyişinin yavaşlatılması ya da tamamen kilitlenme noktasına getirilmesidir*<sup>52</sup>". Buna göre, işleyen sisteme yöneltilen yoğun elektro manyetik dalgalarla sistem merkezinin etkilenmesini sağlamak ya da sisteme yapılacak müdahaleyle işletim sisteminin geçici süre devre dışı bırakılması, söz konusu kavram doğrultusunda sayılabilecek örneklerdendir<sup>53</sup>. Bunların dışında bilişim sistemi hiç kullanılmaksızın, bir iç ağda (intranet) bilgisayarları birbirine bağlayan kabloların kesilmesi veya sistemin olağan işleyişinin yavaşlatılması, sisteme bilişim virüsü ya da mantık bombası gibi

<sup>51</sup> MERAN, Yeni Türk Ceza..., s.370

<sup>52</sup> ÖNGÖREN, İnternet Hukuku, s. 48; Engelleme bakımından bilişim sistemini kesintiye uğratmanın geçici mi yoksa sürekli mi olması gerektiği doktrinde tartışma yaratmıştır. Bu doğrultuda ARTUK/GÖKÇEN/YENİDÜNYA; sistemi kesintiye uğratmanın geçici olması gerektiği, MERAN, DÜLGER ve YAŞAR/GÖKCAN/ARTUÇ; geçici veya sürekli olması arasında bir fark olmadığı yönünde görüş bildirmiştir. Bizce de sistemi engellenmenin geçici veya sürekli olması arasında bir fark olmadığını savunan ikinci görüş daha isabetlidir. (ARTUK/GÖKÇEN/YENİDÜNYA, Türk Ceza..., s.4661; DÜLGER, Bilişim Suçları, s.234; MERAN, Yeni Türk Ceza..., s.371; YAŞAR/GÖKCAN/ARTUÇ, Yorumlu Uygulamalı..., s.6758)

<sup>53</sup> DEĞİRMENCİ, 2004 Türk Ceza..., s.205

zararlı bir yazılımın bulaştırılması ya da sistemde olmayan bir şifrenin sisteme yerleştirilmesi veya mevcut şifrenin değiştirilmesi de engellemedir<sup>54</sup>.

**Bozma** ise “sistemin veri işleme faaliyeti yapamayacak hale getirilmesidir<sup>55</sup>”. Sistemin olağan ve normal koşullarda yerine getirmiş olduğu işlevini yapamaz hale getirmesi bu kapsamda bozmadır<sup>56</sup>. Bozma bilişim sistemi kullanılarak, sistemin bütününe veya bir kısmına yönelik gerçekleştirilebileceği gibi, sisteme fiziksel müdahaleyle de gerçekleştirilebilir<sup>57</sup>.

## ii. Verilere Zarar Verme (TCK md. 244/2)

Bilişim sistemindeki verileri *bozmak*, *yok etmek*, *değiştirmek* veya *erişilmez kılmak*, *sisteme veri yerleştirmek* ve *var olan verileri başka bir yere göndermek* fiilleri, TCK md.244/2’de yaptırım altına alınmıştır<sup>58</sup>. Maddede bahsi geçen bu seçimlik hareketlerden birinin gerçekleşmesiyle suç tamamlanmış olacaktır.

Anılan kavramları açıklamak gerekirse; **bozmak**, verilerden elde edilmek istenen faydanın, değiştirme, tamamen veya kısmen tahrip etme gibi hareketlerle, elde edilememesini sağlamaktır. Bilişim sistemlerine sızan ve virüs olarak adlandırılan programlar vasıtasıyla sistemde yer alan verilerin tahrip edilmesi bozmaya örnektir<sup>59</sup>. Sistemin fiziki varlığına yapılacak müdahaleler bakımından ise içindeki verilerin de zarar görmesi halinde, verilerin bozulmasından söz edilebilir<sup>60</sup>.

**Yok etmek**, verilerin ortadan kaldırılması anlamına gelmektedir. Verilerin silinmesi veya bulunduğu sistemin biçimlendirilmesi hareketlerinin yok etme olduğu söylenebilir. Bu hareketler sisteme fiziksel müdahale yoluyla olabileceği gibi bir ağla bağlanmak suretiyle de gerçekleştirilebilir<sup>61</sup>.

**Değiştirmek**, veriler üzerinde yapılan bir tür manipülasyondur. Verilerin başka biçimlere sokulması, yeni içerik kazandırılması veya niteliklerinin değiştirilmesi bu eyleme örnek teşkil eder<sup>62</sup>.

**Erişilmez kılmak**, “verilere erişimi sağlayan yolların (path) değiştirilmesi veya silinmesidir<sup>63</sup>”. Bu halde aslında veriler mağdurun sisteminde olduğu halde fail, yaptığı birtakım işlemlerle, mağdurun kendi verilerine ulaşmasını imkânsız hale getirmektedir.

**Sisteme veri yerleştirmek**, “sistemde yer alan verilere herhangi bir zarar vermeden, onlara ulaşma imkânını ortadan kaldırmadan ek birtakım veri-

<sup>54</sup> DÜLGER, Bilişim Suçları, s.234

<sup>55</sup> ÖNGÖREN, İnternet Hukuku, s.48

<sup>56</sup> MERAN, Yeni Türk Ceza..., s.371

<sup>57</sup> ARTUK/GÖKCEN/YENİDÜNYA, Türk Ceza..., s.4661

<sup>58</sup> 765 sayılı kanun bakımından daha önce de yapmış olduğumuz karşılaştırmaya burada da yer vermek isteriz. Şöyle ki; TCK md.244’ün 765 sayılı yasanın 525/b-1’de düzenlenen “sistem ve unsurlarına zarar verme suçunun” karşılığı olduğu anlaşılmaktadır. Ancak yeni düzenlemede eskisinden farklı olarak madde metninde “zarar verme” teriminin tercih edilmediği görülmektedir. Böylelikle bilişim sisteminin donanım kısmına yapılacak mala zarar verme kastı taşıyan eylemler, bu madde kapsamı dışında tutulmaktadır.

<sup>59</sup> ARTUK/GÖKCEN/YENİDÜNYA, Türk Ceza..., s.4666

<sup>60</sup> ARTUK/GÖKCEN/YENİDÜNYA, Türk Ceza..., s.4666

<sup>61</sup> DÜLGER, Bilişim Suçları, s.236-237

<sup>62</sup> DÜLGER, Bilişim Suçları, s.237

<sup>63</sup> ARTUK/GÖKCEN/YENİDÜNYA, Türk Ceza..., s.4667

leri sisteme ilave etmektedir<sup>64</sup>. Bu durumda verilerin güvenilirliđi zarar görmektedir.

**Var olan verileri başka yere göndermek** ise, mağdura ait verilerin farklı bir bilişim sistemine gönderilmesidir.

### **iii. Bilişim Sistemini Kullanarak Haksız Menfaat Sağlama (TCK md.244/4)**

TCK md. 244/4'te 1. ve 2. fıkralarda tanımlanan fiillerin işlenmesi suretiyle kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlama suç olarak düzenlenmiştir. Fakat kanun koyucu madde kapsamında sayılan fiillerin işlenmesi halinde, başkaca suçların oluşması ihtimalini de gözeterek, fiillerin başka bir suç oluşturulmaması halinde bu maddenin uygulanacağını öngörmüştür.

#### **4. Manevi Unsur**

Sistemi engelleme, bozma, verileri yok etme veya deđiştirme, kasten işlenebilen bir suçtur. Suçun taksirli hali ise cezalandırılmaz. Bu nedenle fail, bilişim sistemini engellediđini, bozduđunu, verileri yok ettiđini veya deđiştirdiđini bilmeli ve istemelidir. Suç tipinde doğrudan kasta ilişkin bir ibare bulunmadıđından, olası kastla işlenmesi de mümkündür.

#### **5. Hukuka Aykırılık**

Hukuka aykırılık unsuru bakımından yukarıda “*Bilişim Sistemine Girme Suçu*” bakımından ifade ettiğimiz hususlar burada da geçerlidir.

#### **6. Daha Ağır Cezayı Gerektiren Nitelikli Unsur**

TCK md. 244/3'te bu fiillerin bir banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinde işlenmesi hali, cezayı yarı oranında arttıran bir nitelikli unsur olarak karşımıza çıkmaktadır.

#### **7. Suçun Özel Görünüş Şekilleri**

##### **a. Teşebbüs**

Bu suça teşebbüs mümkündür. İcra hareketlerinin failin elinde olmayan nedenlerle yarıda kalması ve bu nedenle sisteme etki edememesi halinde teşebbüsten bahsedilir.

Söz konusu suçun seçimlik hareketli olmasından dolayı akla, maddede sayılan hareketlerin birden fazlasının olayda mevcut olması, ancak bunlardan bir kısmının tamamlanmış, diğer kısmının ise teşebbüs aşamasında kalması durumunda, nasıl bir değerlendirme yapılacağı sorusu gelmektedir. Burada dikkat edilmesi gereken, seçimlik hareketli suçlarda, birden fazla hareket aynı anda gerçekleşse de olayda tek bir suçun oluştuđunun kabul edileceđi kuralıdır. Bu kural uyarınca, seçimlik hareketlerden biri teşebbüs aşamasında kalmış olsa bile, diğeri tamamlanmışsa, ortada yine tek bir suçun varlıđından söz edilecektir.

Bunların dışında sisteme veri yerleştirmek için erişen fail, gönüllü olarak bu fiilden vazgeçmiş ise, TCK 244/2'ye teşebbüsten deđil, TCK 243'ten sorumlu tutulacaktır. Gönüllü vazgeçme halinde failin gönüllü olarak vazgeçtiđi ana

<sup>64</sup> DÜLGER, Bilişim Suçları, s.237

kadar yapmış olduğu eylemler eğer başka bir suçu oluşturuyorsa fail bu suçtan cezalandırılır (TCK md.36) hükmü gereği fail, bilişim sistemine girme suçundan dolayı cezalandırılacaktır.

### **b. İştirak**

Söz konusu suç iştirak açısından bir özellik göstermez. İştirake ilişkin genel hükümler burada da uygulanır.

### **c. İçtima**

Bilişim sisteminin işleyişinin bozulması ve verilere zarar verilmesi, aynı zamanda TCK md. 151'de düzenlenen mala zarar verme suçunu da oluşturmaktadır. Bu duruma ilişkin olarak doktrinde farklı görüşler mevcuttur. Bir görüşe göre burada, TCK md.44 uyarınca farklı neviden fikri içtima kuralının uygulama alanı bulacağı ve failin ağır olan suçtan cezalandırılacağı kabul edilmektedir<sup>65</sup>. Buna karşın diğer görüş ise; anılan suç tipinde bahsi geçen bilişim sisteminin, TCK md.151'de yer alan klasik mal kapsamında olmadığını, işler ve fayda sağlayan bir araç olduğunu, bu nedenle de TCK md. 151 ile 244'ün farklı hukuksal değeri koruduğunu ileri sürmüştür<sup>66</sup>. Kanaatimizce bu suçla korunan hukuksal değer soyut olarak sadece veriler olmayıp aynı zamanda somut olarak bilişim sistemine ait donanımlardır<sup>67</sup>. Bu sebeple bilişim sisteminin donanımlarına zarar verilmesi halinde hem mala zarar verme hem de TCK md.244 oluşacaktır. Buradaki sorun özel normun genel norma önceliği prensibi gereği bilişim sistemini özel olarak koruyan bir norm olan TCK md.244'ün uygulanması ile çözülecektir. Zira aynı hukuki değeri koruyan farklı iki normun ihlali söz konusudur. Ancak md. 244, mala zarar verme suçuna göre birtakım ek özelliklere sahip olan özel norm niteliğinde olduğundan uygulama alanı bulacaktır<sup>68</sup>.

Yine bu maddede yer alan suçun işlenmesi için hukuka aykırı olarak bilişim sistemine girmek ve sistemde kalmak gerektiğinden bahisle TCK md.243'ün TCK md.244'e nazaran geçit suç olarak kabul edilmesi ve failin sadece TCK md.244'e göre cezalandırılması gerektiğini ifade eden görüşe<sup>69</sup> karşılık diğer bir görüş, TCK md.244'ün, TCK md.243'ün öngördüğü biçimde sisteme girmeden gerçekleştirilmiş olmasının olanaklı olabileceğini, bu sebeple de TCK md.243'te yer alan eylemlerin TCK md.244'ün ögesi ya da nitelikli hali olmadığı gerekçesiyle burada gerçek içtima hükümlerinin uygulanması gerektiğini ileri sürmektedir<sup>70</sup>. Gerçekten bilişim sistemine girmeden verilerin bozulması söz konusu olabilir. Bu durumda zaten TCK md.243'ten bahsedemeyiz. Ancak bilişim sistemine girerek veri bozma, yok etme halleri var ise bu durumda yine görünüşte içtima söz konusu olup fikri içtima kabul eden ikinci görüş isabetsizdir. Zira TCK md. 244'ün oluşması halinde bu suç tipinin gerçekleştirilebilmesi için TCK md.243'ün gerçekleştirilmiş olması gerekir. Bu halde md. 244, md.243 açısından tüketen norm niteliğindedir. Tüketen- tüketilen norm ilişkisi gereği TCK md. 244'ün uygulanacağı kabul edilmelidir.

<sup>65</sup> YENİDÜNYA/DEĞİRMENCİ, Mukayeseli Hukukta..., s.27

<sup>66</sup> DÜLGER, Bilişim Suçları, s.242; TAŞKIN, Bilişim Suçları, s.55

<sup>67</sup> PARLAR, Türk Ceza..., s.24

<sup>68</sup> Özel norm-genel norm ilişkisi için bkz: İÇEL/SOKULLU AKINCI/ÖZGENÇ/ MAHMUTOĞLU/ ÜNVER, İçel Suç Teorisi, s.566 vd.

<sup>69</sup> YENİDÜNYA/DEĞİRMENCİ, Mukayeseli Hukukta..., s.27

<sup>70</sup> MERAN, Yeni Türk Ceza..., s.368

TCK md. 244/2 kapsamında bir bilişim sistemindeki verilerin başka bir yere gönderilmesi aynı zamanda TCK md. 136'daki kişisel verilerin hukuka aykırı olarak başkasına vermek, yaymak veya ele geçirmek fiillerini de gündeme getireceğinden bu iki suç arasında TCK md. 44 gereği farklı neviden fikri içtima kurallarının uygulanması söz konusu olacaktır<sup>71</sup>.

Bir belgenin gerçeğe aykırı şekilde düzenlenmesi ya da gerçeğe uygun bir belgenin değiştirilmesi amacıyla bilişim sistemine veri eklenmesi, verilerin değiştirilmesi gibi hallerde, fail belgede sahtecilik suçundan ve 244/2'den cezalandırılacaktır.<sup>72</sup>

İçtima ile ilgili başkaca önemli bir problem ise TCK md. 244/4'te yer alan bilişim sistemini kullanarak haksız yarar sağlama suçunda gündeme gelecektir. İlk olarak belirtmek gerekir ki, bu fıkranın kapsamına giren hallerde fail aynı zamanda TCK md. 244/2 ve md. 244/3'ten cezalandırılmayacaktır<sup>73</sup>. Ayrıca TCK md. 244/4 tamamlayıcı norm niteliğinde olduğundan, fail tarafından gerçekleştirilen fiiller başka bir suç tipi kapsamına girmekteyse TCK md. 244/4 uygulanmayacaktır. Bu nedenle TCK md. 244/4 ile TCK md. 142/1-e ile TCK md. 157 arasındaki ilişkiye değinmek gerekir. Fakat bundan önce belirtmek gerekir ki madde metninin aksine gerekçede eylemin daha ağır bir cezayı gerektiren suçu oluşturması halinde TCK md. 244/4'nin uygulanmayacağı belirtilmesinin hatalı olduğu, çünkü madde metninde ağır ya da hafif farkı olmaksızın eylemin başka bir suçu oluşturması halinde TCK md. 244/4'ün uygulanmayacağı belirtilmektedir<sup>74</sup>. TCK md. 142/1-e ve md. 157'nin TCK md. 244/4 ile ilişkisine gelince md. 244/4'ün uygulanabilmesi için fiilin başka bir suçu oluşturmaması gerekir. Yani md. 244/4 tamamlayıcı norm niteliğindedir. Bu sebeple bu gibi hallerde koşulları varsa TCK md. 142/1-e veya md. 157 uygulanacaktır.

### **C. BANKA VEYA KREDİ KARTLARININ KÖTÜYE KULLANILMASI (TCK md.245)**

#### **1. Genel Olarak**

Banka ve Kredi Kartlarının Kötüye Kullanılması Suçu, TCK'nın ikinci kitabının, topluma karşı suçlara yer veren üçüncü kısmının, "*Bilişim Alanında Suçlar*" başlıklı onuncu bölümünde, md. 245'te düzenlenmiştir<sup>75</sup>. Bu hükme, 29.06.2005 tarih ve 5377 sayılı Kanunun md. 27 ile iki fıkra ve 06.12.2006 tarih ve 5560 sayılı Kanunla 5. fıkranın eklenmesiyle, iki kez değişiklik yapılarak, maddeye bugünkü şekli verilmiştir. Temel olarak söz konusu hükümle, *banka ve kredi kartlarını hukuka aykırı kullanma, sahte banka veya kredi kartı üretme, satma, devretme veya kabul etme, sahte banka veya kredi kartları oluşturma ve kullanma* fiilleri, yaptırım altına alınmıştır.

<sup>71</sup> YENİDÜNYA/DEĞİRMENCİ, Mukayeseli Hukukta..., s.32

<sup>72</sup> YENİDÜNYA/DEĞİRMENCİ, Mukayeseli Hukukta..., s.32

<sup>73</sup> YENİDÜNYA/DEĞİRMENCİ, Mukayeseli Hukukta..., s.35; ARTUK/GÖKCEN/ YENİDÜNYA, Ceza Hukuku Özel Hükümler, s. 731

<sup>74</sup> DÜLGER, Bilişim Suçları, s. 249

<sup>75</sup> Alman Ceza Kanunu StGB'de 245. maddeye yakın suç §266b maddesiyle "dolandırıcılık ve güveni kötüye kullanma" kapsamında ve §152a ve §152b maddeleriyle de "para ve kıymetli damgalarda sahtecilik" bölümünde yaptırım altına alınmıştır. "Alm. CK'nın, TCK md. 245'tekilere yakın düzenlemeleri olarak §152a, §152b ve §266b maddeleri ile benimsenen kavramın bize nazaran farklılık arz eden şekli özelliği, bunun bizde olduğu gibi bilişim alanında suçlar başlığı altında ve tek bir hüküm içerisinde ele alınmak yerine, Kanun'un farklı bölümlerinde ve ayrı hükümler içerisinde düzenlenmiş olmasıdır." (ERDAĞ, Bilişim Alanında Suçlar, s.300).



## **2. Korunan Hukuksal Yarar**

Bu suç ile birden fazla hukuksal yarar korunmak istenmektedir. Bu husus madde gerekçesinde “*hırsızlık, dolandırıcılık, güveni kötüye kullanma ve sahtecilik suçlarının ratio legis’lerinin tümünü de içeren bu fiillerin, duraksamaları ve içtihat farklılıklarını önlemek amacıyla, bağımsız suç haline getirilmeleri uygun görülmüştür.*” şeklinde ifade edilmiş ve böylece suçla korunan hukuksal yarar ortaya konulmuştur.

Buradan anlaşılan söz konusu suç tipi ile korunması amaçlanan hukuki değer; hırsızlık, dolandırıcılık, güveni kötüye kullanma suçlarını içerdiği için malvarlığı<sup>76</sup> ve kişilere duyulan güven, sahtecilik suçunu karşıladığı için ise, kamuya duyulan güven ve itibardır<sup>77</sup>.

## **3. Maddi Unsurlar**

### **a. Fail**

Bu suçun faili sahte banka ve kredi kartlarını üreten kişi olabileceği gibi, bunların dışındaki üçüncü kişiler de olabilir. Ancak suçun oluşması bakımından failin kartın mahiyeti hakkında bilgi sahibi olması gerekir<sup>78</sup>.

Diğer taraftan suçun işlenmesi suretiyle bir tüzel kişi yararına haksız menfaat sağlanması durumunda ise, TCK md. 246 atfıyla, TCK md. 60 uygulama alanı bularak, tüzel kişi hakkında güvenlik tedbirine hükmolunur.

### **b. Mağdur**

Bu suçun mağduru herkes olabilir<sup>79</sup>. Filin işlenmesi sonucunda malvarlığında azalma meydana gelen gerçek kişiler bu suçun mağduru. Banka veya kredi kartı kullanılan banka ise, suçun mağduru değil, suçtan zarar göreni konumundadır<sup>80</sup>.

### **c. Fiil**

TCK md. 245’te *banka ve kredi kartlarını hukuka aykırı kullanma, sahte banka veya kredi kartı üretme, satma, devretme veya kabul etme ve sahte banka veya kredi kartları oluşturma ve kullanma* şeklinde üç grup fiilin<sup>81</sup>, yaptı-

<sup>76</sup> PARLAR Ali- AKIN Mustafa- HATİPOĞLU Muzaffer, **Bankacılık Ceza Hukuku**, Ankara-2010, s. 702.

<sup>77</sup> ERMAN Sahir, **Kamu Güvenine Karşı Suçlar**, İstanbul, 1996, s.222-223; DÖNMEZER, Kişilere ve Mala Karşı Cürümler, s.619; ÖNDER, Şahıslara ve Mala Karşı..., s.506; DÜLGER, Bilişim Suçları, s.251

<sup>78</sup> ARTUK/GÖKCEN/YENİDÜNYA, Türk Ceza..., s.4697

<sup>79</sup> “Örneğin bir banka veya kredi kurumu, bir kimse hakkında kredi kartı düzenleyip göndermiş, ancak eline geçmeden, örneğin kargo elemanı tarafından kullanılmış ise, bu durumda kart adına düzenlenen ancak henüz kart eline geçmemiş olan kimse de suçun mağduru olacaktır.” (YAŞAR/GÖKCAN/ARTUÇ, Yorumlu Uygulamalı..., s.6799).

<sup>80</sup> YAŞAR/GÖKCAN/ARTUÇ, vermiş olduğu şu örnekte; “Bu suçta 5464 sayılı Kanun’un 12. maddesine göre, kart hamilinin rıza dışında elden kartının çıktığına dair bildirimden geriye doğru 24 saat içinde yapılan kullanımın 150 TL lik kısmından sorumlu olduğundan, alan şahıs daha fazla harcama yaptıysa bu durumda kartı çıkaran banka ve finans kurumu da suçun mağduru olacaktır.” demektedir. (YAŞAR/GÖKCAN/ARTUÇ Yorumlu Uygulamalı..., s.6798). Ancak bizce burada bankanın sıfatı suçtan zarar gören olmalıdır.

<sup>81</sup> Bu noktada 765 sayılı TCK ile bir karşılaştırma yaptığımızda, 765 sayılı TCK’da banka ve kredi kartlarıyla ilgili eylemleri açıkça düzenleyen bir maddenin bulunmaması ne-

rım altına alındığını yukarıda belirtmiştik. Buna göre biz de maddede bahsi geçen eylemleri ayrı ayrı izah edeceğiz.

### **i. Banka ve Kredi Kartlarını Hukuka Aykırı Şekilde Kullanma (TCK md. 245/1)**

TCK md. 245/1'de *başkasına ait bir banka veya kredi kartını, her ne suretle olursa olsun ele geçiren veya elinde bulunduran kimsenin, kart sahibinin veya kartın kendisine verilmesi gereken kişinin rızası olmaksızın bunu kullanarak veya kullandırarak kendisine veya başkasına yarar sağlaması* cezalandırılmıştır<sup>82</sup>. Başka bir deyişle başkasına ait kredi kartının ele geçiriliş şekline bakılmaksızın, kartın, sahibinin rızası hilafında kullanılması veya kullandırılması suç haline getirilmiştir.

Belirtmeliyiz ki; söz konusu suçun oluşabilmesi için, ortada sahte olmayan gerçek bir kredi kartının bulunması gereklidir. Nitekim kartın sahte olduğu ihtimalinde, ikinci ve üçüncü fıkrada yer alan suçların varlığı bakımından bir tartışma söz konusu olacaktır.

Madde metninde “her ne suretle olursa olsun” ibaresine yer verildiğinden, failin kartı ne şekilde ele geçirdiğinin ise bir önemi yoktur. Başka bir deyişle kartın hamilinin rızasıyla veya rıza dışı ya da çalınarak, hıleyle, tehditle ele geçirilmesi bakımından bir fark bulunmamaktadır<sup>83</sup>.

Ayrıca TCK md. 245'teki suç tipi bakımından, kredi kartının fiziki olarak kullanımı da şart değildir<sup>84</sup>. Fiziki varlığı bulunmayan kredi kartı numarası kullanımı da, suçun maddi unsurunun oluşumu açısından yeterlidir. Yargıtay 11. CD. de 14.10.2010 tarih, E.2009/22925, K.2010/11207 sayılı kararında bu hususa vurgu yaparak 5464 Sayılı Banka Kartları ve Kredi Kartları Kanununun 3/e maddesi uyarınca “**Kredi kartının, nakit kullanımı gerekmeksizin mal ve hizmet alımı veya nakit çekme olanağı sağlayan basılı kartı veya fiziki varlığı bulunmayan kart numarasını**” ifade etmesi karşısında kredi

---

deniyle banka ve kredi kartlarıyla gerçekleştirilen söz konusu fiillerin bu yasa zamanında en çok sorun yaratan konulardan biri olduğu hatırlatılmaktadır.

<sup>82</sup> MAHMUTOĞLU Fatih Selami, **Ekonomik Suçlar Bağlamında Kredi Hukukundan Kaynaklanan Suç ve İdari Suçlar**, Ankara, 2003. Eski yasa döneminde, banka ve kredi kartlarının hukuka aykırı kullanımı ile ilgili olarak, 765 sayılı TCK'nın 525/b maddesinin 2. fıkrasının uygulanıp uygulanmayacağı tartışmalıydı. Ancak Yargıtay Ceza Genel Kurulu 2001 yılında verdiği bir kararla (Yargıtay CGK'nın 10.04.2001 tarih, E.2001/6-30, K.2001/57 sayılı kararı), bu tartışmaya son vererek, söz konusu eylemler bakımından 765 sayılı TCK'nın 525/b-2 maddesinin uygulanabileceğine karar vermiştir. Fakat bu sefer de banka veya kredi kartlarının nasıl ele geçirildiğine ve kullanıldığına ilişkin ayrımlarla, olayda dolandırıcılık mı bilişim suçu mu olduğu hususları tartışmalı hale gelmiştir. 5237 sayılı TCK'nın 245. maddesinin yürürlüğe girmesi neticesinde ise, bu tartışmalar azalmıştır.

<sup>83</sup> ÖZBEK Veli Özer, **Banka ve Kredi Kartlarının Kötüye Kullanılması Suçu**, Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi, Cilt:9, 2007, Özel sayı, Ayrı Basım, İzmir, 2007, s.1030-1031.

<sup>84</sup> Aynı görüşteki ÖZBEK de; “bu suçun oluşması için kartın ‘fiziksel olarak’ kullanılması zorunludur kanısındayız. Hükümde yer alan “kartın kullanılması ya da kullandırılması” sadece karta ilişkin bilgilerin değil, bizzat kartın kullanılması şeklinde anlaşılmalıdır. Ancak kredi kartının banka kartından farklı olarak “basılı kart veya fiziki varlığı bulunmayan kart numarası” şeklinde tanımlanması karşısında bu suç bakımından kredi kartının fiziksel olarak kullanılmasının zorunlu olmadığı sonucu çıkmaktadır.” demektedir. ÖZBEK, Banka ve Kredi Kartlarının Kötüye Kullanılması Suçu, s.1032

kartı bilgilerinden yararlanarak menfaat sağlanmasının kredi kartı gibi değerlendirilmesi gerektiği... ifadelerine yer vermektedir.

Son olarak belirtmek isteriz ki, suçun tamamlanmış olduğundan söz edebilmek için, kartın kullanımıyla, kullanılan kimseye veya başkasına bir yarar sağlanması gerekir. Bu suretle, örneğin; “arkadaşının kartlarını alıp, çevresindekilere göstererek itibar sağlamaya çalışan bir kimse<sup>85</sup>” bakımından yararın gerçekleştiği söylenemez.

## **ii. Gerçeğe Aykırı Banka veya Kredi Kartı Üretmek (TCK md. 245/2)**

TCK md. 245/2’de, başkalarına ait banka hesaplarıyla ilişkilendirilerek, sahte banka veya kredi kartı üretilmesi, satılması, devredilmesi veya kabul edilmesi fiilleri cezalandırılmaktadır. Bu nedenle kişinin kendi hesabıyla bağlantılı olarak kredi kartı üretmesi halinde aşağıda açıklanacağı üzere TCK md. 245/3 söz konusu olacaktır<sup>86</sup>. Ayrıca kredi kartı sözleşmesi düzenlenmesi amacıyla sahte belge ibraz edilmesi durumunda BKKK md. 37/2, sahte bilgilerle sözleşmenin düzenlenmesinin ardından kartın üretilmesi neticesinde ise TCK md. 245/2’den doğan sorumluluk gündeme gelecektir<sup>87</sup>.

TCK md. 245/2 ile ilgili bir diğer düzenleme BKKK md. 38’dir. Söz konusu maddede Bankacılık Düzenleme ve Denetleme Kurulu’ndan gerekli izinleri almaksızın kredi kartı çıkarma eylemi yer almaktadır. Dikkat edilmelidir ki bu hüküm, banka ya da kredi kartı gerçeğe uygun hesap bilgileri ile düzenlenmiş olsa bile tatbik imkanı bulabilecektir. Gerçeğe aykırı ve başkasının hesap-

<sup>85</sup> YAŞAR/GÖKCAN/ARTUÇ Yorumlu Uygulamalı..., s.6805

<sup>86</sup> YAŞAR/GÖKCAN/ARTUÇ Yorumlu Uygulamalı..., s.6806

<sup>87</sup> ÖZBEK Veli Özer, **Banka ve Kredi Kartlarının Kötüye Kullanılması Suçu**, Bilişim Hukuku, TC. Yargıtay Başkanlığı, Ankara, 2008, s.110. Yargıtay 11. CD 19.7.2010 tarih, E.2010/639, K. 2010/9199 sayılı kararında; “Failin sahte isimle çeşitli bankalarda hesap açtırması ve kredi kartı başvurusunda bulunması olayında; Sahte belgelere dayanarak hesap açtırmanın özel belgede sahtecilik suçunu oluşturduğuna, Sanığın kredi kartı talebinde bulunması fiilinin ise 5464 sayılı Kanun md. 37/2’de yer alan düzenlemeye göre “kredi kartı veya iş yeri sözleşmesinde veya eki belgelerde sahtecilik yapanlar veya sözleşme imzalamak amacıyla sahte belge ibraz edenler ile ilgili düzenlemenin sözleşmeye kadar olan safhada uygulanabileceği, kredi kartı sözleşmesinin düzenlenmesinden sonra kartın üretilmesi halinde 5237 sayılı TCK ‘nın 245/2, üretilmeden sahteliğin anlaşılması halinde bu suça teşebbüs ve sahte üretilen bu kartına kullanılarak menfaat temin edilmesi halinde ise ayrıca 245/3.maddesine temas eden suç oluşturacağı... olayda ise sanığın A...bank ... şubesi ile kredi kartı sözleşmesi imzalamış, ancak talebi reddedilmiş, F... bank ... şubesi ile ... kredi kartı sözleşmesi imzalamış, ancak sonradan yapılan değerlendirme sonucunda talebinin reddedilmiş olmakla; sanığın eylemlerin her bir banka yönünden TCK 245/2. maddesinde düzenlenen suça teşebbüs aşamasında kaldığı”na hükmetmiştir. Sahteciliğe ilişkin diğer kararlar ise şu şekildedir: Yargıtay 11. CD. 15.10.2007 tarih, E.2007/5158, K.2007/6701 sayılı kararında “Sanığın üzerine kendi fotoğrafını yapıştırdığı, katılana ait nüfus cüzdanını aynı suç işleme kararı altında değişik zamanlarda farklı bankalara karşı birden fazla otomobil kredisi müracaatında kullanmasının zincirleme biçimde resmi evrakta sahtecilik suçunu oluşturduğunun kabulü ile TCK’nun 204/1, 43. Maddeleri uyarınca mahkumiyeti yerine eylemin tek kabulü ile yazılı şekilde ceza tayini” diyerek kredi almak için sahtecilik yapılmasını sahtecilik suçu içerisinde değerlendirmiştir. Yargıtay 11. CD. 26.05.2010 tarih, E.2010/4953, K.2020/6357 “Sanığın başkası adına sahte kimlik, ikametgâh belgesi, maaş bordrosu oluşturarak değişik tarihlerde 5 ayrı bankaya başvurarak kredi sözleşmeleri imzalayıp kredi tahsisini sağladığının iddia ve kabul olunması karşısında; mağdur banka sayısınca teselsül eden “sahtecilik” suçunun oluşacağı gözetilmelidir. Teselsül eden tek suç kabulü suretiyle eksik ceza tayini bozma nedenidir.”

larıyla ilişkilendirilerek<sup>88</sup> banka veya kredi kartı oluşturulması ise, hem BKKK md. 38 hem de TCK md. 245/2 ile birlikte düşünölmelidir. Bu durumda farklı neviden fikri içtima kuralı gereğince en ağır cezayı gerektiren suçtan mahkümüyet verilir. Sonuç olarak her iki suçı karşılaştırdığımızda TCK'da yer alan düzenlemenin cezası daha fazla olduğundan, TCK md. 245 uygulanır.

Üzerinde durulacak bir diđer husus, kişinin başkasına ait kredi kartını sadece üzerinde bulundurmasının TCK md. 245/2 kapsamında değeriendirilip değeriendirilemeyeceğidir. Aslında bulundurmamak maddede sayılan fiillerden biri değildir. Fakat bizce kabul etmek bulundurmaya da içinde barındırdığından, bu da TCK md. 245/2 hükmü kapsamında değeriendirilmelidir<sup>89</sup>.

Açıklamalarımızdan da fark edileceğı üzere; TCK md.245/2'de, ortada sahte bir banka veya kredi kartı olması gerekirken, TCK md. 245/1'de sahte olmayan, gerçek bir banka veya kredi kartının mevcudiyeti zorunludur. Ayrıca suçun tamamlanması için birinci fıkrada failin kendisine veya başkasına bir yarar sağlaması aranırken, ikinci fıkra açısından failin böyle bir yarar elde etmesi şart değildir.

Son olarak değinmek istediğimiz nokta ise, bu fıkranın, 1 Haziran 2005 tarihinde yürürlüğe giren 5237 sayılı TCK'nın ilk halinde bulunmadığı, 5377 sayılı yasa ile md. 245'te yapılan değışiklikle getirilmiş olduğudur. Bu nedenle 1 Haziran 2005 ile 5377 sayılı yasanın yürürlüğe girdiğı, 08.07.2005 tarihleri arasında işlenen banka ve kredi kartı sahteciliğı suçlarında nasıl bir uygulama yapılacağı, doktrinde tartışmalıdır. Konuya ilişkin olarak bir görüş; "765 sayılı TCK'nın 525/2-a maddesinin uygulanacağı<sup>90</sup>", diđer bir görüş ise<sup>91</sup>; "765 sayılı TCK 1 Haziran tarihinde yürürlükten kalktığından ve bir kanunun yürürlükten kalktıktan sonraki olaylara uygulanması mümkün olmadığından, bu çözüm şekli hukuki değildir. Ancak bu tarihler arasında gerçekleştirilen kredi kartı sahteciliğı eylemlerinde genel sahtecilik suçlarının uygulanabileceğini ve lehe kanun değeriendirmesinin TCK md.245. maddesinin yeni hali ile bu hükümler arasında yapılacağını düşünmekteyiz." şeklindedir. Kanaatimizce bu dönemde gerçekleşen fiiller bakımından mevzuatın diđer hükümlerine bakılmalıdır. Somut olayın özelliğine göre dolandırıcılık, duruma göre belgede sahtecilik hükümleri incelenmelidir. Eğer fiiller bu suçların kapsamına girmiyorsa, TCK md.244/2'de sayılan hareketler o tarihte kanunda suç olarak düzenlenmediğinden kanunilik ilkesi gereğı fiil cezalandırılmamalıdır.

### **iii. Sahte Banka veya Kredi Kartı Kullanarak Yarar Sağlama (TCK md. 245/3)**

TCK md. 245/3 ile sahte oluşturulan veya üzerinde sahtecilik yapılan bir banka veya kredi kartını kullanmak suretiyle kendisine veya başkasına yarar sağlamak fiili cezalandırılmaktadır.

Yukarıda da ifade ettiğimiz gibi kişinin kendi hesabıyla bağlantılı olarak ya da hiçbir hesabı kullanmadan kredi kartı üretmesi halinde 'başkalarının hesaplarıyla ilişkilendirme' unsuru bulunmadığından TCK md.245/2'de yer alan gerçeğe aykırı banka veya kredi kartı üretmek suçu oluşmayacaktır.

<sup>88</sup> Başkalarının hesaplarıyla ilişkilendirilmeksizin gerekli izinleri almamış kişilerin gerçeğe aykırı banka veya kredi kartı çıkarması durumunda ise BKKK md.38 ve TCK md. 245/3'ün uygulama alanı bulup ve fikri içtima hükümlerine gidileceğini belirtmeliyiz.

<sup>89</sup> Aynı görüş için bkz: ÖZBEK, Banka ve Kredi Kartlarının Kötüye Kullanılması Suçu, s.1047

<sup>90</sup> MALKOÇ İsmail, **Açıklamalı Yeni Türk Ceza Kanunu 2. Cilt**, 2007, s.1687

<sup>91</sup> YAŞAR/GÖKCAN/ARTUÇ Yorumlu Uygulamalı..., s.6808

Doktrinde verilen<sup>92</sup> bir örneği naklederek açıklayacak olursak; kara listede olan birinin, kendisine kredi kartı verilmemesi nedeniyle kendi hesabıyla irtibatlandırarak sahte kart basması veya hiçbir hesaba ilişkilendirilmeden kart üretmesi ve bunu kullanarak yarar sağlanması söz konusu olsun. Yargıtay kararında<sup>93</sup> da belirtildiği üzere 245. maddenin 2. ve 3. fıkrası birbirinin nitelikli hali ya da unsuru olmayıp bağımsız suç tipleridir. Dolayısıyla 3. fıkra kapsamında yer alan sahte kart oluşturma hareketi 2. fıkrada olduğu gibi bir başkasının hesabı ile ilişkili olmak zorunda değildir. Bu açıdan örnekte de olduğu herhangi bir kişinin bilgileri kullanılmadan oluşturularak kullanılan kartlar bakımından 3. fıkranın söz konusu olabileceğini düşünüyoruz. Ancak bu kartlar kullanılmamış ve dolayısıyla herhangi bir yarar temin edilmemişse kartı üretme fiilini icra hareketi olarak değerlendirip suçta teşebbüsten bahsedebiliriz.

#### **4. Manevi Unsur**

Suçun manevi unsuru kasttır. Bu nedenle failin bilerek ve isteyerek hareket etmesi gereklidir. Suçun taksirli hali ise cezalandırılmamaktadır.

Bu maddede 765 sayılı TCK md. 525/b-2 hükmünden farklı olarak, failin belirli bir saikle hareket etmesi şartına yer verilmediğinden, suçun manevi unsurunda saik aranmamaktadır.

#### **5. Hukuka Aykırılık**

Hukuka aykırılık unsuru kapsamında varsayılan rıza değerlendirilebilir. Örneğin, yanında çalıştığı patronunun fatura borcunu gecikmeye düşmesin diye patronuna ait banka veya kredi kartı ile ödeyen kişi varsayılan rıza hukuka uygunluk nedeninden faydalanır.

#### **6. Suçun Özel Görünüş Şekilleri**

##### **a. Teşebbüs**

Banka ve Kredi Kartlarının Kötüye Kullanılması Suçu, teşebbüse elverişli bir suç tipidir. Teşebbüs bakımından, TCK md.245'in, 1 ve 3. fıkraları özellik arz etmektedir. Şöyle ki bu fıkralarda suçun tamamlanmış olması bakımından failin, kendisine veya üçüncü bir kişiye yarar sağlaması arandığından, yarar sağlanmamışsa suç teşebbüs aşamasında kalmış olacaktır<sup>94</sup>.

<sup>92</sup> YAŞAR/GÖKCAN/ARTUÇ Yorumlu Uygulamalı..., s.6808

<sup>93</sup> Yargıtay 11. CD 15.3.2011 tarih, E. 2010/16131, K. 2011/1406 sayılı kararında; "Failin kendisinin gerçeğe aykırı banka veya kredi kartı ürettiği ve sahte belgelerle bankaya banka veya kredi kartı ürettirdiği olayda, gerçeğe aykırı banka veya kredi kartı üretmek yahut sahte belgelerle bankaya sahte banka veya kredi kartı ürettirmek fiilinin TCK md.245/2'de düzenlenen suçta uygun olup TCK md. 245/3'te düzenlen sahte banka veya kredi kartı kullanarak yarar sağlamak" suçunun unsuru ya da ağırlatıcı nedeni olmayıp bağımsız suç olduğuna hükmetmiştir.

<sup>94</sup> Yargıtay 11. CD 20.9.2010 tarih, E.2010/9643, K.2010/9400 sayılı kararında; "Failin başkasına ait kimlikle oluşturduğu sahte kimlik Telekom'a başvurup telefon hattı ve internet bağlatması, yine oluşturduğu bu sahte kimlik ile kredi kartı başvurusunda bulunduğu olayda; "sanığın katılan A...bank'a müracaat ederek kredi kartı talebinde bulunduğu ancak başvurusunun sahte kimlikle yapıldığı ihbarı üzerinde sanığa herhangi bir teslimat yapılmadan ve kredi kartı henüz kullanılmadığından eylemin TCK.nun 245/3. Maddesindeki sahte kredi kartı kullanmaya teşebbüs suçunu oluşturmayacağı, kredi kartı sözleşmesi imzalandıktan sonra kredi kartı düzenlenmiş ise fiilin TCK.nun 245/2. madde ve fıkrasında öngörülen suçu oluşturacağı, sözleşme im-

**b. İştirak**

Bu suç iştirak açısından herhangi bir özellik göstermemektedir.

**c. İçtima**

Banka ve Kredi Kartlarının Kötüye Kullanılması Suçu, bir suç işleme kararının icrası kapsamında, değişik zamanlarda, aynı kişiye karşı, birden fazla kez işlenirse, fail, zincirleme suç hükümlerine göre tek bir suçtan cezalandırılacaktır<sup>95</sup>. Daha açık bir deyişle, fail tarafından başkasına ait kredi kartı, değişik zamanlarda birden fazla kez kullanıldığında, tek bir suçtan sorumluluk doğacak, ancak TCK md. 43/1 gereğince failin cezasında artırım yoluna gidilecektir.

Öte yandan kart taşıyıcısına ait birden fazla kartın kullanılması halinde zincirleme suç hükümlerinin uygulanacağı ileri sürülmüşse de<sup>96</sup> Yargıtay kullanılan kartı esas alarak kart sayısınca suçun oluştuğuna karar vermekte idi<sup>97</sup>. Nitekim Yargıtay 11. Ceza Dairesinin E.2009/22925, K.2010/11207, 14.10.2010 tarihli kararında da kartları düzenleyip veren banka sayısınca suç oluşacağı belirtilmiştir. Ancak Ceza Genel Kurulu'nun 18.10.2011 tarih ve 2011/6-166 E. numaralı kararında, bu husus şu şekilde değerlendirilmiş ve yukarıda yer verilen Yargıtay kararından farklı bir sonuca ulaşılmıştır: "Sanıkların eylemleri sonucu malvarlığında azalma meydana gelen, diğer bir ifade ile suçun mağduru olan kişi kart hamilidir. Kart hamilinin malvarlığına yönelik bu suçun banka veya kredi kartları aracılığıyla işlenmiş olması korunan hukuki yararın katılanın malvarlığı olduğu gerçeğini değiştirmeyecektir. Suçta kullanılan banka ve kredi kartlarının hangi bankaya ait olduğunun da suçun oluşumu bakımından bir önemi bulunmamaktadır. Suçun mağduru kart hamili olduğuna göre Özel Dairenin banka sayısınca suç oluşacağı yönündeki bozma nedeninde isabet bulunmamaktadır."

---

zalandıktan (sonra) fakat kartın düzenlenmemesi halinde ise TCK.nun 245/2. madde ve fıkrasında öngörülen suçun "teşebbüs aşamasında" kalacağı" na hükmetmiştir.

<sup>95</sup> "Sahte oluşturulan birden fazla kredi kartının kullanılması halinde eylemlerin her farklı banka kartı için ayrı ayrı suç oluşturup kartların birden çok kullanımı halinde her kart için zincirleme şekilde işlenen suç hükümlerinin uygulanması gerekmektedir." Yargıtay 11. CD. 16.02.2010 tarih, E.2009/22078, K.2010/1382. Yargıtay 11. CD 30.3.2011 tarih, E. 2011/450, K. 2011/1748 sayılı kararında;"Failin çeşitli bankalara ait kredi kartlarının manyetik şeritlerini kopyalama suretiyle oluşturmuş olduğu sahte kredi kartlarını kullandığı olayda TCK md. 245/2'de düzenlenen suçun oluştuğuna hükmetmiştir. Aynı bankaya ait birden fazla kartın kullanılmasında veya aynı bankaya ait bir kartın değişik zamanlarda kullanılması halinde zincirleme suç hükümlerinin uygulanacağına" karar vermiştir. Yine Yargıtay 11. CD. 30.03.2011 tarih, E.2011/450, K.2011/1748, kararında; "Sanığın, yabancı bankalara ait kredi kartlarının manyetik şeritleri kopyalanarak sahte olarak oluşturulmuş kredi kartlarını kabul etmek ve alışverişler yapmaktan ibaret eylemlerinde; kredi kartlarını çıkartan yabancı bankaların zarar görmesi nedeniyle mağdur olan yabancı banka sayısınca suçun oluşacağı, banka veya kredi kartlarının manyetik şeritlerinde yer alan ilk altı rakama ilgili katalogdan bakıldığında kartı çıkaran bankanın belirlenebileceği; sahte üretilen ve kullanılan kredi kartlarının manyetik şeritlerinde yapılan inceleme sonucu tespit edilecek bankalar sayısınca ve aynı bankaya ait birden fazla sahte kredi kartının ya da aynı bankaya ait kartın değişik zamanlarda birden fazla kullanılması halinde zincirleme biçimde ayrı ayrı suçların oluşacağı gözetilmeden, her bir kart ayrı eylem kabul edilerek karar verilmesi hukuka aykırıdır." şeklinde sonuca varmıştır.

<sup>96</sup> ÖZBEK, Banka ve Kredi Kartlarının Kötüye Kullanılması Suçu, s. 1056

<sup>97</sup> TEZCAN/ERDEM/ÖNOK, Teorik ve Pratik..., s.787

TCK md. 243'te düzenlenen bilişim sistemine girme suçunun bu suç içinde geçit suç niteliğinde<sup>98</sup> (görünüşte içtiman söz konusu) olduğu ileri sürülmektedir. Zira fail, elde ettiği kart ve şifre sayesinde her ne kadar görünüşte bilişim sistemine hukuka uygun olarak giriyor olsa da kartı çıkaran ve bilişim sisteminin sahibi olan banka ya da finans kurumu bu sisteme kart aracılığıyla "kartı hukuka uygun şekilde elinde bulunduran" kişilerin sisteme girmesini istemektedir; bunun dışında sahte kart ya da rızanın bulunmadığı durumlarda bilişim sistemine girişlerde öncelikle TCK md. 243 ihlal edilmiş olur<sup>99</sup>. Ancak burada tüketen norm olan md. 245'in uygulanması gerekir.

Banka ve Kredi Kartlarının Kötüye Kullanılması Suçunu düzenleyen TCK md. 245/3'ün haksız yarar sağlama suçunu düzenleyen TCK md. 244/4'e göre özel norm niteliğinde olduğu belirtilmektedir<sup>100</sup>. Böyle bir düzenleme olmazdı, 244/4 uygulama alanı bulurdu.

Benzer bir olasılık 245. maddenin kendi fıkraları arasında da olabilir. Daha net ifade etmek gerekirse, TCK md. 245/3 uyarınca sahte bir kartın kullanılması suretiyle yarar elde edilmesi durumunda TCK md. 245/2'deki suç, tüketilen norm niteliğinde olduğundan sadece TCK md. 245/3'ten ceza verilmesi gerekir<sup>101</sup>. Ancak başka bir görüşe göre; bir kişi hem sahte banka kartı üretmiş (veya bu niteliğini bilerek kabul etmiş) hem de bu kartı kullanmış ise, 245. maddenin ikinci ve üçüncü fıkrada ayrı ayrı cezalandırılmalıdır<sup>102</sup>. Yargıtay 11. Ceza Dairesinin 29.05.2007 tarih ve 2007/2538-2007/3738 nolu kararı da bu durumu şu şekilde ifade etmiştir: "*Başkalarına ait banka hesapları ile ilişkilendirilerek sahte banka veya kredi kartı üretmek ile sahte oluşturulan veya üzerinde sahtecilik yapılan bir banka veya kredi kartını kullanmak suretiyle kendisine veya başkasına yarar sağlamak suçlarının birbirinden bağımsız iki ayrı suç oluşturduğu gözetilmeyerek fikri içtima kurallarının uygulanması gerektiğinden bahisle tek suç kabulü ile eksik ceza tayini aleyhe temyiz olmadığından bozma nedeni yapılmamıştır*"<sup>103</sup>.

TCK md. 245'te "her ne surette olursa olsun ele geçirme" yer aldığından bu suç ile dolandırıcılık ve hırsızlığın birleşip birleşmeyeceği de tartışmalıdır. Doktrinde bir görüş kişinin dolandırıcılık yapmak suretiyle ele geçirdiği kartı kullanılmasyla menfaat temini söz konusu olsa da burada bilişim sistemleri aracılığıyla dolandırıcılık düşünülmemeyeceği için TCK md. 158/1'in değil, TCK md. 245/1'in uygulanması gerektiğini belirtmektedir<sup>104</sup>. Bu noktada kartın ele geçirilişi bakımından dolandırıcılık suçu, kullanılmasi bakımından ise TCK md. 245/1 uygulanacağını kabul eden görüş de vardır<sup>105</sup>. Bir diğer görüşe göre ise bu suçlar arasında tüketen-tüketilen norm ilişkisi olduğu için fail sadece banka veya kredi kartının kötüye kullanılması suçundan dolayı sorumlu olacaktır<sup>106</sup>. Konuya ilişkin olarak Yargıtay 30.03.2010 tarihli kararında; madde metninde yer alan "her ne surette olursa olsun" ifadesinin banka veya kredi

<sup>98</sup> PARLAR/AKIN/HATİPOĞLU, Bankacılık Ceza Hukuku, s.705

<sup>99</sup> DÜLGER, Bilişim Suçları, s.264

<sup>100</sup> TEZCAN/ERDEM/ÖNOK, Teorik ve Pratik..., s.788

<sup>101</sup> TAŞKIN, burada "geçit suçu" kavramını kullanmaktadır. TAŞKIN, Bilişim Suçları, s. 85

<sup>102</sup> YAŞAR/GÖKCAN/ARTUÇ Yorumlu Uygulamalı..., s.6808

<sup>103</sup> Hem söz konusu tartışmanın önüne geçmek hem de failin gereğinden fazla cezalandırılmasını engellemek bakımından üretmek ve kullanmak fiillerini TCK md. 204'te olduğu gibi seçimlik hareketler olarak düzenlemenin amaca daha uygun olduğunu düşünmekteyiz.

<sup>104</sup> TAŞKIN, Bilişim Suçları, s. 81

<sup>105</sup> ÖZBEK, Banka ve Kredi Kartlarının Kötüye Kullanılması Suçu, s.1044

<sup>106</sup> TEZCAN/ERDEM/ÖNOK, Teorik ve Pratik..., s.788

kartlarının sadece hukuka uygun yollardan ele geçirmesini kapsadığını, kartın ele geçirilmesi aşamasında başka bir suç örneğın hırsızlık suçı söz konusu ise hem hırsızlık suçundan hem de banka veya kredi kartının kötüye kullanılması suçundan hüküm kurulacağını belirtmiştir<sup>107</sup>. Nitekim 6. CD. 17.10.2006 tarih E.2004/1306, K.2006/9962 kararında çalınan kredi kartıyla deęişik işyerlerinden alışveriş yapılması durumunda hem hırsızlık hem de banka ve kredi kartlarının kötüye kullanılması suçundan ceza verileceđi belirtilmiştir. Diđer bir görüŖe göre, fail kredi kartını hırsızlık yapmak suretiyle elde etmişse, TCK md.44'ün devreye gireceđini ve failin TCK md.245/1'den sorumlu olacağı kabul edilmektedir<sup>108</sup>. Dolandırıcılık suçı bakımından doktrinde bir görüŖ, TCK md.244'ün yardımcı norm (tali norm) niteliğinde olduğundan bahisle olayda dolandırıcılık suçı oluşmuşsa failin asli norm olan dolandırıcılık suçundan sorumlu tutulması gerektiđini ileri sürmektedir<sup>109</sup>.

Konu hakkında bizim düşüncemiz ise Ŗu şekildedir; Banka veya kredi kartlarının kötüye kullanılması suçunun oluşabilmesi için başkasına ait banka veya kredi kartının bir şekilde ele geçirilerek suçun oluşumunda araç olarak kullanılıp yarar sağlama neticesinin gerçekleşmesi gerekmektedir. Bu durumda failin maddede belirtilen neticeye ulaşması hukuka uygun ya da hukuka aykırı yollardan kartı ya da bilgileri elde ederek mümkün olacaktır. Dolayısıyla Ŗayet kartın ele geçirilmesi hırsızlık, dolandırıcılık ya da yağma suretiyle gerçekleşmişse bu durum 245. madde bünyesinde bir icra hareketi olarak görülmeli ve yalnızca banka veya kredi kartlarının kötüye kullanılması suçunun gerçekleştiđi sonucuna varılmalıdır. TCK md. 245'in gerekçesinde de belirtildiđi üzere söz konusu suç tipi aslında hırsızlık, dolandırıcılık, güveni kötüye kullanma ve sahtecilik suçlarının ratio legislerinin tümünü içeren bağımsız bir suçtur.

Failin kendisine emanet edilen kredi kartını; güveni kötüye kullanarak, mağdurun rızası olmadan ya da verilen rıza sınırını aşarak kullanıp, haksız yarar sağlaması haline ilişkin olarak da çeşitli görüşler ileri sürülmüştür. Bu durumda TCK md. 44'e göre deęerlendirme yapılması gerektiđini savunanlar olduğđ gibi; kendisine emanet edilen kartı kullanma durumunda, kart sahibinin rızası olmadan kullanma unsuru gerçekleşmediğinden TCK md. 245/1'deki suçun deęil, güveni kötüye kullanma ya da hırsızlık suçlarının oluşacağını savunanlar da vardır. Başka bir görüŖe göre ise kredi kartı alışveriş yapıldığında bedelini ödeyebilme olanađı verdiğinden bir hak olarak güveni kötüye kullanma suçunu oluştıracaktır<sup>110</sup>.

Özel belgede sahtecilik suçunu düzenleyen TCK md. 207 ile TCK md. 245/3'ün birlikte uygulanıp uygulanamayacağı konusunda doktrinde bir görüŖ, kartın manyetik alanı üzerinde depolanmış bilgilerin belgede sahtecilik anlamında bir yazı olarak nitelendirilemeyeceğinden bahisle belgede sahtecilik ve banka veya kredi kartının kötüye kullanılması suçunun birlikte oluşmayacağı kabul etmektedir<sup>111</sup>. Banka veya kredi kartıyla ilgili bir başvuru formunu düzenleyerek sahte kart oluşturulmasını sağlayan ve bundan sonra da bu kartı kullanarak bankamatikten para çeken sanığın eylemi TCK md. 245/3 kapsamında deęerlendirilmesi gerekirken, eđer sanık bu kartı üye bir mağazada kullanmışsa TCK md. 207'nin oluşacağı ileri sürülmüştür. Yine bu durumda ayrıca dolandırıcılık suçunun da oluşacağı ve farklı neviden fikri içtima hükümler-

<sup>107</sup> CGK, 30.3.2010, 11-17/65; YENİDÜNYA/DEĞİRMENCİ, Mukayeseli Hukukta..., s. 47

<sup>108</sup> TAŞKIN, Bilişim Suçları, s. 81

<sup>109</sup> TEZCAN/ERDEM/ÖNOK, Teorik ve Pratik..., s.787-788

<sup>110</sup> TAŞKIN, Bilişim Suçları, s. 82

<sup>111</sup> TEZCAN/ERDEM/ÖNOK, Teorik ve Pratik..., s.787



rinin uygulanacağı kabul edilmektedir. TCK md. 212 uyarınca hem dolandırıcılık hem de özel evrakta sahtecilik suçundan ceza verilmesi gerekmekte ise de bu iki suçun toplam cezası TCK md. 245/3'ten düşük olduğundan TCK md. 44 gereği TCK md. 245/3 uygulanacaktır<sup>112</sup>.

## **7. Cezalandırılabilirliğin Diğer Koşulları**

### **a. Şahsi Cezasızlık Sebebi**

TCK md. 245/4 uyarınca, maddenin birinci fıkrasında 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 olarak işlenmesi halinde, ilgili akraba hakkında cezaya hükmolünmayacaktır.

### **b. Cezayı Kaldıran veya Azaltan Neden Olarak Etkin Pişmanlık**

TCK md.245/5'e göre, birinci fıkra kapsamındaki fillerle ilgili, malvarlığına karşı suçlara ilişkin etkin pişmanlığın düzenlendiği TCK md.168 uygulanacaktır.

Bu madde kapsamında failin etkin pişmanlıktan faydalanabilmesi için;

-Suçun tamamlanmış olması,

-Failin azmettirenin veya yardım edenin bizzat pişmanlık göstererek mağdurun uğradığı zararı aynen geri verme veya tazmin suretiyle tamamen gidermesi, kısmen giderme söz konusuysa mağdurun buna rıza göstermesi,

-Kovuşturmadan önce veya kovuşturma başlamışsa hüküm verilmeden önce aynen iade veya tazminin sağlanması gerekmektedir. Bu konuda aynen iade veya tazminin, ilk derece mahkemesi aşamasında hüküm verilinceye kadar mı yoksa Yargıtay'ca verilecek onama kararına kadar mı gerçekleşmesi gerektiği tartışmalıdır. Bizce ilk derece mahkemesine hüküm verilinceye kadar aynen iade veya tazminin sağlanması gerekir.

## **VI. UYGULAMADA BİLİŞİM SUÇLARININ BENZER SUÇLARLA ARASINDA ÇIKAN SORUNLARI VE YARGI KARARLARI IŞIĞINDA BU SORUNLARA İLİŞKİN DEĞERLENDİRMELERİMİZ**

Somut olayda bilişime ilişkin hususların mevcut olması, burada, bilişim suçlarının mı yoksa hırsızlık, dolandırıcılık veya güveni kötüye kullanma gibi klasik suçların mı uygulama alanı bulacağı tartışmasını beraberinde getirmektedir. TCK md. 244/4'teki "*yukarıdaki fıkralarda tanımlanan fiillerin işlenmesi suretiyle kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlamanın başka bir suç oluşturmaması*"ve TCK md. 245/3'deki "*daha ağır cezaı gerektiren başka bir suç oluşturmadığı takdirde*" şeklindeki ibareler de, söz konusu tartışmanın çıkış noktasını oluşturmaktadır.

Söyle ki, bu hükümlerde yer verilen tipik hareketin varlığından bahsedebilmek için, failin, kendisinin veya başkasının lehine haksız yarar sağlaması gerekir. Ancak TCK md. 244'den sorumluluk için fiil; başkaca bir suç, TCK md. 245'ten sorumluluk içinse, daha ağır cezaı gerektiren diğer bir suç oluşturmamalıdır. Bu suretle TCK md. 244 somut olaydaki hareket neticesinde gündeme gelecek başkaca suçlar, TCK md. 245 ise, fiil sonucu oluşacak daha ağır cezaı gerektiren suçlar karşısında tali norm niteliğindedir.

<sup>112</sup> TAŞKIN, Bilişim Suçları, s. 87

Esasında buraya kadar olan kısım gayet açıktır. Fakat TCK'daki birçok klasik suç tipine, içinde bilişimle ilgili hususların geçebileceği örnekler vermenin mümkün olduğu ve hatta bazılarında suçun bilişim suretiyle işlenmesinin nitelikli bir hal olarak yasada açıkça öngörüldüğü düşünülürken, konu karmaşık bir hal almaktadır. Böylelikle somut olayda, TCK md. 243, TCK md. 244 veya md. 245'in mi, yoksa diğer bir suçun mu oluştuğunun tespiti güçleşmektedir. Bu nedenle, her ne kadar bazı vakalarda bir ayrım yapmak çok kolay gözükmesine de, teorik olarak, bu suç tipleriyle bilişim suçları arasındaki ince çizgiyi iyi izah etmek gerekmektedir. Bizde çalışmamızda bu başlık altında, bilişim suçlarıyla diğer suç tiplerinin farkını, yargı kararları ışığında açıklamak isteriz.

### **A. Bilişim Sisteminin Kullanılması Suretiyle İşlenen Hırsızlık Suçu**

Zilyedinin rızası olmadan başkasına ait taşınır bir malı, kendisine veya başkasına bir yarar sağlamak amacıyla bulunduğu yerden alan kişinin cezalandırıldığı hırsızlık suçunda<sup>113</sup> yasa koyucu, tipik hareketin bilişim vasıtasıyla gerçekleşmesini, cezayı ağırlaştırıcı nitelikli bir hal olarak düzenlemiştir. Maddede bu şekilde yer verilen bilişim hususu, TCK 244/4'deki "*yukarıdaki fıkralarda tanımlanan fiillerin işlenmesi suretiyle kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlamasının başka bir suç oluşturması*" baresi dolayısıyla, somut olayda hırsızlık suçunun gerçekleşip gerçekleşmediği bakımından da bir inceleme yapılmasını gerekli kılmıştır.

Ancak bu konuda doktrinde farklı görüşler ileri sürülmüştür. Bir görüşe göre, "Hırsızlık suçunun bilişim sistemlerinin kullanılması suretiyle işlenmesinin, TCK'nın 244 hükmü karşısında mümkün olmadığını, çünkü hırsızlık suçunun konusunu "taşınır bir malın" oluşturduğunu, ancak hırsızlığın bilişim sistemlerinin kullanılması suretiyle işlendiği iddia edilen her durumda esasen işlenen suçun konusunun taşınır bir mal değil, duruma göre TCK md. 244/2-3 ya da 4. fıkranın uygulama alanı bulabileceğidir"<sup>114</sup>.

Diğer bir görüş ise, "Kanunun, hırsızlık ve dolandırıcılık suçlarının bilişim sistemleriyle işlenmesi ihtimallerini de nitelikli hal olarak düzenlediğini, ancak düzenlenmesine hiçbir şekilde katılmadığı bu nitelikli hallerin, bir yandan uygulayıcıları ikileme sokacağı gibi bir yandan da suçta ve cezada kanunilik ilkesi gereği bir iki ihtimalin dışında uygulama imkânı bulamayacağını, bilgisayar tarafından üzerinde işlem yapılabilen bir değer ifade eden 'verinin' taşınabilir bir mal olmadığını ve ekonomik değer taşıyan enerji kavramı gibi ayrıca tanımlanmadığı için bilgisayar marifetiyle yapılan haksız kazanç edimi eylemleri bakımından hırsızlık suçunu uygulayabilmenin mümkün olmayacağını, bu ihtimalin olsa olsa bir bilişim sistemine veya uygulamasına bağlanmış bir kasanın veya bir kapının açılması suretiyle buralardan yapılan hırsızlık fiilleri bakımından söz konusu olabileceğini ki, bu ihtimalleri nitelikli hal kabul etmenin de mantıklı bir izahının bulunmadığını"<sup>115</sup> belirtir.

<sup>113</sup> Hırsızlık suçuyla ilgili ayrıntılı bilgi için bakınız; TEZCAN/ERDEM/ÖNOK, Teorik ve Pratik..., s.502-548; SOYARSLAN Doğan, **Ceza Hukuku Özel Hükümler**, Ankara, 2010, s.363-392; ÖZBEK Veli Özer, **Yeni Türk Ceza Kanunu Anlamı**, Ankara, 2008, s.970-1045

<sup>114</sup> ÖZBEK, Banka ve Kredi Kartlarının Kötüye Kullanılması Suçu, s.1058-1059

<sup>115</sup> YAZICIOĞLU Yılmaz, **Yeni Türk Ceza Kanunu'ndaki Bilişim Suçlarının Genel Değerlendirmesi**, Yeni Türk Ceza Kanunu Sempozyumu, 5 Mart 2005, s.106; YAZICIOĞLU, Bilişim Suçları, s.144

Bu husustaki bir başka görüşe göre; “Bilişim sistemiyle hukuka aykırı yarar sağlama eylemlerinin, genellikle bilişim suçları veya dolandırıcılık suçları kapsamında değerlendirilebileceği, gelişen teknolojiyle birlikte değişen suç türleri nedeniyle bilişim hırsızlığı suçuna yer verilmesinin gerekli bulunduğu, ancak bu suçun bağımsız bir suç tipi olarak düzenlenerek, hangi eylemleri kapsayacağını açıkça belirlenmesi gerektiği, bilişim sistemini kullanmak suretiyle hırsızlık suçunu düzenleyen hükmün uygulamasının bir iki örnek dışında imkânsız olduğu<sup>116</sup>” kabul edilmektedir.

Aksi yönde bir görüşe göre ise; “Başkasının banka hesabına internet üzerinden girerek bu hesaptan failin kendisi veya başkasının hesabına para aktarması şeklinde gerçekleşen olaylarda da bilişim sistemlerini kullanarak hırsızlık veya dolandırıcılık suçlarının unsurları itibariyle gerçekleşip gerçekleşmediğinin tartışılması gerektiği<sup>117</sup>” ileri sürülmüştür.

Bir diğer görüşe göre de; “244/4. maddedeki suçun maddi unsurunun gerçekleştiğinden bahsedebilmek için failin; a) Bir bilişim sisteminin işleyişini engellemek veya bozmak suretiyle kendisinin veya başkasının yararına haksız bir çıkar sağlaması, b) Bir bilişim sistemindeki verileri bozmak, yok etmek, değiştirmek veya erişilmez kılmak, sisteme veri yerleştirmek, var olan verileri başka bir yere göndermek suretiyle kendisinin veya başkasının yararına haksız bir çıkar sağlaması gerekmektedir. İncelenmekte olan Yargıtay kararında ise; sanıkların, müştekiye ait banka hesabındaki parayı 244/1 ve 2. fıkralarında sayılan eylemlerden herhangi bir tanesinin gerçekleştirerek kendi hesaplarına geçirmedikleri görülmektedir. Yani sanıklar söz konusu hesaba girmek ve içerisindeki paraları almak için yukarıda sayılan eylemlerden hiçbirini yapmamışlardır. Ne bir bilişim sisteminin işleyişini engellemişler veya bozmuşlar, ne bilişim sistemindeki verileri bozmuşlar, yok etmişler, değiştirmişler, erişilmez kılmışlar, ne de sisteme veri yerleştirmişler ya da var olan verileri başka bir yere göndermişlerdir. Sadece katılana ait internet hesabına girmek suretiyle hesapta bulunan parayı almışlardır. Dolayısıyla sanıkların eylemini, TCK md. 244/4. maddesindeki normun ihlali şeklinde değerlendirmek imkânı bulunmadığı<sup>118</sup> kabul edilmektedir.

Söz konusu tartışma bakımından, failin başkasının banka hesabına internet üzerinden girerek bu hesaptan kendisi veya başkasının hesabına para aktarması şeklinde gelişen olayda, bilişim sistemlerini kullanarak hırsızlık suçunun oluşabileceğini düşünmekteyiz<sup>119</sup>. Bu olasılıkta veri hırsızlık suçunun

<sup>116</sup> DÜLGER, Bilişim Suçları s.289-290

<sup>117</sup> KOCA Mahmut, **Yargıtay Kararları Işığında Bilişim Sistemlerinin Kullanılması Suretiyle Haksız Yarar Sağlama Suçları**, Prof. Dr. Ali Güzel’e Armağan, C. II, İstanbul, 2010, s.1657.

<sup>118</sup> EVİK, Ali Hakan, **“İşleme ve Bilgiye Dayalı Manipülasyon Suçları”**, Prof. Dr. Uğur Alacakaptan’a Armağan, İstanbul, İstanbul Bilgi Üniversitesi Yay., 2008

<sup>119</sup> Yargıtay 11. CD 06.10.2010 tarih, E.2010/4946, K.2010/10749 sayılı kararında; “ATM’den para çekmeye çalışan mağdura yardım etme bahanesiyle yaklaşıp, ATM’ye kartı yerleştirip, mağdurun şifreyi girmesinden sonra hesapta bulunan parayı mağdura fark ettirmeden çekip, sonra da paramı vermiyor diyerek kartı geri veren failin eyleminin hırsızlık suçunu oluşturduğuna” hükmetmiştir. Yargıtay 11.CD 31.3.2011 tarih, E. 2011/821, K. 2011/1777 sayılı kararında;” ATM’den para çekmek isteyen mağdurun yardım isteği üzerine mağdurun kartını alıp şifresini öğrenerek ATM’den para çekmesi ancak çekilen parayı el çabukluğu ile cebine koyup ATM’nin para vermediği başka bir ATM’ye gidilmesi gerektiğini söyleyip, yolda giderken aniden mağdurun yanından uzaklaşan failin failinin hırsızlık suçunu oluşturduğuna hükmetmiştir. Banka veya kredi kartının kötüye kullanılması suçu ile karşılaştırma yapan Yargıtay, banka veya kredi kartlarının kötüye kullanılması suçunda banka veya kredi kartının

konusu olmayıp, suçun tamamlanması açısından, bir araç niteliğindedir. Şayet fail sadece veriyi taşıma amacı güdüyorsa ve hırsızlık suçunun konusu dışında bir menfaat temin ediyorsa, TCK md. 244/4'ün ihlalden söz edilecektir<sup>120</sup>.

Yargıtay Ceza Genel Kurulu da 17.11.2009 tarih 2009/11-193E., 2009/268E. sayılı kararında bu görüşümüzü destekleyerek “Sanık Volkan’ın, firari Saim ile birlikte hareket ederek, daha önceden haksız bir şekilde ele geçirdikleri katılan firmanın internet bankacılık şifresini kullanmak suretiyle, katılanın Ş Bank Ankara K... Şubesindeki hesabından 10.750 YTL’yi Ş...Bank İstanbul Z Şubesinde sanık Volkan adına açtırdıkları hesaba havale edip, aynı gün banka hesabında bulunan, taşınır nitelikteki parayı bilişim sistemini kullanmak suretiyle kendi hesaplarına geçirmeye, katılanın rızasına aykırı olarak mal varlığında azalmaya neden olmaya; başka bir anlatımla var olan veriyi başka bir yere göndermekten ziyade, bu verinin temsil ettiği parayı alarak mal edinmeye yöneliktir. Kaldı ki sanığın katılanın internet bankacılık hesabında bulunan parasına ulaşmak için bilişim sistemlerini araç olarak kullanmaktan başka alternatifi de yoktur. Dolayısıyla olayımızda, 5237 sayılı TCK’nın 142/2-e maddesinde düzenlenmiş bulunan “bilişim sistemi kullanılmak suretiyle hırsızlık” suçunun gerçekleştiği kabul edilmelidir. Şu halde, sanığın eyleminin 5237 sayılı TCK’nın 142/2-e maddesindeki nitelikli hırsızlık suçunu oluşturduğunun kabul edilmesi karşısında, 244. Maddenin 4.fıkrası uyarınca uygulama yapma olanağı da bulunmamaktadır.” şeklinde karar vermiştir<sup>121</sup>.

Bunun dışında, sadece bankamatik kartının, hamilinin rızası dışında ele geçirilmesinin, hırsızlık suçunu oluşturup oluşturmayacağı konusu da bir başka tartışmaya yol açmıştır. Bu bakımdan da kartın anılan suç anlamında “mal” sayılıp sayılmayacağının üzerinde durulmalıdır.

Bizce bankamatik kartı, ilişkin olduğu hesaptaki parayı yansıtmamaktadır. Başka bir ifadeyle kart kullanılmadığı müddetçe, sahip olduğu ekonomik

---

rızaya aykırı olarak kullanılması söz konusudur. Ancak somut olayda fail, mağdurun rızasına dayanarak kartı kullandığı için TCK md. 245’te tanımlanan banka veya kredi kartlarının kötüye kullanılması suçunu oluşturmayacaktır.” demektedir. Kanaatimizce bu olayda Yargıtay’ın dolandırıcılık suçunu da tartışması gerekirdi. Çünkü fail, ATM’nin para vermediğini söyleyerek ATM ve banka kartı kullanımında pek fazla bilgisi olmayan mağduru yanılgıya uğratmıştır. Dolayısıyla bir aldatma söz konusudur. Bu durumda dolandırıcılık suçunun da tartışılması gerekmektedir.

<sup>120</sup> Yargıtay Ceza Genel Kurulu 17.11.2009 tarih, E.2009/11-193, K.2009/268 sayılı kararında; “Daha önceden haksız bir şekilde ele geçirdikleri internet bankacılığı şifresinin kullanılması suretiyle faillerden birisinin hesabına para transferi yaptığı olayda, failerin “kastı, katılan firmanın banka hesabında bulunan taşınır nitelikteki parayı bilişim sistemini kullanmak suretiyle kendi banka hesaplarına geçirmeye, katılanın rızasına aykırı olarak malvarlığında azalmaya neden olmaya, başka bir anlatımla var olan veriyi başka bir yere göndermekten ziyade, bu verinin temsil ettiği parayı alarak mal edinmeye yöneliktir. Kaldı ki sanığın, katılanın internet bankacılık hesabında bulunan parasına ulaşmak için bilişim sistemlerini araç olarak kullanmaktan başka alternatifi de yoktur.” Yargıtay bu kararında failerin fiillerinin bilişim sistemi kullanılmak suretiyle hırsızlık suçunu oluşturduğuna hükmetmiştir. Ancak çoğunluk görüşüne katılmayan üye karşı oy yazısında verilerin taşınabilir mal kavramına girmediği, failin bilişim sistemine girdikten sonra oradaki verileri başka bir hesaba göndermiş olduklarından TCK md.244/4’te düzenlenen verileri başka bir yere göndermek suretiyle haksız çıkar sağlama suçunun oluşacağını” belirtmiştir.

<sup>121</sup> Yargıtay 6. CD. 02.06.2008 tarih, E.2008/55, K.2008/12249 sayılı kararında, somut olayda hırsızlık suçunun ne zaman tamamlanmış sayılacağı hususunda, “Bilişim sisteminin kullanılması suretiyle işlenen hırsızlık suçunun, sanık tarafından yakınının hesabına havale edilmesi anında tamamlandığı gözetilmelidir.” şeklinde görüş bildirmiştir.

değerin bir önemi bulunmamaktadır. Paraya ulaşmak noktasında sadece bir anahtar işlevi görmektedir. Böylelikle de hırsızlık suçunun oluştu-  
maktan değil, başka bir suçun vasıtası olarak kabul etmek daha isabetli bir  
yorum tarzıdır. Bu nedenle de failin üzerinde sadece kartın yakalanmış, he-  
saptan henüz hiç para çekilmemiş olmasının, bizce Banka ve Kredi Kartlarının  
Kötüye Kullanılması Suçu anlamında icra hareketi kabul edilip, teşebbüs aş-  
masında kalmış bir fiil şeklinde değerlendirilmesi gerekir. Hatta failin kartı ele  
geçirmesinin üzerinden çok uzun zaman geçmişse, failin burada bir gönüllü  
vazgeçme içinde olduğu dahi düşünülebilir.

Bu hususlar, somut olayda hırsızlık suçunun oluşup oluşmadığına iliş-  
kindi. Bundan başka bir de, örneğin; kurduğu düzenekle ATM makinesine para  
çekmek için gelen kişinin şifresini öğrenip, bankamatik kartını ele geçiren ve  
sonrasında başka bir ATM cihazına giderek parayı çeken kişinin, sadece bilişim  
suçundan mı, yoksa hem bilişim hem de hırsızlık suçundan mı cezalandırıl-  
cağı konusunun da üzerinde durmak gerekir. Yüksek Mahkeme vermiş oldu-  
ğumuz örneğin benzerini, 30.03.2010 tarih, 2010/11-17E., 2010/65K. sayılı  
Ceza Genel Kurul Kararı'nda inceleyerek; " *Sanığın kurduğu düzenek ile ATM  
makinesine para çekmek için gelen mağdurların şifresini de öğrenmek suretiyle  
ele geçirdiği, ekonomik değeri bulunduğu kuşku bulunmayan menkul mal  
niteliğindeki banka kartı ile başka bir ATM cihazına gidip para çekmesi şeklinde  
gerçekleştirdiği eylemlerinde, banka veya kredi kartının kötüye kullanılması  
suçu yanında hırsızlık suçu da oluşmaktadır. Çünkü 5237 sayılı Yasa'nın 245/1.  
maddesinde düzenlenen banka veya kredi kartlarının kötüye kullanılması suçu-  
nun yasadaki düzenleniş şekli göz önüne alındığında bileşik suç olarak düzen-  
lenmediği görülmektedir. Banka veya kredi kartının kötüye kullanılması suçu ile  
birlikte oluşabilecek diğer suçlara yasadaki öngörülen ceza miktarları da, bu su-  
çun bileşik suç olarak düzenlenmediğini açıkça ortaya koymaktadır. Bu nedenle,  
banka veya kredi kartının hukuka aykırı olarak ele geçirilmesi durumunda oluş-  
abilecek hırsızlık, yağma, güveni kötüye kullanma, dolandırıcılık gibi suçlar ile  
banka veya kredi kartlarını kötüye kullanma suçu arasında gerçek içtima kuralı  
uygulanarak fail her bir suçtan ayrı ayrı cezalandırılmalıdır. Bu açıklamalar ışık-  
ğında birinci uyumsuzluk konusu değerlendirildiğinde; 5237 sayılı TCK'nın  
245/1. maddesindeki Banka veya Kredi Kartlarını Kötüye Kullanma Suçu bileşik  
suç olarak düzenlenmemiş olup, yasa maddesinde geçen "her ne surette olursa  
olsun" ifadesi banka veya kredi kartlarının sadece hukuka uygun yollardan ele  
geçirilmesini kapsamaktadır. Sanığın kurduğu düzenek ile ATM makinesine para  
çekmek için gelen mağdurların şifresini de öğrenmek suretiyle ele geçirdiği, eko-  
nomik değeri bulunduğu kuşku bulunmayan menkul mal niteliğindeki banka  
kartı ile başka bir ATM cihazına gidip para çekmesi şeklinde gerçekleştirdiği ey-  
lemlerinde, banka veya kredi kartının kötüye kullanılması suçu yanında hırsızlık  
suçu da oluşmaktadır." sonucuna varmıştır.*

Bizce Yüksek Mahkemenin varmış olduğu bu sonuç, bir önceki parag-  
rafta incelediğimiz şekilde olayda bir hırsızlık suçunun oluşmadığından bahisle  
yerinde değildir. Biraz daha açacak olursak; sanığın kurduğu düzenekle katıla-  
nın bankamatik kartını ele geçirmesi fiilinde, kartın ekonomik değerinin bir  
önemi olmadığı için, hırsızlık suçunun konusunu teşkil etmeyecektir. Burada  
olsa TCK md. 245'te düzenlenen banka ve kredi kartlarının kötüye kulla-  
nılması suçuna teşebbüs bakımından bir tartışma yapılabilecektir. Olayda vü-  
cut bulmayan hırsızlık suçuna, TCK md. 245 ile birlikte gerçek içtima uygu-  
lanması ise bizce doğru bir yol değildir.

### **B. Bilişim Sistemlerinin, Banka veya Kredi Kurumlarının Araç Olarak Kullanılması Suretiyle İşlenen Dolandırıcılık Suçu**

Dolandırıcılık suçunda yasa koyucu, tipik hareketin bilişim sistemlerinin, banka veya kredi kurumlarının araç olarak kullanılması suretiyle gerçekleşmesini, cezayı ağırlaştıran nitelikli bir hal olarak düzenlemiştir<sup>122</sup>. Maddede bu şekilde yer verilen bilişim hususu, TCK md. 244/4'deki *“yukarıdaki fıkralarda tanımlanan fiillerin işlenmesi suretiyle kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlamasının başka bir suç oluşturulmaması”* ibaresi dolayısıyla, somut olayda dolandırıcılık suçunun gerçekleşip gerçekleşmediği bakımından da bir inceleme yapılmasını gerekli kılmıştır<sup>123</sup>. Böylelikle de hangi hallerde dolandırıcılık, hangi hallerde ise TCK 244. maddedeki suç tipinin olduğu hususunun açığa kavuşturulması gerekmektedir.

Açıklayacak olursak, genel olarak hileli davranışlarla bir kimseyi aldatıp, onun veya başkasının zararına olarak, kendisine veya başkasına yarar sağlayan kişinin cezalandırıldığı dolandırıcılık suçunda, suçun maddi unsurunu oluşturan hareketin, **gerçek bir kişiye yöneltilmiş olması**, onun kandırılarak çıkar sağlanması gerekir<sup>124</sup>. Bilişim sistemlerinin araç olarak kullanılması suretiyle dolandırıcılık suçunda da, verileri toplayıp yerleştirdikten sonra bunları otomatik işlemlere tabi tutma olanağını veren manyetik sistemler vasıta-

<sup>122</sup> Dolandırıcılık suçuyla ilgili ayrıntılı bilgi için bakınız; TEZCAN/ERDEM/ÖNOK, Teorik ve Pratik..., s.589-617; SOYARSLAN, Ceza Hukuku Özel Hükümler, s.416-422; ÖZBEK, Yeni Türk Ceza Kanunu'nun Anlamı, s. 1204-1288

<sup>123</sup> Yargıtay Ceza Genel Kurulu 27.5.2008 tarih, E. 2008/11-87, K. 2008/150 sayılı kararında; “Failin başkasına ait nüfus cüzdanını kullanarak banka görevlilerince basımını sağladığı kredi kartını kullanarak alışveriş yapması, nakit para çekmesi olayında basımın yapılan ve failin kullanmış olduğu kredi kartının “sahte oluşturulan” kart niteliğinde olduğu, bu kartın kullanılması ile de TCK md. 245/3'te düzenlenen suçun oluştuğu, aynı zamanda dolandırıcılık suçunu (TCK md. 158/1-j) oluşturduğu, ancak md.245'te daha ağır bir cezayı gerektiren suç oluşmadığı takdirde md.245/3'ün uygulanacağı düzenlenmiş olduğundan ve dolandırıcılık suçunun bu özel hükme göre daha az ceza gerektirmesi nedeniyle dolandırıcılık suçunun olaya uygulama olanağı olmadığına” hükmetmiştir.

<sup>124</sup> Yargıtay 11. CD 24.11.2009 tarih, E.2007/849, K.2009/14539 sayılı kararında; “başkasına ait kredi kartı bilgilerinin temin ederek internette satış yapan elektronik mağazasından alışveriş yapmasında dolandırıcılık suçunun oluşmayacağına hükmetmiştir. Yargıtay'a göre dolandırıcılık suçunun oluşabilmesi için gerçek kişilerin aldatılarak bir çıkar sağlanmalıdır. Gerçek kişilerle yüz yüze gelmeden, telefonda konuşmadan, her hangi bir şekilde temas olmadan sadece bilişim sisteminin kullanılması suretiyle çıkar sağlanması halinde dolandırıcılık suçunun oluşmayacağı” sonucuna varmıştır. Yargıtay 11. CD 20.9.2006 tarih, E.2006/2696, K.2006/7334 sayılı kararında; “ATM'ye kurdukları düzenek ile mağdurun bankamatik kartının ATM'ye sikkışmasını sağlayıp, daha sonra kendilerini banka görevlisi olarak tanıtarak kartın şifresini öğrenip, mağdura kartı iptal edeceğini söyleyerek ATM'den uzaklaşmasını bekleyip daha sonra bankamatik kartı kullanılarak para çekilmesi eyleminin dolandırıcılık suçunu oluşturduğuna” hükmetmiştir. Yargıtay 11. CD 22.6.2010 tarih, E. 2008/11089, K.2010/7131 sayılı kararında; “Failin üye işyeri olarak katılan bankaya başvuruda bulunduğu, bunun üzerine pos cihazı aldığı, bilgileri ele geçirilen kredi kartları ile de alışveriş yapılmış gibi slip çektiği olayda; “dolandırıcılık suçunun unsuru olan aldatıcı hareketlerin gerçek kişiye yönelmesi ve gerçek kişinin hataya düşürülerek kendi veya başkasının malvarlığı aleyhine, sanık veya bir başkasının lehine bir işlemde bulunmaya yöneltilmesi ve bu işlem sonucunda sanığın kendine veya başkasının yararına haksız bir menfaat sağlanması gerekir. Somut olayda....dolandırıcılık suçunun unsurları oluşmamıştır.”, “...başkasına ait kredi kartının, kart sahibinin rızası dışında kullanılarak yarar sağlanmasının ..... 5237 sayılı TCK'nın 245/1 maddesine uygun bulunduğu...” yönünde karar vermiştir.

ıyla **gerçek kişiler aldatılıp çıkar sağlanmaktadır**. Buna karşılık gerçek bir kişi ile karşı karşıya gelmeden, yüz yüze veya telefon, bilgisayar, bilgi geçer gibi başka bir vasıta kullanılarak görüşmeden, konuşmadan, kişilere yönelik hileli davranışlarla aldatılmadan sadece bilişim sistemi kullanılarak doğrudan doğruya çıkar elde edilmesi durumunda, bilişim sistemine girerek haksız çıkar sağlama suçu oluşmaktadır<sup>125</sup>.

Teorik kısım böyle olmakla birlikte, konunun daha iyi anlaşılması için uygulamada sıklıkla rastlanabilecek bazı durumları nakletmek isteriz. Söz gelimi, **mal alımı için kendisine gelen satıcının mobil POS'undan kredi kartı ödemesi yapacak müşterinin, kartını satıcıya vermesinin ardından, satıcının hileli hareketlerle alıcıyı kandırıp, müşteri bilgilerini ele geçirmesi ve kendisine haksız menfaat temin etmesi durumunda** “Bilişim Sistemlerinin Araç Olarak Kullanılması Suretiyle Dolandırıcılık Suçu” (TCK md.158/1-f) söz konusu olacaktır. Çünkü yukarıda da ifade ettiğimiz üzere, dolandırıcılık suçunda fail, hileli davranışlarla bir kimseyi aldatıp, onun veya başkasının zararına olarak, kendisine veya başkasına yarar sağlamaktadır. Anılan suçun maddi unsurunun oluşması için, hareketin **gerçek bir kişiye yöneltilmiş olması**, onun kandırılarak çıkar sağlanması gerekmektedir. Suçun bilişim marifetiyle işlenmesi ise bu suç tipi için TCK 158. maddede öngörülen cezayı artıran nitelikli hallerden biridir. Bu suretle burada da gerçek kişiye yöneltilmiş bir hileli hareket ve bu fiilin gerçekleşmesi için bir bilişim aracı olan pos cihazı vasıta olarak kullanıldığı için TCK md.158/1-f'nin varlığından bahsedilecektir.

Diğer taraftan uygulamada yine sık rastlanan bir dolandırıcılık türü de Phishing siteleri aracılığıyla yapılmaktadır. Kısaca açıklayacak olursak; örneğin müşteriye, bankası ya da bankalar adına inandırıcılığı yüksek bir kurumdan elektronik posta iletisi gönderilmektedir. İletide on-line bankacılık hesabının hizmet süresinin bittiği, bunun için aşağıdaki linke tıklayarak gerekli işlemleri yapması istenmektedir. Ya da TC Merkez Bankası veya T. Bankalar Birliği adına gönderilen bir uyarı mesajı ile müşteri bir adrese yönlendirilmekte ve tıpkı phishingde olduğu gibi müşterinin bilgileri ele geçirilmektedir<sup>126</sup>. Görüldüğü üzere burada da hileli davranışlarla **gerçek bir kişi** aldatıp, onun zararına olarak, fail yarar sağladığı ve yine bilişim vasıta kılındığı için TCK 158/1-f'de düzenlenen “Bilişim Sistemlerinin Araç Olarak Kullanılması Suretiyle Dolandırıcılık Suçu” söz konusudur.

Fakat başkasına ait kredi kartı bilgilerini öğrenen kişinin, elektronik eşya alım satımı yapan bir şirketin internet sitesine girerek, elektronik ortamda “mail order” yoluyla mal siparişinde bulunması ve “mail order” formlarına başkasına ait kredi kartı bilgilerini yazarak satıcı firmaya, şikâyetçinin hesabından ödeme yapılmasını sağlayıp kargoyla gönderilen malları teslim alması<sup>127</sup> olayında dolandırıcılıktan değil, TCK 245. Maddedeki Banka ve Kredi Kartlarının Kötüye Kullanılması Suçunun varlığından bahsedilecektir. Çünkü burada fail

<sup>125</sup> ÖZBEK, Banka ve Kredi kartlarının Kötüye Kullanılması Suçu, s.1059; YAZICIOĞLU, Bilişim Suçları, s.144. Yargıtay 11. CD 10.10. 2006 tarihli kararında;” failin, mağdura ait kredi kartını hırsızlık suretiyle ele geçirdikten sonra, değişik iş yerlerinde farklı zamanlarda alışveriş yapması dolandırıcılık suçunu değil, TCK md. 245'te düzenlenen banka veya kredi kartlarının kötüye kullanılması suçunu oluşturduğu” yönünde karar vermiştir.

<sup>126</sup> Konu hakkında bilgi için bakınız; ILDIR Ece, **Bankacılıkta Bilişim Suçları, Banka ve Finans Hukuku**, Panel ve Seminer Notları, İstanbul Barosu, İstanbul, 2009, s.290-292

<sup>127</sup> Bu örnek olay, Yargıtay 11. CD.'nin, 24.11.2009 tarih, E.2007/849, K.2009/14539 sayılı kararından alınmıştır.

bir başkasının kart bilgileri vasıtasıyla alışveriş yapmakta ve satış bedelinin, suçtan zarar gören şikâyetçinin kredi kartı hesabından ödenmesi sağlamaktadır. Başka bir deyişle **gerçek bir kişi ile karşı karşıya gelmeden, yüz yüze veya telefon, bilgisayar, bilgi geçer gibi başka bir vasıta kullanılarak görüşmeden, konuşmadan, kişilere yönelik hileli davranışlarla aldatılmadan** sadece bilişim sistemi kullanılarak doğrudan doğruya çıkar elde edilmektedir<sup>128</sup>.

### C. Yağma Suçu

Tehdit veya cebir kullanarak bir malı teslim etme ya da malın alınmasına karşı koymamaya mecbur bırakma fiilleri ile oluşan yağma suçunun bilişim sistemini kullanmayı sağlayan karta yönelik olması durumunda, kartın ele geçirilmesi ve kullanılması bakımından hangi hükümlerin uygulanması gerekeceği tartışmalıdır. Bir görüşe göre suçun oluşması için kartın ne şekilde ele geçirilmiş olduğunun önemi olmadığından TCK md. 245/1 uygulanacaktır. İkinci bir görüşe göre bu tip durumlarda ihlal edilen yağma ve banka veya kredi kartlarının kötüye kullanılması suçları arasında fikri içtima kuralı TCK md. 44 gereği en ağır cezayı gerektiren suçtan hüküm kurulacaktır<sup>129</sup>. Yargıtay Ceza Genel Kurulunun 2011/6-166 sayılı kararına konu olayda yağma ile mağdurun hem parasına hem de çeşitli bankalara ait banka ve kredi kartlarına el konulduğu, daha sonra ATM cihazlarından farklı zamanlarda para çekimlerinin olduğu anlaşılmaktadır. Olay bakımından yağma suçunun bütün unsurları gerçekleşmiş olduğundan yani suç sadece kartın ele geçirilmesi bakımından değil tüm olay kapsamında olduğundan yukarıdaki tartışma gündeme gelmemiştir. Ancak daha önce de belirtildiği üzere Yargıtayın, kartın hırsızlık ve dolandırıcılık vasıtası ile elde edilmesi hallerinde hem bu suçlardan hem de bilişim suçlarından cezalandırma yolunu seçtiği düşünülürse yağma bakımından da aynı sonuca ulaşılacağı söylenebilir.

Kartın yağma yoluyla elde edilmesi konusunda bizim değerlendirmemiz ise şu şekildedir: Hırsızlık ve dolandırıcılık suçlarında da ifade edildiği üzere failin yağma suretiyle banka ve kredi kartlarını alması ve devamında bilişim sistemine girip haksız menfaat elde etmesi hareketini TCK md. 245'in ihlali olarak görmekteyiz. Başka bir ifade ile cebir ve tehdit hareketlerini TCK md. 245'in icra hareketi olarak değerlendirmekteyiz. Çünkü madde metninde yer alan kartın 'her ne suretle olursa olsun' ele geçirilmesi ifadesinin yalnız hukuka uygun değil hukuka aykırı kazanımları da bünyesine aldığı kanısındayız<sup>130</sup>.

Ancak fail bilişim sistemine girmediği takdirde gerçekleşen cebir veya tehdit fiilleri bakımından iki durum söz konusu olabilir. Öncelikle bilişim sistemine girememeye, suçun elde olmayan nedenlerle tamamlanamamasından

<sup>128</sup> Yargıtay 11. CD. 22.06.2010 tarih, 2008/11089E., 2010/7131K. sayılı kararında da "Sanığın katılan bankaya üye işyeri olarak başvurup pos cihazı aldığı, fikir ve eylem birliği içinde, bilgileri ele geçiren kredi kartları ile sahiplerinin izni olmaksızın alışveriş yapılmış gibi slip çıktıkları olayda, dolandırıcılık suçunun hile unsurunun oluşmadığı, eylemin suç tarihinde yürürlükte bulunan TCK'nın 525/b-2 maddesinde yazılı bilişim sistemini kullanarak yarar sağlama suçunu oluşturacağı gözetilmelidir." şeklinde benzer yönde görüş bildirmiştir.

<sup>129</sup> TAŞKIN, Bilişim Suçları, s.83.

<sup>130</sup> Ancak kartın yağma sureti ile elde edilmesine sonuç bağlamayıp bilişim suçuna ilişkin hükmü uyguladığımız takdirde TCK md. 245'te yer alan cezalar yağma suçundan daha az olacaktır. Bu sonucun suç ve ceza siyaseti açısından isabetli olmadığını da belirtmek durumundayız. Bu nedenle yaptırım açısından ortaya çıkacak adaletsizlikleri önlemek adına kanunda bir düzenleme yapılması isabetli olur.



kaynaklanabilir. Bu halde TCK md.245'e teşebbüs söz konusu olur. Kartın elde edildiği ancak sisteme girilmediği diğer hal ise gönüllü vazgeçmedir. Fail, kartı ele geçirmesine rağmen icra hareketini tamamlamaz ve vazgeçerse; TCK md.245'e teşebbüsten cezalandırılmaz. Ancak unutulmamalıdır ki, kartın alınmasını sağlayan cebir veya tehdit hareketleri ayrıca suç oluşturduğundan vazgeçmeden önceki bu hareketler cezalandırılır.

Yağma ve bilişim suçları açısından ortaya çıkabilecek bir başka olasılık ise, cebir ve tehdit kullanarak kartın zilyedinin bilişim sistemine girmesinin istenmesidir. Somut olayda bu yolla başka bir hesaba para transferi gerçekleştirilebileceği gibi, işlem sonucu erişilen nakit paraya da el konulabilir. Bu tip ihtimallerde tek hareketle her iki suçun da gerçekleştiği sonucuna ulaşılmalıdır. Dolayısıyla TCK md. 44 gereği daha ağır cezayı gerektiren suçtan hüküm kurulması gerekecektir.

#### **D. Güveni Kötüye Kullanma Suçu**

Başkasına ait olup da, muhafaza etmek veya belirli bir şekilde kullanmak üzere, zilyetliği kendisine devredilmiş olan mal üzerinde, kendisinin veya başkasının yararına olarak, zilyedinin devri amacı dışında tasarrufla bulunan veya bu devir olgusunu inkâr eden kişinin cezalandırıldığı Güveni Kötüye Kullanma Suçu, TCK md.155 düzenlenmiştir<sup>131</sup>.

Söz konusu hükme bakıldığında, bilişimle ilgili özel bir nitelikli hale yer verilmediği görülmektedir. Ancak bu suç tipiyle bağlantılı olarak içinde bilişimle ilgili hususların geçebileceği örnekler vermek mümkündür.

Mesela; bir kimsenin rızası ile banka veya kart bilgilerini bir başkasına vermesi ve bu kişinin birtakım işlemleri gerçekleştirmesini istemesi halinde; çeşitli problemler ortaya çıkabilir. Söz gelimi; kart bilgilerine sahip kişinin hesaptan bir miktar parayı rıza verilen işlem gereği çekip teslim etmesi gerekirken kendisinin veya başkasının hesabına aktarması ya da kartın belli bir amaca uygun olarak kullanılması gerekirken kişinin bu amacın dışında işlemler yapması durumlarında; hem Güveni Kötüye Kullanma hem de Banka veya Kredi Kartlarının Kötüye Kullanılması Suçu gerçekleşecektir. Fakat fikri içtima kuralı gereği daha ağır cezayı gerektiren suçtan hüküm kurulacaktır.

Bir başka ihtimalde ise kendisinden istenen meblağı hesaptan çeken ancak bunu teslim etmeyen kişinin cezai sorumluluğu değerlendirilmelidir. Aslında bu durum salt güveni kötüye kullanma problemidir. Çünkü bilişim sistemine erişilmesi ve işlem yapılması yönünde geçerli bir rıza mevcuttur fakat paranın teslimine duyulan güven sonuçsuz kaldığından TCK md. 155'in ihlali söz konusu olmaktadır.

Farklı bir olasılık ise çekilmesi istenen miktarın üzerinde işlem yapılarak fazlaya ilişkin kısım ile menfaat sağlanması suretiyle hırsızlık suçunun oluşmasıdır. Bu halde güven duyulan işlem yani istenilen tutarın teslimi gerçekleşmiştir. Ancak hesap sahibinin bilgisi olmadan fail bir miktar para aldığından hırsızlık suçu oluşmaktadır. Bununla birlikte Hırsızlık Suçunun yanında Güveni Kötüye Kullanma Suçunun oluşmayacağını düşünüyoruz. Çünkü güvenilen işlemin bir miktar paranın teslimine ilişkin olduğunu ve bunun da gerçekleştiğini görüyoruz.

<sup>131</sup> Güveni Kötüye Kullanma Suçuyla ilgili ayrıntılı bilgi için bakınız; TEZCAN/ERDEM/ÖNOK, Teorik ve Pratik..., s.579-588; ÖZBEK, Yeni Türk Ceza Kanunu'nun Anlamı, s.1188-1198

### **KAYNAKÇA**

AKINCI Füsün Sokullu, **Avrupa Konseyi Siber Suç Sözleşmesinde Yer Alan Maddi Ceza Hukukuna İlişkin Düzenlemeler ve Özellikle İnternette Çocuk Pornografisi**, İÜHF M., Cilt:LIX, Sayı:1-2, 2001

ARTUK Mehmet Emin, GÖKCEN Ahmet, YENİDÜNYA Caner, **Ceza Hukuku Özel Hükümler**, 10. Bası, Ankara, 2010

ARTUK Mehmet Emin, GÖKCEN Ahmet, YENİDÜNYA Caner, **Türk Ceza Kanunu Şerhi, Özel Hükümler**, Ankara, 2009

DEĞİRMENCİ Olgun, **2004 Türk Ceza Kanunu'nun Bilişim Suçları Bakımından Değerlendirilmesi**, TBB Dergisi, Sayı:58, Mayıs/Haziran 2005

DEMİRBAŞ Timur, **Ceza Hukuku Genel Hükümler**, Ankara, 2011

DEMİRCAN Tunç, **Bilişim Alanında Suçlar**, Yayınlanmamış Yüksek Lisans Tezi, Konya, 2007

DÖNMEZER Sulhi, **Kişilere ve Mala Karşı Cürümler**, İstanbul, 1998

ÜLGER Murat Volkan, **Bilişim Suçları**, Ankara, 2004

ERDAĞ Ali İhsan, **Bilişim Alanında Suçlar (Türk ve Alman Ceza Hukukunda)**, Gazi Üniversitesi Hukuk Fakültesi Dergisi, C.XIV, Sayı:2, 2010

ERMAN Sahir, **Kamu Güvenine Karşı Suçlar**, İstanbul, 1996

EVİK, Ali Hakan, **"İşleme ve Bilgiye Dayalı Manipülasyon Suçları"**, Prof. Dr. Uğur Alacakaptan'a Armağan, İstanbul, 2008

ILDIR Ece, **Bankacılıkta Bilişim Suçları, Banka ve Finans Hukuku**, Panel ve Seminer Notları, İstanbul Barosu, İstanbul, 2009

İÇEL Kayıhan, **Suçların İçtimalı**, İstanbul, 1972

İÇEL Kayıhan, Özgenç İzzet, SÖZÜER Adem, MAHMUTOĞLU Fatih S., ÜNVER Yener, **İçel Suç Teorisi, 2. Kitap**, İstanbul, 1999

KANGAL Zeynel, **Tüzel Kişilerin Ceza Sorumluluğu**, Ankara, 2003

KARAGÜLMEZ Ali, **Bilişim Suçları ve Soruşturma-Kovuşturma Evreleri**, 2.bası, Ankara, 2011

KETİZMEN Muammer, **Türk Ceza Hukukunda Bilişim Suçları**, Ankara, 2008

KOCA Mahmut, **Yargıtay Kararları Işığında Bilişim Sistemlerinin Kullanılması Suretiyle Haksız Yarar Sağlama Suçları**, Prof. Dr. Ali Güzel'e Armağan, C. II, İstanbul, 2010

MAHMUTOĞLU Fatih Selami, **5237 Sayılı Türk Ceza Kanunu'nda Hukuka Uygunluk Nedenleri**, Hukuk ve Adalet Dergisi, Yıl:2, Sayı:5, Nisan 2005

MAHMUTOĞLU Fatih Selami, **Ekonomik Suçlar Bağlamında Kredi Hukukundan Kaynaklanan Suç ve İdari Suçlar**, Ankara, 2003.

MAHMUTOĞLU Fatih Selami, **Karşılaştırmalı Hukuk Bakımından İnternet Sujelerinin Ceza Sorumluluğu**, İÜHF M, Cilt:LIX, Sayı:1-2, İstanbul, 2001

MAHMUTOĞLU Fatih Selami, **Kusurluluk Prensibi Açısından Azmettirenin Ceza Sorumluluğu**, İÜHF M, Cilt: LXIII, Sayı:1-2, 2005

MALKOÇ İsmail, **Açıklamalı Yeni Türk Ceza Kanunu 2. Cilt**, 2007

MERAN Necati, **Yeni Türk Ceza Kanununda Sahtecilik - Malvarlığı Bilişim Suçları İle Ekonomi Ve Ticaret Alanında Suçlar**, Ankara, 2005

ÖNDER Ayhan, **Şahıslara ve Mala Karşı Cürümler ve Bilişim Alanında Suçlar**, İstanbul, 1994

ÖNGÖREN Gürsel, **İnternet Hukuku**, İstanbul, 2006

- ÖZBEK Veli Özer, **Banka ve Kredi Kartlarının Kötüye Kullanılması Suçu**, Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi, Cilt:9, 2007, Özel sayı, Ayır Basım, İzmir, 2007
- ÖZBEK Veli Özer, **Banka ve Kredi Kartlarının Kötüye Kullanılması Suçu**, Bilişim Hukuku, TC. Yargıtay Başkanlığı, Ankara, 2008
- ÖZBEK Veli Özer, **Yeni Türk Ceza Kanunu Anlamı**, Ankara, 2008
- ÖZGENÇ İzzet, **Türk Ceza Hukuku Genel Hükümler**, Ankara, 2009
- PARLAR Ali, **Türk Ceza Hukukunda Bilişim Suçları**, Ankara, 2011
- PARLAR Ali- AKIN Mustafa- HATİPOĞLU Muzaffer, **Bankacılık Ceza Hukuku**, Ankara-2010
- SOYARSLAN Doğan, **Ceza Hukuku Özel Hükümler**, Ankara, 2010
- SÖZÜER Adem, **Suçta Teşebbüs**, İstanbul, 1994
- TAŞKIN Şaban Cankat, **Bilişim Suçları**, İstanbul, 2008
- TEZCAN Durmuş, ERDEM Mustafa R., ÖNOK R. Murat, **Teorik Ve Pratik Ceza Özel Hukuku**, 7.bası, Ankara, 2010
- ÜNVER Yener, **Türk Ceza Kanunu'nun ve Ceza Kanunu Tasarısının İnternet Açısından Değerlendirilmesi**, İÜHFİM, C.LIX, S.1-2, 2001
- YAŞAR Osman, GÖKCAN Hasan Tahsin, ARTUÇ Mustafa, **Yorumlu Uygulamalı Türk Ceza Kanunu**, Ankara, 2010
- YAZICIOĞLU Yılmaz, **Yeni Türk Ceza Kanunu'ndaki Bilişim Suçlarının Genel Değerlendirmesi**, Yeni Türk Ceza Kanunu Sempozyumu, 5 Mart 2005
- YAZICIOĞLU Yılmaz, **Bilişim Suçları**, HPD Hukuki Yorum ve Haber Dergisi, Sayı:2, 2004
- YENİDÜNYA Caner, DEĞİRMENCİ Olgun, **Mukayeseli Hukukta ve Türk Hukukunda Bilişim Suçları**, İstanbul, 2003