"4 Ayda Bir Yayınlanır"

CHD
Ceza Hukuku Dergisi

Yıl: 5 Sayı: 14 Aralık 2010 17,50 TL

"Hakemli Dergidir"

- Karşılıksız İşlemi Yapılmasına Sebebiyet Verme Suçu (5941 sayılı Çek Kanunu m.5/1-3) ve Çek Düzenleme ve Çek Hesabı Açma Yasağı (5941 sayılı Çek Kanunu m.5/4-10)
  Prof. Dr. Veli Özer Özbek
- Tefecilik Suçu (TCK m.241)
  Prof.Dr. Veli Özer Özbek
- Türk Ceza Yasası'nda Kamuya Gerekli Şeylerin Yokluğuna Neden Olma Suçu (TCK m.238)
  Doç.Dr.Özlem Yenerer Çakmut
- Ceza Hukukunda Belge Kavramı
  Dr. Koray Doğan
- Alman Ekonomi Ceza Hukukuna Giriş
  Gülsün Ayhan AYGÖRMEZ
- Fiyatları Etkileme Suçu (TCK m. 237)
  Arş. Gör. İlker TEPE
- Ticari Sır, Bankacılık Sırrı veya Müşteri Sırrı Niteliğindeki Bilgi veya Belgelerin Açıklanması Suçu (TCK m. 239/1-3)
  Arş. Gör. İlker TEPE
- İnternet Bankacılığı Hakkında Yargıtay'ın 17.11.2009 Tarih, 2009/11-193 Esas sayılı Kararının İncelenmesi
  Arş. Gör. M. Emre YILDIZ
- Hırsızlık ve Dolandırıcılık Suçlarının Bilişim Sistemlerinin Araç Olarak Kullanılması Suretiyle İşlenmesi
  Arş. Gör. İsa BAŞBÜYÜK
- Alman Menkul Kıymetlerin Ticareti Kanunu § 14'ün Atfı ile § 38'e Göre Yasak Olan "İçeriden Öğrenenlerin Ticareti"nde Kazanç Müsaderesi (Alman Ceza Kanunu § 73 vd.) Kararının Verilmesi Sorunu
  Prof. Dr. Hans Kudlich - Dr. Silke NOLTENSMEIER
  Çev.: Serkan MERAKLI

ISSN 1307-0851 2301 3



seçkin

Ticari Ceza Özel Sayısı

CamScanner ile tarandı

Ceza Hukuku Dergisi

İÇİNDEKİLER

Karşılıksız İşlemi Yapılmasına Sebebiyet Verme Suçu (5941 sayılı Çek Kanunu m.5/1-3) ve Çek Düzenleme ve Çek Hesabı Açma Yasağı (5941 sayılı Çek Kanunu m.5/4-10)
Prof. Dr. Veli Özer Özbek 7

Tefecilik Suçu (TCK m.241)
Prof.Dr. Veli Özer Özbek 29

Türk Ceza Yasası'nda Kamuya Gerekli Şeylerin Yokluğuna Neden Olma Suçu (TCK m.238)
Doç.Dr.Özlem Yenerer Çakmut 41

Ceza Hukukunda Belge Kavramı
Dr. Koray Doğan 51

Alman Ekonomi Ceza Hukukuna Giriş
Gülsün Ayhan AYGÖRMEZ 67

Fiyatları Etkileme Suçu (TCK m. 237)
Arş. Gör. İlker TEPE 89

Ticari Sır, Bankacılık Sırrı Veya Müşteri Sırrı Niteliğindeki Bilgi veya Belgelerin Açıklanması Suçu (TCK m. 239/1-3)
Arş. Gör. İlker TEPE 103

İnternet Bankacılığı Hakkında Yargıtay'ın 17.11.2009 Tarih, 2009/11-193 Esas sayılı Kararının İncelenmesi
Arş. Gör. M. Emre YILDIZ 129

Hırsızlık ve Dolandırıcılık Suçlarının Bilişim Sistemlerinin Araç Olarak Kullanılması Suretiyle İşlenmesi
Arş. Gör. İsa BAŞBÜYÜK 151

Alman Menkul Kıymetlerin Ticareti Kanunu § 14'ün Atfı ile § 38'e Göre Yasak Olan "İçeriden Öğrenenlerin Ticareti"nde Kazanç Müsaderesi (Alman Ceza Kanunu § 73 vd.) Kararının Verilmesi Sorunu
Prof. Dr. Hans Kudlich - Dr. Silke NOLTENSMEIER
Çev.: Serkan MERAKLI 193

CamScanner ile tarandı

İNTERNET BANKACILIĞI HAKKINDA YARGITAY'IN 17.11.2009 TARİH, 2009/11-193 ESAS SAYILI KARARININ İNCELENMESİ•

Arş. Gör. M. Emre YILDIZ•

Özet: *Bilgi ve iletişim teknolojilerindeki gelişmeler, klasik bankacılık hizmetlerinin değişik dağıtım kanalları ile sunulması sonucunu doğurmuştur. Bu dağıtım kanallarından biri olan internet ile birlikte klasik bankacılık hizmetleri zamana ve mekana bağlı olmaksızın banka müşterilerine sunulmaya başlanmıştır. İnternet bankacılığı olarak adlandırılan ve finansal işlemleri kapsayan bu hizmet, internetin olumlu yanlarını içermekle beraber internetin kendine özgü yapısı nedeniyle birçok güvenlik açığını da bünyesinde barındırmaktadır. Bu nedenle, haksız olarak ele geçirilen başkasına ait internet bankacılığı şifresini kullanmak suretiyle gerçekleştirilen eylemler ile özellikle banka havalesi işleminin, ceza hukuku açısından yaptırımının ne olacağı hususu üzerinde durulmalıdır. İncelememize konu Yargıtay Ceza Genel Kurulu'nun 17.11.2009 tarihli kararı ise, bu eylemlerin, 5237 sayılı TCK'da yer alan hangi normu (m. 142/2-e "Bilişim sistemlerinin kullanılması suretiyle hırsızlık" veya m. 244/4 "Bilişim Sistemine veya Verilere Müdahale Suretiyle Haksız Çıkar Sağlanması") ihlal ettiğini belirlemesi bakımından önem arz etmektedir.*

Bu nedenlerle çalışmada öncelikle söz konusu kararın özeti, mercilerin çözüm şekli, çözümlenmesi gereken hukuki sorun ile internet bankacılığı kavramı ve internet bankacılığının işleyişi üzerinde durulmuştur. Daha sonra ise haksız olarak ele geçirilen başkasına ait internet bankacılığı şifresi kullanılmak suretiyle başkasına ait hesaptan kendi hesabına havale yoluyla haksız çıkar sağlama eylemi, 5237 sayılı TCK'da yer alan ilgili düzenlemeler ışığında irdelenmeye çalışılmıştır.

Anahtar Kelimeler: *İnternet bankacılığı, bilişim sistemi, veri, nitelikli hırsızlık, bilişim sistemine veya verilere müdahale, haksız çıkar.*

I. OLAYIN ÖZETİ

1 Haziran 2005 tarihinden önce, sanık (Volkan) ve diğer firari sanık (Saim) birlikte hareket ederek, katılan firmanın internet bankacılık şifresini haksız bir şekilde ele geçirmiştir. Sanık ve diğer firari sanık, haksız olarak ele geçirdikleri katılan firmaya ait internet bankacılık şifresini kullanarak, katılan firmanın Ş...bank Ankara K... şubesindeki hesabından 10.750 YTL'yi, internet kanalı ile Ş....bank İstanbul Z.... Şubesine sanık Volkan adına açtırdıkları, hesaba havale etmiş ve aynı gün banka şubesinden 10.750 YTL'yi çekmişlerdir.

• MAKALE HAKEM DENETİMİNDEN GEÇMİŞTİR.

• Dokuz Eylül Üniversitesi Hukuk Fakültesi, Ceza ve Ceza Muhakemesi AD.

CamScanner ile tarandı

II. MERCİLERİN ÇÖZÜM ŞEKLİ

A. İlk Derece Mahkemesi

Bakırköy İkinci Ağır Ceza Mahkemesi, sanığın 765 sayılı TCY'nin 525/b-2 ve 59. maddeleri uyarınca 1 yıl 8 ay hapis ve 407 YTL ağır para cezası ile cezalandırılmasına hükmetmiştir. Bakırköy İkinci Ağır Ceza Mahkemesi 'nce verilen 27.10.2005 gün ve 218-204 sayılı hüküm, katılan vekili tarafından temyiz edilmiş ve dosya Yargıtay 11. Ceza Dairesi tarafından incelenmiştir.

B. Yargıtay Ceza Dairelerinin Çözüm Şekli

1. Yargıtay 11. Ceza Dairesinin Çözümü

11. Ceza Dairesi, sanıkların katılanın internet bankacılığı şifresini hukuka aykırı olarak ele geçirip, katılan hesabından kendi açtırdıkları hesaba havale yapmaktan ibaret eylemi değerlendirmiştir. 11. Ceza Dairesi'ne göre bu eylem nedeniyle hüküm kurulurken olay tarihinde yürürlükte bulunan 765 sayılı TCK'nın 525/b-2. maddesindeki düzenleme ile, karar tarihinde yürürlükte bulunan 5237 sayılı TCK'nın 244/4. maddesindeki düzenlemenin karşılaştırılması gerektiği sonucuna varmıştır. Bu nedenle ilk derece mahkemesinin, eylemin olay tarihinde yürürlükte bulunan 765 sayılı TCK'nın 525/b-2. maddesi ile karar tarihinde yürürlükte bulunan 5237 sayılı TCK'nın 158/1-f (Bilişim sistemlerinin, banka veya kredi kurumlarının araç olarak kullanılması suretiyle Dolandırıcılık) maddesine uyduğu gerekçesi ile sanıklar hakkında 765 sayılı TCK'nın 525/b-2 maddeleri uyarınca mahkumiyet hükmünü bozmuştur.

Ayrıca Yargıtay 11. Ceza Dairesi; 22.01.2008 gün ve 8423-117, 28.02.2008 gün ve 22-1141, 28.02.2008 ve 23-1160, 26.09.2007 gün ve 5875-7637 sayılı kararlarında, eylemin 5237 sayılı TCK'nın 244/4. maddesindeki suçu oluşturduğu yönünde karar vermiştir.

2. Yargıtay 6. Ceza Dairesinin Çözümü

Yargıtay 6. Ceza Dairesi 02.06.2008 gün ve 555-12249 sayılı kararında ise benzer eylemin, 5237 sayılı TCK'nın 142/2-e maddesinde düzenlenen nitelikli hırsızlık suçunu oluşturduğu, yönünde karar vermiştir.

C. Yargıtay Ceza Genel Kurulunun Çözümü

Sanıkların haksız bir şekilde ele geçirdikleri katılan firmanın internet bankacılık şifresini kullanmak suretiyle banka şube hesabındaki parayı kendi adına açtırdıkları hesaba havale edip aynı gün banka şubesinden çekmesi eyleminin, "Bilişim Sistemi Kullanılmak Suretiyle Hırsızlık" suçunu oluşturduğunu yönünde karar vermiştir.

CamScanner ile tarandı

III. ÇÖZÜMLENMESİ GEREKEN HUKUKİ SORUN

Haksız olarak ele geçirilen başkasına ait internet bankacılık şifresi kullanılarak, başkasına ait hesaptan kendi adına açtırdıkları hesaba, belli miktar para havalesi şeklinde gerçekleştirilen eylemin, 5237 sayılı TCK'da düzenlenmiş olan "Bilişim sistemlerinin kullanılması suretiyle hırsızlık (m. 142/2-e)" suçunu mu yoksa, bilişim alanında suçlar bölümünde düzenlenmiş " Sistemi engelleme, bozma veya sistemdeki verilere müdahale suretiyle haksız çıkar sağlama (m. 244/4)" suçunu oluşturduğu çözümlenmesi gereken hususdur.

IV. DEĞERLENDİRMELER

A. Genel Olarak İnternet Bankacılığı

1. Tanım

Bilgi ve iletişim teknolojileri alanında gün geçtikçe artan ilerlemeler, hemen hemen her alanda olduğu gibi, bankacılık sektöründe de bir takım köklü değişikliklere neden olmuştur. Bir taraftan bankaların maliyetlerini düşürme ve müşterilerinin memnuniyetini sağlama çabası, diğer taraftan banka müşterilerinin zaman kaybetmeden, hızlı, banka şubesine gitmeden finansal işlemlerini rahatça yapma isteği, klasik bankacılık hizmetlerinin değişik iletişim araçlarıyla sunulmasına yol açmıştır. Kuşkusuz bu iletişim araçlarından en önemlisi de, artık normal hayatın bir parçası olan ve büyük kitlelere hitap etmeyi sağlayan internettir.

Elektronik bankacılığın[1] bir türü olan internet bankacılığı, banka ve müşterisi arasındaki karşılıklı sözleşme gereği, bankacılık hizmetlerinin internet üzerinden sunulması olarak tanımlanabilir. Banka sözleşmelerinde internet bankacılığı, *şahsın (tüketicinin) kablolu, kablosuz iletişim sistemleri ile teknik şartlara haiz bilgisayar (avuç içi dizüstü) GSM, telefon gibi araçlar üzerinden ve İnternet-Wap aracılığı ile otomatik, sesli, yanıt sistemi ile şifre ve parolayı kullanarak, bankanın belirleyeceği kurallar ve limitler dahilinde şahsın banka hesapları üzerinde her türlü işlem yapma yöntemi*[2] olarak tanımlanmaktadır.

---

1 Elektronik bankacılık, bankacılık hizmetlerinin her türlü elektronik vasıtalar aracılığıyla verilmesi şeklinde tanımlanabilir. Elektronik Bankacılık (*Electronic Banking*), Ev ve Ofis Bankacılığı (*Home and Office Banking*), Telefon Bankacılığı *Telephone Banking*), Televizyon Bankacılığı (Television Banking), Kablosuz Uygulama Protokolü (*Wireless Application Protocol-WAP*) Bankacılığı, Avuç içi (*Palmtop*) Bilgisayar Bankacılığı, Kabin (Kiosk) Bankacılığı, Kısa Mesaj Servisi (*SMS – Short Message Service*) Bankacılığı ve Internet Bankacılığı (*Internet Banking*) şeklinde gruplara ayrılabilir. (**Yılmaz** Süleyman, " Hukuki Açıdan İnternet Bankacılığı", Ankara Üniversitesi Sosyal Bilimler Enstitüsü Doktora Tezi, Ankara, 2007, s. 19-20).

2 **Özdamar** Naci, " İnternet Bankacılığı ve Banka Kartları", Bilişim ve Hukuk, Ankara Barosu Uluslar arası Hukuk Kurultayı, C. II, 2008, s. 67; **Lale** Muktedir, " İnternet Bankacılığında Hukuki Sorumluluk", Terazi Hukuk Dergisi, S. 42, Şubat 2010, s. 22.

CamScanner ile tarandı

İnternet bankacılığı, Bankacılık Düzenleme ve Denetleme Kurulu tarafından çıkarılan, Bankalarda Bilgi Sistemleri Yönetiminde Esas Alınacak İlkelere İlişkin Tebliğ[3] m.3/1-ö'de ise, *müşterilerin banka tarafından sunulan hizmetlere internet yoluyla ulaşmalarını ve yapmak istedikleri işlemleri gerçekleştirmelerini sağlayan bankacılık hizmeti dağıtım kanalı* olarak tanımlanmıştır.

2. İnternet Bankacılığının İşleyişi

Bankacılık işlemlerinin internet ortamında gerçekleştirilebilmesi için ilk başta bankaların buna olanak sağlayacak web sayfası ve işlemlerin gerçekleşebilmesi için gerekli teknik altyapıyı oluşturması gerekmektedir[4]. Genellikle banka web sayfaları bünyesinde oluşturulan bu yapıya internet şubesi[5] adı verilmektedir.

İnternet bankacılığının kullanılması için, banka ve müşterisi arasında yapılacak sözleşme[6] ile banka müşterisine internet şubesinde oturum[7] açabilmesi için kullanıcı adı ve parola verilir. Müşteri, bankanın web sitesindeki internet şubesine bağlanarak kullanıcı adı ve parolasını ilgili bölümlere girer[8]. Müşterinin kullanıcı adı ve parolası, web sitesine yüklenen yazılım sayesinde bankanın web sunucusunda tutulan verilerle karşılaştırılır. Web sunucusunda tutulan verilerle müşterinin girdiği veriler aynı değilse, müşterinin hatalı işlem yaptığı, yine web sitesi üzerinden müşteriye bildirilir. Genellikle bankalar güvenlik gerekçesiyle, müşterilerin kullanıcı adı ve parolalarını üç kez yanlış girmeleri halinde, internet şubesi girişini bloke ederler ve onları yeni kullanıcı adı ve parolalarını almak üzere, bankaların fizikî şubelerine yönlendirirler[9]. Web sunucusunda tutulan verilerle müşterinin girdiği veriler aynı ise müşterinin bir sonraki aşa-

---

3 R.G., T: 14.09.2007, S : 26643.

4 Bankalarda Bilgi Sistemleri Yönetiminde Esas Alınacak İlkelere İlişkin Tebliğ(Bundan sonra BBSYEAİT olarak anılacaktır)'in 24. maddesine göre, internet bankacılığına ilişkin her türlü altyapı bankanın bilgi sistemlerinin bir parçası olarak değerlendirilir.

5 İnternet şubesi, banka sözleşmelerinde; müşterinin teknik şartlara sahip donanımlarla internet üzerinden bankaya bağlanarak, münhasıran kendisine verilen parolayı/şifreyi ve diğer güvenlik unsurlarını kullanarak ve bankaca tanımlanacak yetki çerçevesinde hesaplarını görüntüleme, hesapları üzerinde her türlü işlem ve sorgulama ile bankanın daha sonra kullanıma sunabileceği diğer işlemleri yapma olanağının sağlanması olarak tanımlanmaktadır. Bkz. **Lale**, s. 22.

6 Bu sözleşme, mevduat açtırma sözleşmesi içerisinde yer alan hükümlerden oluşabileceği gibi ayrıca internet üzerinden yapılan hukuki işlemlerin durumu hakkında bkz. Zevkliler Aydın / Aydoğdu Murat, Tüketicinin Korunması Hukuku, Ankara 2004,s. 272 vd.

7 BBSYEAİT m. 3/1-ü'ye göre oturum; *veri aktarımı, sunuşu veya gerçekleştirilecek finansal işlemler için taraflar arasında kurulan mantıksal bağı* ifade eder.

8 Artık bankalar sisteme giriş için kimlik doğrulamada, yetkisiz kimselerin işlem yapmasını engellemek için, kullanıcı adı ve parolanın yanında tek kullanımlık parolaya da ek bir unsur olarak yer vermektedirler. BBSYEAİT m. 3/1-çç'ye göre tek kullanımlık parola; *kimlik doğrulamada sadece bir kez kullanılmak üzere rastgele yaratılan alfabetik ve/veya rakamsal karakterler dizisini* ifade eder.

9 Yılmaz, s. 33-34.

CamScanner ile tarandı

maya geçerek internet bankacılığı hizmetlerinden yararlanmasına izin verilir[10]. Bir başka deyişle, mevduat sahibi, banka tarafından kendisine tanınan yetki alanı içinde, bankanın hazırladığı web sayfasına girip işlem yaptığında, kendisine özel parolayı girmek suretiyle bu işlemin kendi iradesiyle yapıldığını beyan etmiş olur ve sonuçlarından şahsen sorumludur[11]. İnternet bankacılığında kullanıcı olan müşteri bankanın fiziki şubedeki banko çalışanı gibi düşünülebilir. Farkı ise banko çalışanı tüm hesaplara ve işlemlere ulaşabilirken kullanıcı sadece sisteme tanımlı işlemleri yapabilir[12].

İnternet bankacılığı işlemleri açısından kuşkusuz en önemli unsur, finansal nitelik taşıyan işlemlerin, sadece yetkili kişiler tarafından gerçekleştirilmesinin sağlanmasıdır[13]. İnternet aracılığıyla bankacılık işlemlerinin gerçekleştirilmesi, kullanıcılarına birçok avantaj sağlamasına karşılık, internete özgü birtakım güvenlik sorunlarını da beraberinde getirmiştir. Gerçekten de gerek internetin anonim olması ve bir üst otoritenin olmayışı gerekse bazı suç faillerinin tespitindeki zorluk[14], suç ve suçlu açısından elverişli bir ortam sağlamaktadır. Bu elverişli ortamın yanında, ayrıca internet bankacılığının gün geçtikçe artan uygulaması[15] ve asli unsurunu ekonomik değerlerin oluşturması, bu alanda suçluluk açısından takviye edici unsurlardır.

B. Bilişim Sisteminin İşleyişine veya Verilere Müdahale Suretiyle Haksız Çıkar Sağlanması (TCK. m. 244/4)

1. Genel Olarak

765 sayılı TCK'ya, 1991 yılında, 10. babın mal aleyhine cürümler başlığını taşıyan bölümünün ardından gelecek şekilde 11. babta düzenlenen "Bilişim Alanında

---

10 Yılmaz, s. 33-34.

11 Çeker Mustafa, "İnternet Bankacılığı ve Bankaların Sorumluluğu", Prof. Dr. Hüseyin Ülgen'e Armağan, İstanbul, 2007, s. 1339.

12 Kaya Taner, " İnternet Bankacılığı", Bilişim ve Hukuk Dergisi(Ankara Barosu), S. 9, 2008, s. 32.

13 Bankalar, mevduat sahiplerinin hesaplarına internet bankacılığı yolu ile yetkisiz kişilerce erişilememesi için değişik güvenlik uygulamaları kullanmaktadırlar. Bunlardan bazıları sanal klavye kullanımı, erişimde veya işlem yapılabilmesi için tek kullanımlık parolalar, erişim için IP kısıtlamalarıdır. Her ne kadar bu güvenlik uygulamaları kullanılsa da, banka müşterisinin internet bankacılığını kullandığı bilgisayarda konuşlanmış, key logger(tuş kaydedici) ve screen logger (ekran kaydedici) adlı kötü yazılımlar sayesinde gerek güvenli şifre gerekse sanal klavye uygulamaları, 3. kişilerin başkasına ait banka hesaplarına yetkisiz erişimini engelleyememektedir.

14 Özellikle internet kafelerden ve başkasına ait şifrelenmemiş veya şifrelenmiş olmakla birlikte şifresi kırılmış kablosuz internet yoluyla gerçekleştirilen eylemlerde, faillere ulaşmada büyük zorluklar yaşanmaktadır.

15 Türkiye Bankalar Birliği verilerine göre, Ekim-Aralık 2009 dönemi itibariyle, internet bankacılığı hizmeti kullanılarak yapılan yatırım işlemleri dışındaki finansal işlemlerin toplam adedi 70,9 milyon, tutarı ise 171 milyar TL olmuştur. Yine Aralık 2009 tarihi itibariyle, sisteme kayıtlı ve en az bir kere login olmuş internet bankacılığı kullanan müşteri sayısı ise, 13,361,926 dır. Bkz. Türkiye Bankalar Birliği İnternet Bankacılığı İstatistikleri, Aralık 2009.

CamScanner ile tarandı

Suçlar" a, bir takım değişikliklerle 5237 sayılı TCK'da da yer verildiği görülmektedir. Kanun sistematiğine bakıldığında, bu suçlar 5237 sayılı TCK'nın ikinci kitabının, üçüncü kısmı olan "Topluma Karşı Suçlar" altında "Bilişim Alanında Suçlar" başlıklı onuncu bölümünde düzenlenmiştir. Bu bölüm altında düzenlenen suçlara bakıldığında ise, m. 243'de "Bilişim Sistemine Girme", m. 244'de "Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme", m. 245'de "Banka veya Kredi Kartlarının Kötüye Kullanılması" suçlarının düzenlendiği görülmektedir.

Yukarıda da belirtildiği üzere, bilişim alanında işlenen suçlardan birisi de konumuzu oluşturan, bilişim sistemine veya verilere müdahale suretiyle haksız çıkar sağlanması suçu (m. 244/4)dur[16] [17]. 5237 sayılı TCK m. 244'e bakıldığı zaman, bu suç kapsamında birden fazla suçun aynı madde içerisinde düzenlendiği görülmektedir. Öyle ki, TCK m. 244/1'e göre; bir bilişim sisteminin işleyişini engellemek veya bozmak eylemleri düzenlenirken, TCK m. 244/2'de bir bilişim sistemindeki verileri bozmak, yok etmek, değiştirmek veya erişilmez kılmak, sisteme veri yerleştirmek, var olan verileri başka bir yere göndermek eylemleri suç kapsamına alınmıştır. Nihayet TCK m. 244/4'de ise; birinci ve ikinci fıkralardaki eylemlerin işlenmesi suretiyle, başka bir suçun oluşmaması koşulu ile[18], kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlaması cezalandırılmıştır. Bu üç fıkranın yanında TCK m. 244/3'de ayrıca bir nitelikli hal olarak ağırlaştırıcı sebep düzenlenmiştir. Buna göre; yukarıda birin-

---

16 Bu suçun 765 sayılı TCK'da karşılığı, m. 525/b-2' dir. Bu madde, *"Bilgileri otomatik işleme tabi tutmuş bir sistemi kullanarak kendisi veya başkası lehine hukuka aykırı yarar sağlayan kimseye bir yıldan beş yıla kadar hapis ve ikimilyon liradan yirmimilyon liraya kadar ağır para cezası verilir."* şeklinde düzenlenmişti. Dülger'e göre, söz konusu madde 5237 sayılı TCK ile dört ayrı suç olarak düzenlenmiştir. Bunlar; banka ve kredi kartlarının kötüye kullanılması, bilişim sistemi aracılığıyla dolandırıcılık, bilişim sistemleri aracılığıyla hırsızlık ve en son olarak m. 244/4' de düzenlenen bilişim sistemine veya verilere müdahale suretiyle haksız çıkar sağlanması suçlarıdır. Bkz. **Dülger** Murat Volkan, Bilişim Suçları, Ankara, 2004, s. 211, 244.

17 Benzer düzenleme, Bilişim Ağı Hizmetlerinin Düzenlenmesi Ve Bilişim Suçları Hakkında Kanun Tasarısının 19. maddesinde "Bilişim Ortamında Yarar Sağlamak" başlığıyla yer almaktadır. Bu düzenlemeye göre: " *(1) Bilişim sistemiyle kendisi veya başkası lehine haksız yarar sağlayan kişi, fiil daha ağır cezayı gerektiren başka bir suç oluşturmadığı takdirde, iki yıldan beş yıla kadar hapis ve bin günden beşbin güne kadar adlî para cezası ile cezalandırılır.*". Dikkat edilecek olursa tasarıyla, bilişim sistemleri aracılığıyla haksız yarar sağlama eylemleri bağımsız suç haline getirilmiş ve bilişim sistemine yahut verilere müdahaleden söz edilmemiştir. Ayrıca söz konusu düzenlemenin uygulanabilmesi için, fiilin daha ağır cezayı gerektiren bir suçu oluşturmaması koşulu ile 5237 sayılı TCK m. 244/4'den ayrılmıştır. Zira, TCK m. 244/4' ün uygulanabilmesi için, sadece fiilin başka bir suçu oluşturmamış olması gerekmektedir.

18 5237 sayılı TCK m. 244/4' de yer alan *"başka bir suç oluşturmaması halinde"* düzenlemesi, madde gerekçesinde, kanundaki metninden farklı olarak yer almaktadır: *"...bir ve ikinci fıkralarda tanımlanan fiillerin işlenmesi suretiyle kişinin kendisine veya başkasına yarar sağlaması, ceza yaptırımı altına alınmıştır. Ancak, bu fıkra hükmüne istinaden cezaya hükmedilebilmesi için, fiilin daha ağır cezayı gerektiren başka bir suç oluşturmaması gerekir. Bu bakımdan, fiilin örneğin dolandırıcılık, hırsızlık, güveni kötüye kullanma veya zimmet suçunu oluşturması hâlinde, bu fıkra hükmüne istinaden cezaya hükmedilmeyecektir."*. Madde gerekçesi ve kanun metninin çelişmesi karşısında, gerekçenin bağlayıcı olmaması nedeniyle, gerekçedeki bu ibareye itibar edilmeyecektir.

CamScanner ile tarandı

ci ve ikinci fıkralarda sayılan eylemlerin banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinde işlenmesi halinde, verilecek ceza yarı oranında artırılır[19].

Kanımızca, m. 244/4'de düzenlenen, bilişim sistemine veya verilere müdahale suretiyle haksız çıkar sağlanması suçu, bağımsız bir suç[20] olarak değil, m. 244/1 (bilişim sisteminin işleyişini engellemek veya bozmak) ve m. 244/2 (bilişim sistemindeki verileri bozmak, yok eden, değiştirmek veya erişilmez kılmak, sisteme veri yerleştirmek, var olan verileri başka bir yere göndermek)'deki suçların nitelikli hali olarak düzenlenmiştir. Bu nedenle, temel suç tipi oluşmadığı sürece, yani 244/1 ve 244/2' deki suçlar oluşmadığı sürece, bu nitelikli halin uygulanması mümkün değildir. Ayrıca, nitelikli halin gerçekleşmemesi durumunda teşebbüsten söz edilemez. Sadece bu hal uygulanmaz ancak suçun basit şeklinden (m. 244/1 veya m. 244/2) ceza verilebilir[21].

2. Suçla Korunan Hukuki Değer

5237 sayılı TCK m. 244/4'de düzenlenen, bilişim sistemine veya verilere müdahale suretiyle haksız çıkar sağlanması suçunun düzenleniş şekline bakıldığında, aslında bu suçla korunan birden fazla hukuki değer olduğu görülmektedir. Gerçekten de, söz konusu suçun oluşması bakımından, m. 244/1 ve m. 244/2'deki unsurların gerçekleşmesi gerekliliği nedeniyle, bu suçlarla korunan hukuki değerler, m. 244/4 için de geçerli olacaktır. Buradan çıkan sonuç ise, bu suçla korunan hukuki değerlerden ilki, m. 244/1 gereğince, bir bilişim sisteminin dış müdahalelerden uzak düzgün işleyişi ve aynı zamanda m. 244/2 gereğince, bilişim sisteminde yer alan soyut unsurların yani verilerin güvenliğidir. Bu durum, bilişim suçlarının, kanun sistematiğinde "Topluma Karşı Suçlar" kısmında düzenlenmesinin bir sonucudur. Öyle ki, bu suçların konusunu oluşturan bilişim sistemlerinin veya verilerin zarar görmesi halinde, malvarlığına karşı işlenen suçlarda olduğu gibi sadece kişinin malvarlığında bir zarar meydana gelmeyip, toplumun bilişim sistemlerinin doğru işleyişine olan güvenleri de etkilenmektedir[22].

Bu suçla korunan ikinci hukuki değer ise, mülkiyet hakkıdır. Zira, TCK m. 244/1 ve 2'deki eylemler nedeniyle, gerek bilişim sisteminin fonksiyonlarını gerektiği gibi yerine getirememesi yani işleyişinin bozulması ve engellenmesi,

---

19 **Özbek** Veli Özer/**Kanbur** M. Nihat/**Doğan** Koray/**Bacaksız** Pınar/**Tepe** İlker, Türk Ceza Hukuku Özel Hükümler, Ankara, 2010, s. 908.

20 Koca, m. 244/4'deki hükmü bağımsız bir suç olarak nitelemekte ve bu suçun TCK. m. 42 gereğince bileşik suç özelliğine sahip olduğunu belirtmektedir. Bkz. **Koca** Mahmut, "Hukukumuzda TCK'nun 244. Maddesi Kapsamında Bilişim Sistemini Engelleme, Bozma, Verileri Yok Etme veya Değiştirme Suçu", Yargıtay Bilişim Hukuku Konferansı, 09-10 Ekim, 2008, s. 96 vd.

21 **Özbek/ Kanbur/ Doğan/ Bacaksız/ Tepe**, s. 921.

22 **Koca**, s. 91.

CamScanner ile tarandı

gerekse veriler üzerinde tasarrufta bulunmaya yetkili kişinin bu veriler üzerindeki tasarruf hakkının ihlali nedeniyle zarara uğraması söz konusudur[23].

3. Maddi Unsurlar

a. Suçun Hukuki Konusu

Bilişim sisteminin işleyişine ve verilere müdahale yolu ile haksız yarar sağlama (m.244/4) suçunun hukuki konusu, fail tarafından müdahalede bulunulan bilişim sistemi ve verilerdir[24,25]. Öyle ki, bilişim sisteminin işleyişinin engellenmesi veya bozulması yoluyla haksız yarar sağlanması durumunda, suçun hukuki konusu bilişim sistemiyken, verilere müdahale yoluyla haksız yarar sağlanması durumunda suçun hukuki konusu veridir. Bu nedenle, bilişim sistemi ve veri kavramlarının neyi ifade ettikleri önem arz eden hususlardır.

i. Bilişim Sistemi Kavramı

5237 sayılı TCK'nın yürürlüğe girmesi ile birlikte, 765 sayılı TCK'da yer alan "*bilgileri otomatik işleme tabi tutan sistem*" terimi terk edilerek, yerinde olarak bunun yerine bilişim suçları açısından daha kapsayıcı bir terim olan "*bilişim sistemi*" terimi tercih edilmiştir. 5237 sayılı TCK'nın 243 ve 244'üncü maddelerinde "bilişim sistemi" terimi kullanılmakla birlikte, bu terimin tanımına kanun metninde yer verilmemiştir. Bilişim sistemi 243'üncü maddenin gerekçesinde, "*...verileri toplayıp yerleştirdikten sonra bunları otomatik işlemlere tâbi tutma olanağını veren manyetik sistemlerdir...*" şeklinde tanımlanmıştır[26]. Bilişim Ağı Hizmetlerinin Dü-

---

23 *Kurt*'a göre, TCK m. 244/2'de düzenlenen verilere müdahale suçunda, müdahale edilen verinin özelliğine göre, suçla korunan hukuki değer çeşitlilik arz etmektedir. Bunlar mülkiyet hakkı, fikri mülkiyet hakkı, özel hayatın gizliliği olabileceği gibi mülkiyet hakkı da olabilir. Örneğin, haksız müdahale edilen veri, özgün bir çalışmayı içeriyorsa fikri mülkiyet hakkı, özel bilgiler içeriyorsa özel hayatın gizliliği, ticari sırlar içeriyorsa mülkiyet hakkı suçla korunan hukuki değerdir. **Kurt** Levent, Açıklamalı-İçtihatlı Tüm Yönleriyle Bilişim Suçları ve Türk Ceza Kanunundaki Uygulaması, Ankara, 2005, s. 162.

Dülger'e göre ise, failin bilişim sistemi aracılığıyla gerçekleştirdiği eylemler neticesinde suçun oluşması için mağdurda bir zararın meydana gelmesi gerekmektedir; ancak bu zararın nasıl bir zarar olduğu açıklanmamıştır. Fail tarafından zarara uğratılan bu maddi veya manevi hak suçla korunan hukuki değerdir. **Dülger**, s. 244.

24 Suçun hukuki konusu icra hareketlerinin üzerinde gerçekleştiği şey olarak tanımlandığına göre, bu suç bakımından hukuki konunun, failin sağladığı hukuka aykırı yarar olduğu görüşüne katılmıyoruz. Bu görüş için bkz. **Dülger**, s. 246.

25 Benzer açıklama 244'üncü maddenin gerekçesinde de yer almaktadır: "*Maddenin birinci fıkrasında bir bilişim sisteminin işleyişini engelleme, bozma, sisteme hukuka aykırı olarak veri yerleştirme, var olan verileri başka bir yere gönderme, erişilmez kılma, değiştirme ve yok etme fiilleri, suç olarak tanımlanmaktadır. Böylece sistemlere yöneltilen ızrar fiilleri özel bir suç hâline getirilmiştir. Aracın fizik varlığı ve işlemesini sağlayan bütün diğer unsurları, söz konusu suçun konusunu oluşturmaktadır.*".

26 Avrupa Siber Suç Sözleşmesinde, bilişim sistemi tanımlanmamakla beraber "bilgisayar sistemi" tanımlanmıştır: "*Herhangi bir cihaz ve birbiriyle bağlantılı bir grup veya cihazlar yoluyla bir veya birden fazla program tarafından devam ettirilen verinin otomatik olarak işlenmesi, bu işlemin yerine getirilmesi.*".

CamScanner ile tarandı

zenlenmesi ve Bilişim Suçları Hakkında Kanun Tasarısı'nın tanımlar başlıklı 2/1-d maddesinde ise bilişim sistemi, "*Bilgisayar, çevre birimleri, iletişim altyapısı ve programlardan oluşan veri işleme, saklama ve iletmeye yönelik sistem...*" şeklinde tanımlanmıştır. Görüldüğü üzere, bilişim sistemi kavramı, bilgisayar ile aynı anlama gelmemektedir. Bilişim sistemi, "bilgisayar" a göre daha geniş bir kavram olup bu haliyle bir üst kavramdır[27]. Bilgisayar[28], verilerin depo edilmesi, saklanması, işlenmesi ve yeniden değerlendirilmesi faaliyetini gerçekleştirmesine karşın, "bilişim sistemi" hem verilerin işlenmesi hem de verilerin aktarılmasını kapsar. Ancak bilişim sisteminden söz edilebilmesi için, bir bilgisayarı gerekli kılar[29].

ii. Veri Kavramı

TCK m. 244/2'de sistemdeki verileri bozma, yok etme, değiştirme veya erişilmez kılma, sisteme veri yerleştirme veya var olan verileri başka bir yere gönderme suç olarak tanımlanmıştır. Bu eylemler suç olarak tanımlanmakla birlikte, veri kavramından ne anlaşılması gerektiğine yer verilmemiştir. TCK m. 243'ün gerekçesinde verinin tanımı yapılmamakla birlikte sadece sistemdeki soyut unsurların veri olduğu belirtilmiştir[30]. 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun m. 2/1-k' da ise veri, "*Bilgisayar tarafından üzerinde işlem yapılabilen her türlü değeri..*" ifade etmektedir. Bu anlamda veri, bilişim sistemlerinin üzerinde işlem yapabildiği, bu işlemlere dayalı sonuçlar üretebildiği, saklayabildiği, sakladıklarını sonradan tekrar okuyup işleyebildiği ve diğer bilişim sistemlerine iletebildiği her türlü bilgi olarak açıklanabilir[31]. Benzer şekilde Avrupa Siber Suç Sözleşmesinin Tanımlar başlıklı 1. maddesinde "bilgisayar verisi", "*...bir bilgisayar sisteminin belli bir işlevi yerine getirmesini sağlayan yazılımlar da dahil olmak üzere, bir bilgisayar sisteminde işlenmeye uygun nitelikteki her türlü bilgi ve konsept...*" olarak tanımlanmıştır.

---

27 Benzer yönde bkz. **Koca**, s. 92.

28 Bilgisayar, "*Çok sayıda aritmetiksel ya da mantıksal işlemlerden oluşan bir işi, çalışması sırasında bir işletmen'in işe karışması gerekmeksizin, önceden verilmiş bir izlenceye göre, özdevimli olarak yürüten bir veri işleyici.*" olarak da tanımlanabilir. (Bilişim Terimleri Sözlüğü TDK) http://tdkterim.gov.tr/?kelime=bilgisayar&kategori=terim&hng=md (Erişim tarihi: 23.10.2010).

29 Bilişim sistemi kavramının temel unsurunu bilgisayar, bilgisayarın temel unsurunu da donanım(Hardware) ve yazılım(Software) oluşmaktadır. Donanım, bilgisayarın fiziksel yani somut kısımlarına verilen isimdir. Bu anlamda ekran, klavye, fare, sabit disk, RAM, mikroişlemci, kart okuyucu vb. elemanlar bilgisayarın donanım unsurunu teşkil eder. Yazılım ise, bilgisayarın donanım elemanlarını kullanmak için gereken, donanıma hayat veren tüm soyut unsurlardır. Bu anlamda, yazılım donanım elemanlarına nasıl hareket edeceklerini belirten komutlardır.

30 "*Sistem içindeki bütün soyut unsurlar, fıkrada geçen "veri" teriminin kapsamındadır.*" m. 243 gerekçesi.

31 **Dülger**, s. 50; *Koca*'ya göre, veri, bilgilerin belirli bir formata dönüştürülmüş şeklidir. Bu bağlamda bir bilişim sisteminde saklanan yazı, resim, web sayfası tasarımı ve rakam gibi bilgiler veri olarak kabul edilmelidir. **Koca**, s. 94.

CamScanner ile tarandı

b. Fail-Mağdur

TCK m. 244/4'de düzenlenen bilişim sisteminin işleyişine ve verilere müdahale yoluyla haksız yarar sağlanması suçunda, fail ve mağdur bakımından önem arz eden bir durum yoktur. Bir başka anlatımla, herkes bu suçun faili ve mağduru olabilir.

c. Eylem

TCK m. 244/4'de yer alan suça bakıldığında, bu suçun m.244/1 ve 244/2'deki eylemlerin işlenmesi suretiyle haksız çıkar sağlanması şeklinde düzenlendiği görülmektedir. Bu nedenle fıkra kapsamında iki eylemden söz edilecektir;

i. Bir Bilişim Sisteminin İşleyişini Engellemek veya Bozmak Suretiyle Haksız Çıkar Sağlama

ii. Bir Bilişim Sistemindeki Verileri Bozmak, Yok Eden, Değiştirmek veya Erişilmez Kılmak, Sisteme Veri Yerleştirmek, Var Olan Verileri Başka Bir Yere Göndermek Suretiyle Haksız Çıkar Sağlama

Aşağıda bu eylemler değerlendirilmeye çalışılacaktır.

i. Bir Bilişim Sisteminin İşleyişini Engellemek veya Bozmak Suretiyle Haksız Çıkar Sağlama

TCK m. 244/1'deki düzenlemeye bakıldığında, bilişim sisteminin işleyişinin engellenmesi ve bozulması şeklinde seçimlik hareketler karşımıza çıkmaktadır. Başka bir suç oluşturmaması halinde, bu hareketlerden birisinin yapılması suretiyle haksız çıkar sağlanması suçun oluşabilmesi için yeterlidir[32]. Daha önce de belirtildiği gibi, 5237 sayılı TCK'da bilişim sisteminin tanımı yapılmamış, sadece m. 243'ün gerekçesinde *"..verileri toplayıp yerleştirdikten sonra bunları otomatik işlemlere tâbi tutma olanağını veren manyetik sistemlerdir."* şeklinde tanımlanmıştır. Bu tanımdan yola çıkılacak olursa, bir bilişim sisteminin işleyişinin temel ekseni; o bilişim sistemine yerleştirilen verilerin otomatik işleme tabi tutulması etrafında şekillenmektedir. O halde bir bilişim sisteminin işleyişini, kendisine yönlendirilen komutlara uygun olarak veri işleme faaliyeti olarak kabul etmek gerekir[33]. Bu faaliyete dışarıdan engelleme veya bozma suretiyle müdahale edilmesi suretiyle haksız çıkar sağlanması da, bu hareketin başka bir suçu oluşturmaması halinde, m. 244/4'deki suçu oluşturacaktır. "Engelleme" sözlükte, bir şeyin gerçekleşmesini veya yapılmasını önlemek[34], şeklinde tanımlanmaktadır. Buradan çıkacak sonuç, bilişim sisteminin işleyişinin engellenmesi, bilişim sistemine verileri işleme yönünde bir komut olmasına rağmen, verile-

---

32 Bu hareketlerden her ikisinin yapılması durumu temel cezanın belirlenmesinde dikkate alınacaktır. **Koca**, s. 93.

33 **Özbek/ Kanbur/ Doğan/ Bacaksız/ Tepe** s. 914.

34 http://tdkterim.gov.tr/bts/ (Erişim Tarihi: 23.10.2010).

CamScanner ile tarandı

rin otomatik işleme tabi tutulmasının kısmen veya tamamen önlenmesi şeklinde tanımlanabilir[35]. Bu anlamda, bilişim sistemi eskisi kadar hızlı çalışmamakta, veri alış verişi yapamamakta, veri işleme hızı düşmekte, istenilen performansta çalışamamakta, kısacası normal şartlarda yerine getirebildiği işlevlerini müdahale nedeniyle yerine getirememektedir. Örneğin, elektronik posta bombardımanı yoluyla sistemin kilitlenmesi[36].

Bilişim sisteminin işleyişini *bozmak* ise, kendisinden beklenen işi yapamayacak şekilde kısmen veya tamamen tahrip edilmesi durumu olarak kabul edilmelidir[37]. "bozma", sözlükte "*Bir şeyi kendisinden beklenilen işi yapamayacak duruma getirmek*" şeklinde tanımlanmaktadır[38]. Şu halde, bilişim sisteminden beklenecek faaliyet, verilerin otomatik işleme tabi tutulması olduğuna göre, bilişim sisteminin verileri otomatik işleme tabi tutması özelliğini yapamayacak duruma getirmek yani bilişim sistemini işlemez hale getirmek "*bozma*" şeklinde anlaşılacaktır[39].

ii. Bir Bilişim Sistemindeki Verileri Bozmak, Yok Etmek, Değiştirmek veya Erişilmez Kılmak, Sisteme Veri Yerleştirmek, Var Olan Verileri Başka Bir Yere Göndermek Suretiyle Haksız Çıkar Sağlama

TCK m. 244/2'de, bilişim sistemindeki soyut unsurlara bir başka deyişle verilere müdahale teşkil edecek seçimlik hareketler düzenlenmiştir. Başka bir suç oluşturmaması halinde, bu seçimlik hareketlerin gerçekleştirilmesi suretiyle haksız çıkar elde edilmesi durumunda m. 244/4'deki suç oluşacaktır. Dikkat edilecek olursa, kanundaki düzenlemede herhangi bir veriden değil, "*bilişim sistemindeki veriler*" den bahsedilmektedir. Bu bağlamda bir bilişim sistemi içinde yer almayan, disket, CD, flash bellek gibi bir bilişim sistemine bağlı olmayan ve tek başına bilişim sistemi olarak değerlendirilemeyecek, veri taşıma ve depolama cihazları içindeki verilere müdahaleler bu suçu oluşturmayacaktır[40].

---

35 Koca'ya göre, bilişim sisteminin veri işleme fonksiyonunu yerine getirememesine yol açacak müdahaleler, bilişim sisteminin işleyişinin engellemesi olarak nitelendirilir. **Koca**, s. 93.

36 **Kurt**, s. 164.

37 **Özbek/ Kanbur/ Doğan/ Bacaksız/ Tepe**, s. 914.

38 http://tdkterim.gov.tr/bts/(Erişim Tarihi: 23.10.2010).

39 Eker'e göre sistemin bozulması, sistemin çalışma düzenini aksatmak, işlemesini engellemekten öte, ayrıca bir sonucu doğuracak nitelikteki, yani sistemin artık olanaksız olduğu, hiçbir fonksiyonunu yerine getiremediği kronik bir çalışmama, bozulma durumunu yaratacak bir fiile tekabül eder. **Eker** Ö. Umut, " Türk Ceza Kanunu'nda Bilişim Suçları, Eski TCK Bağlamında Hukukumuzda Yer Alan İlk Düzenlemeler ve 5237 sayılı Yeni Türk Ceza Kanunu'nun İlgili Hükümlerinin Yorumu", TBBD, S. 62, 2006, s. 125.

40 **Koca**, s. 94; gerçekten de disket, CD, flash bellek gibi portatif veri taşıma araçları ancak bir bilişim sisteminde kullanıldıkları zaman, bilişim sisteminin bir parçası olurlar. Bu bağlamda içerdikleri veriler de ancak bilişim sisteminde kullanıldıkları zaman, "*bilişim sistemindeki veri*" olma

CamScanner ile tarandı

Maddede sayılan seçimlik hareketlerden ilki, "*verileri bozmak*" dır. Sistemin işleyişinin bozulması başlığı altında açıklandığı üzere "*bozmak*" , bir şeyi kendisinden beklenilen işi yapamayacak duruma getirmek anlamında olduğu için, bilişim sistemindeki verinin bozulmasındaki anlam, bu verinin kendisinden beklenen işlevi yerine getiremeyecek hale sokulması[41], verinin içeriğine veya yapısına müdahale etmek suretiyle kısmen veya tamamen kullanılmaz hale getirmektir. Ancak burada dikkat edilecek husus, bu hareketin bilişim sisteminde yer alan, fakat bilişim sisteminin işleyişinin unsuru olmayan veriler üzerinde gerçekleştirilmiş olması gerektiğidir. Zira, bozulan veri, bilişim sisteminin işleyişinin bir unsuru ise, bu durumda yaptırımı daha ağır olarak düzenlenmiş m. 244/1 söz konusu olacaktır.

Bir diğer seçimlik hareket ise, "*verileri yok etme*" dir. Sözlükte, "*yok etmek*" fiilinin anlamının ortadan kaldırmak, varlığına son vermek olduğu ifade edilmektedir. Ancak doktrinde de haklı olarak belirtildiği gibi[42], bir verinin bilişim sisteminden tamamen ortadan kaldırılması veya varlığına son verilmesi mümkün değildir. Bir başka deyişle, bir bilişim sistemindeki verinin silinmesi[43] [44] halinde dahi, sistemde yok olmaları söz konusu değildir. Bu anlamda verinin yok edilmesini, genel bir bakış açısıyla, o veriye erişim için verilen komutun sonuçsuz kalmasına neden olacak şekilde kayıtlardan silinmesi olarak ifade etmek yerinde olacaktır. Bu çerçevede veriye tekrar ulaşabilme imkanının varlığı suçun oluşmasını engellemez[45].

Madde kapsamındaki bir diğer seçimlik hareket, "*verileri değiştirmek*" dir. Verinin değiştirilmesi, verinin içeriğinin değiştirilmesini, bir veri yerine başka bir veri konmasını, bir verinin başka bir görünüm veya konuma getirilmesini ifade eder[46] [47].

özelliğini alırlar. Buradan çıkan sonuç ise, bir bilişim sistemine bağlanmayan bu portatif veri taşıma ve depolama cihazlarının bünyesindeki verilerin zarar görebilmesi için zaten bu cihazların fiziki anlamda zarar görmesi gerekmektedir. Bu durumda da TCK m. 151'de yer alan mala zarar verme suçu gündeme gelecektir.

41 Aynı yönde bkz. **Dülger**, s. 234.

42 **Dülger**, s. 236; **Kurt**, s. 168; **Taşkın** Şaban Cankat, Bilişim Suçları, İstanbul, 2008, s. 46-47.

43 *Doğan*'a göre, verilerin yok edilmesi verilerin silinmesi anlamına gelmektedir. **Doğan** Koray, "Bilişim Suçları ve Yeni Türk Ceza Kanunu", Hukuk ve Adalet Dergisi, S. 6-7, Y. 2, Ekim 2005, s. 303; *Ketizmen* de, verinin yok edilmesinin, verinin varlığına son verilmesi, ortadan kaldırılması ve verinin tamamen ya da büyük güçlüklerle elde edebilecek şekilde tasarrufundan çıkartılması olarak tanımlandığında, verinin silinmesinin de verinin yok edilmesi olarak değerlendirilebileceğini kabul etmiştir. Bkz. **Ketizmen** Muammer, Türk Ceza Hukukunda Bilişim Suçları, Ankara, 2008, s. 138-139.

44 Verinin geri dönüşüm kutusuna gönderilmesi durumunda ise, veri üzerinde tasarruf yetkisi bulunan kişi, bu veriye basit bir şekilde ulaşabileceğinden bu durumda verinin yok olmasından söz edilemez. Aksi görüş için bkz. **Dülger**, s. 236.

45 **Özbek/ Kanbur/ Doğan/ Bacaksız/ Tepe**, s. 919.

46 **Koca**, s. 95.

47 Yargıtay bir kararında, başkasına ait hesaptan internet bankacılığı yoluyla kendi hesabına para aktarmak şeklinde gerçekleşen olayda, m. 244'de yer alan "veri değiştirme" hareketinin oluştuğunu do-

CamScanner ile tarandı

Madde kapsamında yer alan dördüncü seçimlik hareket "*veriyi erişilmez kılmak*" dır. Verinin erişilmez kılınması, genel olarak verinin içerdiği bilgi ya da enformasyona müdahale edilmeden veriye olağan şekilde erişimin engellenmesi olup, burada veri içerik bakımından bütünlüğünü korumaktadır. Veri ne yok edilmekte ne de bozulmakta fakat verilere ulaşım için gereken işlem bağı kopa-rılmaktadır[48]. Örneğin, bir kimsenin bilgisayarındaki word dosyasına şifre koy-mak veya var olan şifreyi değiştirmek bu nitelikte bir harekettir[49]. Veriye erişil-mesi bakımından yasada bir ayırım yapılmadığı için, erişimin engellenmesinin geçici ya da daimi olması arasında bir fark yoktur[50].

Madde kapsamında yer alan beşinci seçimlik hareket ise, "*sisteme veri yer-leştirmek*" dir. TCK m. 244/2'de yer alan seçimlik hareketler içerisinde "*sisteme veri yerleştirmek*" hareketi, bilişim sisteminde hali hazırda bulunan veriler üze-rinde gerçekleşmeyen tek hareket olarak karşımıza çıkmaktadır. Bir başka deyiş-le, bu hareket, bilişim sistemine dışarıdan verilerin kaydedilmesi veya yüklenmesi şeklinde işlendiği için, bilişim sisteminde daha önce mevcut bulunan veriler üze-rinde değil, bilişim sistemi üzerinde gerçekleşmektedir. Bu hareket ile, fail tara-fından bilişim sistemine dışarıdan ve sistemin malikinden ya da ilgili kişiden izin alınmaksızın çeşitli verilerin kaydedilmesi, yüklenmesi ya da eklenmesi[51] ifade edilmektedir. Sisteme veri yerleştirme izinli veya izinsiz girilen sisteme doğrudan veri girişi yapılmak suretiyle gerçekleştirilebileceği gibi, veri saklama veya depo-lama araçlarıyla verinin sisteme aktarılması ya da internet ortamında sisteme her-hangi bir verinin kaydedilmesi şekillerinde gerçekleşebilir[52].

Madde kapsamında yer alan son seçimlik hareket "*sistemde var olan verile-ri başka bir yere göndermek*" dir. Bilişim terimleri sözlüğünde "*göndermek*" sözcüğü, "*Bir yerden veri gönderip başka bir yerden almak*" şeklinde tanım-lanmış[53] ve İngilizce karşılığının "*transfer*" olduğu belirtilmiştir. Veri gönder-mek ya da bir başka deyişle veri transferi, bir bilişim sistemindeki verilerin, başka bir bilişim sistemine veya verilerin saklanabileceği ortamlara, bir kopya-sının alınması, aktarılması, taşınması olarak anlaşılması gerekir[54].

---

laylı da olsa belirtmektedir. "*Bilişim sistemindeki verileri değiştirmek suretiyle haksız menfaat elde edilmesi suçunun sanık tarafından havalenin şikayetçilerin hesaplarından kendi hesabına intikali anında tamamlandığı gözetilmeyerek eylemin teşebbüs aşamasında kaldığından bahisle eksik ceza tayini...*" Yargıtay 11. Ceza Dairesi, E. 2007/6963, K. 2007/5533, T. 18.9.2007(www.kazanci.com.tr).

48 **Özbek/ Kanbur/ Doğan/ Bacaksız/ Tepe**, s. 919.

49 **Koca**, s. 95.

50 **Dülger**, s. 237.

51 **Dülger**, s. 237.

52 **Koca**, s. 95.

53 http://tdkterim.gov.tr/?kelime=g%F6ndermek&kategori=terim&hng=md (Erişim Tarihi: 23.10.2010).

54 Dülger'e göre, somut varlığı olmayan verilerin somut bir hareketi içeren göndermek eylemiyle açıklanması mümkün değildir. Ancak bilişim alanında özellikle e-posta yoluyla veri aktarılması

CamScanner ile tarandı

Bu seçimlik hareketlerin birinin yapılması suretiyle haksız bir çıkar sağlanması durumunda, bu hareketin başka bir suçu oluşturmaması halinde, m. 244/4'de yer alan suç oluşacaktır. Ancak dikkat edilecek olunursa, bir fiilin bu seçimlik hareketlerden hangisinin kapsamına girdiğinin tespiti çok güçtür. Zira bu seçimlik hareketler ve sonuçları birbirleriyle iç içe kavramlardır. Bazı durumda verinin değiştirilmesi onun erişilmez kılınması sonucunu, bazı durumlarda ise veri gönderilmesi verilerin bozulması sonucunu doğurmaktadır. Nitekim Yargıtay, başkasına ait şifrenin ele geçirilerek, internet bankacılığı yoluyla kendi hesabına havale yoluyla para aktarma eylemini, bir kararında veri değiştirme[55], bir başka kararında ise veri göndermek[56] suretiyle haksız çıkar sağlama suçunun oluştuğuna karar vermiştir.

TCK m. 244/4'de yer alan suçun neticesi, failin kendisinin veya başkasının yararına sağlamış olduğu "*haksız çıkar*" dır. Çıkar kelimesi sözlükte[57], "*Dolaylı bir biçimde elde edilen kazanç, menfaat, yarar*" olarak ifade edilmektedir. Bu anlamda failin elde etmiş olduğu her türlü menfaat ya da yarar bu suçun neticesini oluşturabilecektir. Elde edilen çıkarın maddi veya manevi olması önem taşımaz. TCK m. 244/4'de yer alan suç netice bakımından bir zarar suçudur[58].

4. Hukuka Aykırılık

Bilişim sisteminin işleyişine veya sistemdeki verilere müdahale yoluyla haksız çıkar sağlama (m. 244/4) suçunda, gündeme gelebilecek ilk hukuka uygunluk sebebi, ilgilinin rızası (m.26/2) dır. Bu anlamda bilişim sisteminde ve sistemde var olan veriler üzerinde, mutlak tasarruf yetkisi bulunan kişilerin göstermiş oldukları rıza kapsamında gerçekleştirilen eylemlerde hukuka aykırılık kalkacaktır. Ancak, bir bilişim sisteminin işleyişi hakkında tasarruf yetkisine

---

için, somut posta hizmetleri için geçerli olan "göndermek" eylemi yaygın bir şekilde kullanıldığı için olsa gerek yasa koyucu bu kavramdan esinlenmiştir. Bkz. **Dülger**, s. 238.

55 "*Bilişim sistemindeki verileri değiştirmek suretiyle haksız menfaat elde edilmesi suçunun sanık tarafından havalenin şikayetçilerin hesaplarından kendi hesabına intikali anında tamamlandığı gözetilmeyerek eylemin teşebbüs aşamasında kaldığından bahisle eksik ceza tayini...*" Yargıtay 11. Ceza Dairesi, E. 2007/6963, K. 2007/5533, T. 18.9.2007 (www.kazanci.com.tr).

56 "*Somut olayda; sanığın, mağdurların bankalarda bulunan para hesaplarındaki var olan verileri (bilgileri) sahte kimliklerle açtırdığı hesaplara internet yoluyla göndererek, yine sahte kimliklerle bu paraları çekmek istemesinden ibaret eylemlerinin; paranın sanığın açtırdığı hesaplara intikaline kadar gerçek kişilere yöneltilmiş hile bulunmayıp eylemlerin tamamen bilişim sistemi içinde gerçekleştirildiğinden, her bir mağdura karşı işlenmiş ayrı ayrı TCK'nın 244/4 maddesine uyan suçu oluşturduğu ve paranın açtırdığı hesaplara transferiyle suçun tamamlanacağı gözetilmeden, suçun vasıflandırılmasında yanılgıya düşülerek nitelikli dolandırıcılığa teşebbüs suçundan mahkûmiyet hükmü kurulması...*" Yargıtay 11. Ceza Dairesi, E. 2007/6709, K. 2007/6012, T. 27.9.2007. (www.kazanci.com.tr).

57 http://tdkterim.gov.tr/bts/ (Erişim Tarihi: 24.10.2010).

58 *Dülger*'e göre, m. 244/4'de düzenlenen suçun oluşabilmesi açısından kanunda sadece, m. 244/1 ve 2'deki eylemlerin gerçekleştirilmesi yoluyla haksız yarar elde edilmesinin düzenlendiğini, bunun sonucunda bir zararın gerçekleşip gerçekleşmediğinin aranmayacağı gerekçesiyle m. 244/4'de düzenlenen suç tehlike suçudur. Bkz. **Dülger**, s. 247.

CamScanner ile tarandı

sahip olan kişi, her zaman bu sistem içindeki veriler üzerinde tasarruf yetkisine sahip olan kişi olmayabilir. Bu durumda, hukuka aykırılığı ortadan kaldıracak rızanın belirlenmesi açısından, her durumda ilgili kişinin tespiti önem arz etmektedir. Şüphesiz internet bankacılığında gerçekleştirilen eylemler açısından, rıza açıklamasında bulunabilecek ilgili kişi, banka ile internet bankacılığı sözleşmesi yapan banka müşterisidir.

Diğer bir hukuka uygunluk sebebi ise, TCK m. 24/1'de yer alan kanun hükmünün icrasıdır. Bu kapsamda, CMK m. 134 çerçevesinde bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve el koyma işlemleri, verilere müdahale niteliği taşımasına rağmen, hukuka aykırılık unsurunu oluşturmayacaktır. Yine 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun kapsamında verilen erişimin engellenmesi kararları kapsamında gerçekleştirilen eylemler de, haksız olarak nitelendirilemeyecektir.

5. Manevi Unsur

Bilişim sisteminin işleyişine veya sistemdeki verilere müdahale yoluyla haksız çıkar sağlanması suçu ancak kasten işlenebilir. Ancak bu suçun oluşabilmesi için, failin m. 244/1 ve 2'deki eylemleri gerçekleştirmek yönündeki genel kastı yeterli olmayıp, haksız çıkar sağlama yönünde özel kastının da bulunması gerekmektedir. Bir diğer ifadeyle, fail bilişim sisteminin işleyişine ya da sistemdeki verilere müdahaleyi, kendisine veya başkasına haksız çıkar sağlamak amacıyla gerçekleştirmelidir. Bu suçun oluşabilmesi açısından, failin özel kastının aranmasının sonucu, bu suçun olası kastla işlenememesidir[59].

6. Teşebbüs

TCK m.244/4 incelendiğinde, esasen m. 244/1 ve 2'nin devamı niteliğinde olduğu, bu fıkralarda düzenlenen temel suç tipine bağlılığın devam ettiği görülür. Ayrıca, m. 244/4'deki "*yukarıdaki fıkralarda tanımlanan fiillerin işlenmesi suretiyle*" ifadesi bunu ortaya koymaktadır. Bu ifadeden de anlaşılacağı üzere, m. 244/4'de yer alan düzenleme, m. 244/1 ve 2'de yer alan suçların nitelikli hali olarak düzenlenmiştir. Bunun sonucu olarak, nitelikli halin gerçekleşmemesi durumunda teşebbüsten söz edilemez[60]. Sadece bu hal uygulanmaz ancak suçun basit şeklinden ceza verilebilir. Suçun tamamlanması açısından bakıldığında ise, m. 244/1 ve 2'de yer alan fiillerle, haksız çıkarın elde edildiği anda suç tamamlanır[61].

---

59 **Özbek** Veli Özer/**Kanbur** M. Nihat/ **Bacaksız** Pınar/**Doğan** Koray/ **Tepe** İlker, Türk Ceza Hukuku Genel Hükümler, Ankara, 2010, s. 247.

60 Aksi görüş için bkz. **Koca**, s. 98.

61 "Bilişim sistemindeki verileri değiştirmek suretiyle haksız menfaat elde edilmesi suçunun sanık tarafından havalenin şikayetçilerin hesaplarından kendi hesabına intikali anında tamamlandığı gözetilmeyerek ey-

CamScanner ile tarandı

7. Suçluların Çokluğu (Suça İştirak)

TCK m. 244/4'de düzenlenen suç tipinde, iştirak açısından özellikli bir durum yoktur. İştirake ilişkin genel hükümler geçerlidir.

8. Suçların Çokluğu (Suçların İçtimaı)

TCK m. 244/4'de yer alan düzenlemeye bakıldığında, yasa koyucunun özel bir içtima kuralı düzenlediği görülmektedir. Bilişim sisteminin işleyişine veya sistemdeki verilere müdahale yoluyla haksız çıkar sağlanması durumunda, bu fiilin ancak başka suç oluşturmaması halinde, m.244/4'deki suçun oluşacağı maddede düzenlenmiştir. Yasa koyucu burada yasaların tekliği(görünüşte içtima) hali yaratmış ve m. 244/4'ün oluşabilecek diğer suçlara göre tali norm olduğunu düzenlemiştir. Bu özel düzenleme karşısında, bir fiilin kanunda birden fazla ceza normunu ihlal etmesi durumunda, TCK m. 44 (fikri içtima) gereğince yapılacak olan bu suçlardan en ağır cezayı oluşturan suçu belirleme işlemi, bu suç açısından yapılmayacaktır. Bir başka deyişle, bu fiilin daha hafif cezayı öngören bir suçu oluşturması halinde de fail m. 244/4'den değil, bu suçtan cezalandırılacaktır.

Bu suçun zincirleme suç şeklinde işlenmesi mümkündür. Örneğin, başkasına ait internet bankacılığı şifresini hukuka aykırı olarak ele geçirip, bu kişinin banka hesabından bir suç işleme kararı kapsamında değişik zamanlarda haksız çıkar sağlanması. Aynı şekilde, failin başkasına ait mevduattan belirli aralıklarla kesinti sonucunu doğuracak internet bankacılığı yoluyla talimat vermesi durumunda da zincirleme suç gündeme gelecektir. Örn., failin başkasına ait mevduat üzerinde,, internet bankacılığı yoluyla fatura ödeme talimatı veya düzenli kontör yükleme talimatı vermesi.

9. Yaptırım

Bilişim sisteminin işleyişine veya sistemdeki verilere müdahale yoluyla haksız çıkar sağlanması suçu için yasa koyucu, hem hürriyeti bağlayıcı ceza (iki yıldan altı yıla kadar hapis) hem de adli para cezası (beş bin güne kadar) öngörmüştür.

TCK m. 246 uyarınca, bu suçun işlenmesi suretiyle yararına haksız menfaat sağlanan tüzel kişiler hakkında bunlara özgü güvenlik tedbirlerine hükmolunacaktır (TCK m. 60).

10. Muhakeme

TCK m. 244/4' de düzenlenen bilişim sisteminin işleyişine veya sistemdeki verilere müdahale yoluyla haksız çıkar sağlanması suçu, resen takip edilen bir

lemin teşebbüs aşamasında kaldığından bahisle eksik ceza tayini, isabetsizdir." Yargıtay 11. Ceza Dairesi, E. 2007/6963, K. 2007/5533, T. 18.9.2007. (www.kazanci.com.tr).

CamScanner ile tarandı

suçtur. Bu suça ilişkin yargılamada görevli mahkemeler Asliye Ceza Mahkemeleridir (5235 sayılı k. m. 11).

V. GÖRÜŞÜMÜZ

İncelememize konu olan, Yargıtay Ceza Genel Kurulu kararı bakımından da önem arz etmeleri nedeniyle, bu bölümde TCK m. 244/4'de düzenlenen bilişim sisteminin işleyişine veya sistemdeki verilere müdahale yoluyla haksız çıkar sağlama suçu ile, TCK m. 142/2-e'de düzenlenen bilişim sistemlerinin kullanılması suretiyle hırsızlık ve TCK m. 158/1-f'de düzenlenen bilişim sistemlerinin kullanılması suretiyle dolandırıcılık suçlarının ilişkisine değinilmeye çalışılacaktır. 5237 sayılı TCK'nın yürürlüğe girmesiyle birlikte, bilişim suçları TCK'nın ikinci kitabının üçüncü kısmı olan "Topluma Karşı Suçlar" altında "Bilişim Alanında Suçlar" başlığı ile onuncu bölümünde düzenlenmiştir. Bilişim suçlarının ayrı bir bölümde düzenlenmesi ile birlikte ayrıca 765 sayılı TCK'dan farklı olarak, hırsızlık ve dolandırıcılık gibi malvarlığına karşı suçlar altında düzenlenmiş suçların bilişim sistemleri aracılığıyla işlenmesini de bu suçların nitelikli hali olarak öngörülmüştür[62] [63].

TCK m. 244/4 düzenlemesine bakıldığı zaman, bilişim sisteminin işleyişine veya sistemdeki verilere müdahale suretiyle haksız çıkar sağlama eylemi, ancak başka bir suç oluşturmaması halinde, bu madde kapsamına girecek şekilde düzenlenmiştir[64]. Madde kapsamında yer alan "*fiilin başka bir suç oluşturmaması*[65]" koşulunun ne anlama geleceği hususu üzerinde durulmalıdır. Söz konusu ifade bizim yasaların tekliği (görünüşte içtima) hallerinden biri olarak kabul etmiş olduğumuz asli-tali norm ilişkisi içinde değerlendirilmelidir[66]. Bir norm

---

62 Doktrinde 5237 sayılı TCK'daki bu düzenleme tarzı eleştirilmektedir. *Yazıcıoğlu*'na göre, suçta ve cezada kanunilik ve kıyas yasağı gibi ilkeler karşısında uygulama olanağı bulunmayacak olmasına rağmen, bilişim suçlarını hırsızlık ve dolandırıcılık gibi suçlar içinde değerlendirmek yerinde değildir. **Yazıcıoğlu** Yılmaz, "Yeni Türk Ceza Kanunundaki Suçların Genel Değerlendirmesi", Yeditepe ÜHFD, S. 2, 2005, C. II, s. 396.

63 TCK m. 158/1-f'de düzenlenen bilişim sistemlerinin kullanılması suretiyle dolandırıcılık suçunun madde gerekçesine bakıldığında bu nitelikli hale yer verilmesi nedeni "*...Bilişim sistemlerinin...araç olarak kullanılması, dolandırıcılık suçunun işlenmesi açısından önemli bir kolaylık sağlamaktadır.*" şeklinde açıklanmaktadır.

64 Bu husus madde gerekçesinde de vurgulanmıştır: "*...fiilin örneğin dolandırıcılık, hırsızlık, güveni kötüye kullanma veya zimmet suçunu oluşturması hâlinde, bu fıkra hükmüne istinaden cezaya hükmedilmeyecektir.*"

65 Daha önce de belirtildiği üzere, madde gerekçesinde bu husus "*fiilin daha ağır cezayı gerektiren başka bir suç oluşturmaması*" şeklinde yer almış, madde metni ile gerekçesi arasında çelişki meydana gelmiştir. Ancak bağlayıcılık noktasında sadece kanunda yer alan düzenlemeye itibar edileceğinden, söz konusu fiilin TCK'da başka bir suçu oluşturup oluşturmadığına bakılacak, bu suçun daha ağır bir suç olması gerekmeyecektir.

66 Birden fazla ceza kanunundan ya da aynı kanunda yer alan birden fazla ceza normundan birinin uygulanması diğerinin uygulanmasını gereksiz kılıyor ise yasaların tekliğinden (görünüşte içtima) söz edilir. **Özbek/ Kanbur/ Doğan/ Bacaksız/ Tepe,** Genel Hükümler, s. 531, 533.

CamScanner ile tarandı

diğer bir norm uygulanmadığı sürece uygulanabilir hale geliyorsa ikincil ya da talidir. Bu anlamda bilişim sisteminin işleyişine veya sistemdeki verilere müdahale yoluyla haksız çıkar sağlama eylemi açısından, ilk başta m. 244/4'deki düzenlemeye başvurulmayacak, TCK'da yer alan diğer suçların oluşup oluşmadığı yönünde bir irdeleme yapılacaktır.

Bu açıklamalar ışığında, internet bankacılığına değinmek gerekecektir. İnternet bankacılığı kısaca bankacılık işlemlerinin internet üzerinden yapıldığı bankalarca oluşturulmuş sistem olarak tanımlanmaktadır. Gerçekten de, banka müşterisi internet bankacılığı sayesinde, daha önceden banka ile yapmış olduğu sözleşme kapsamı dahilinde, fiziki banka şubesine gitmeksizin, dilediği bankacılık işlemlerini internet aracılığıyla yapabilmektedir. İnternet bankacılığı ile fiziki anlamda banka şubesine gidilerek bankacılık işlemlerinin yapılması arasındaki temel fark, fiziki şubelerde işlem yapabilmek için müşterinin üzerinde işlem yapmak istediği hesaplar açısından, tasarrufta bulunma yetkisi olduğunun kimliği ile saptanmasıdır. İnternet bankacılığında ise durum farklıdır. İnternet bankacılığı kullanan banka müşterisinin kimlik doğrulama işleminde, aradan insan unsuru kalkmakta ve bankanın internet bankacılığı için hazırlamış olduğu bilişim sistemi ve buna ait yazılımlar devreye girmektedir. Banka müşterisi ile banka arasında yapılan sözleşmeyle, bankanın oluşturmuş olduğu bilişim sisteminin banka müşterisini tanıması için bir diğer ifade ile kimlik doğrulaması yapabilmesi için, banka müşterisine kişiye özel kullanıcı adı, parola/şifre ve diğer ek güvenlik unsurları[67] sağlanmaktadır. Bankanın hazırlamış olduğu bilişim sisteminin, ilgili kişiyi tanıması ile, kişi işlem yapabileceği alana geçiş yapabilecektir.

İnternet bankacılığının genel çerçevesi ortaya konulduktan sonra, acaba haksız bir şekilde ele geçirilen internet bankacılığı parolası/şifresi ile başkasına ait mevduatlardan havale yaparak haksız çıkar sağlanması eylemi 5237 sayılı TCK'da hangi suçu oluşturmaktadır? Daha önce de belirtildiği, TCK m. 244/4'de yer alan suçun oluşabilmesi için, fiilin başka bir suçu oluşturmaması gerekecektir. Bu nedenle söz konusu eylemin, ilk başta, TCK m. 142/2-e'de yer alan bilişim sistemleri aracılığıyla hırsızlık suçunu oluşturup oluşturmadığına bakılmalıdır. TCK m. 142/2-e normu hırsızlık suçunun nitelikli hali olarak düzenlenmiştir. Bu nedenle hırsızlık suçunun basit halindeki unsurlar, nitelikli hal açısından da aranacaktır. TCK m. 141/1'e göre, "*Zilyedinin rızası olmadan başkasına ait taşınır bir malı, kendisine veya başkasına bir yarar sağlamak maksadıyla bulunduğu yerden alan kimseye bir yıldan üç yıla kadar hapis cezası verilir.*" Maddeden anlaşılacağı üzere, hırsızlık suçunun hukuki konusu taşınabilir bir maldır[68]. Dokt-

---

67 Bu ek güvenlik unsurları tek kullanımlık parola/şifre, önceden tanımlanmış IP kısıtlaması, mobil telefona gelen onay kodunun sorulması vb. şeklinde gerçekleşebilmektedir.

68 *Yazıcıoğlu*'na göre, kanunun hırsızlık ve dolandırıcılık suçlarında, bu suçların bilişim sistemlerinin kullanılması suretiyle işlenmesi durumunu nitelikli hal olarak düzenlemesi, kendi içinde çe-

CamScanner ile tarandı

rinde haklı olarak, bilişim sistemlerinin kullanılması suretiyle hırsızlık suçunun kapsamının anlaşılamaması nedeniyle m. 142/2-e hükmü eleştirilmiştir[69].

Acaba internet bankacılığı yoluyla başkasına ait hesaplardan kendi hesabına havale yapılması eyleminde, suçun üzerinde gerçekleştiği şey "*taşınabilir bir mal*" mıdır? Bu soruya olumlu yanıt vermek mümkün değildir. Zira dikkat edilecek olursa, fail icra hareketlerini banka bilişim sisteminde var olan soyut unsurlar üzerinde gerçekleştirmektedir. 5237 sayılı TCK'da verinin tanımı yapılmamakla birlikte, TCK m. 243'ün gerekçesinde, sistemdeki soyut unsurların veri olduğu belirtilmiştir. Benzer şekilde, 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun m. 2/1-k' da ise veri, "*Bilgisayar tarafından üzerinde işlem yapılabilen her türlü değeri..*" ifade etmektedir. Buradan çıkacak sonuç, banka müşterileri tarafından internet şubesi aracılığıyla üzerinde işlem yapılan her unsur, aslında banka bilişim sisteminde yer alan soyut unsurlardır yani veridir. Bu verilerin ekonomik değer taşıyan kavramları temsil etmesi, bu unsurları kanunun ifadesi ile "*taşınabilir mal*" kapsamına dahil etmeye yetmemektedir. Gerçekten de internet şubesinde yapılan banka havalelerinde, aslında fiziki anlamda verilerin temsil ettiği paralar taşınmamakta, gönderilmemekte ya da bulunduğu yerden alınmamakta(söz konusu veriler ya da bu verilerin temsil ettiği paralar halen bankada ve bilişim sisteminde var olmaya devam etmektedir)dır. Burada sadece müşteri tarafından banka bilişim sistemine gönderilen komut gereği, veri transferi yoluyla bu verilere, havale edilen kişinin hesabı aracılığıyla işlem yapılabilmesi yetkisi sağlanmaktadır. Ayrıca kanımızca, havale edilen şey bir bilişim sistemi kullanıldığı sürece "veri" dir. TCK m. 244'de yer alan düzenleme bu yönüyle, hırsızlık ve dolandırıcılık suçlarına nazaran özel bir norm niteliği taşımaktadır. Söz konusu transfer edilen unsurun bir malvarlığı değeri olduğunun kabulü halinde, TCK. m. 244/3 ve 4'deki düzenlemelerin bir anlamı kalmayacaktır. Gerçekten de, yasa koyucu bu tür veri transferle-

---

lişki yaratmaktadır. Bu çelişkiyi de m. 163'ün gerekçesi ile açıklamaktadır. 5237 sayılı TCK m. 163'ün gerekçesinde "*...başkasına ya da kamuya ait telefon şebekesinden bedeli ödenmeksizin ve hukuk dışı yollarla yararlanılması durumunda, hırsızlık suçu oluşmaz. Çünkü, ortada taşınabilir bir mal yoktur.*" Bkz. **Yazıcıoğlu**, s. 398.

69 *Hafızoğulları/Özen*'e göre, bilişim sistemlerini kullanarak hırsızlık suçunun işlenmesinin yeterince belli, belirgin olduğu söylenemez. Bu hükümle, şifreli kilitlerin şifrelerinin kırılması, hırsızlığa karşı alınan elektronik tedbirlerin gene bu yolla giderilmesi mi kastedilmektedir, yoksa ..... hükümleri karşısında hukuka aykırı olarak eline geçirdiği kredi kartının şifresini kırarak bir kimsenin banka hesabından para çekmek, banka hesaplarına girerek para çekmek, bir hesaptan diğer bir hesaba para aktarmak, vs. mi anlaşılmaktadır, belli değildir. Yine *Hafızoğulları/Özen*'e göre, bu hüküm, kilit yerine geçen, güvenlik sağlayan elektronik sistemlerin gene bu yolla giderilerek hırsızlık yapılması ile sınırlıdır. Bkz. **Hafızoğulları** Zeki/**Özen** Muharrem, "Hırsızlık", Gazi Üniversitesi HFD ,S. 1-2, C. XII, 2008, s. 794-795; **Hafızoğulları** Zeki/**Özen** Muharrem, Türk Ceza Hukuku Özel Hükümler Kişilere Karşı Suçlar, Ankara, 2010, s. 331-332; **Dülger**, s. 290. **Özbek/ Kanbur/ Doğan/ Bacaksız/ Tepe,** Özel Hükümler, s. 925.

CamScanner ile tarandı

rinin (internet bankacılığı yoluyla başka hesaba havale) gerçekleşeceğini önörmüş olmalıdır ki, fiillerin bir banka veya kredi kurumuna ait bilişim sistemi üzerinde işlenmiş olmasını ağırlatıcı sebep olarak düzenlemiş ve bu fiillerle haksız çıkar sağlanmasını da ayrıca cezalandırma yoluna gitmiştir.

TCK. m. 244/4 ile 142/2-e'nin farkı ortaya konulduktan sonra, bir başka önem arz eden konu da TCK m. 244/4 ile bilişim sistemlerinin kullanılması suretiyle dolandırıcılığı düzenleyen TCK. m. 158/1-f'nin farkının ortaya konulmasıdır. Bilindiği üzere dolandırıcılık suçunun oluşabilmesi için, hileli davranışlarla bir kişinin aldatılması yani aldatıcı davranışların gerçek bir kişiye yönelmesi gerekmektedir. Yargıtay da söz konusu suçlar bakımından ayrımı ortaya koyarken gerçekleştirilen eylemin, kime veya neye karşı gerçekleştirildiği kriterinden yola çıkarak, kararlarını vermektedir. Bir başka deyişle, başkasına ait internet bankacılığı şifresini haksız olarak ele geçirip, bu kişilerin hesabından kendi hesabına para transfer edilmesi olayında, gerçek kişilere yönelik ve bu kişilerin iradesini etkileyecek bir hileli davranış olmaması sebebiyle, TCK m. 158/1-f'de düzenlenen nitelikli dolandırıcılık suçu oluşmayacaktır[70]. Bu durumda, failin eylemi m. 244/4 nedeniyle cezalandırılacaktır. Bilişim sistemlerinin kullanılması suretiyle dolandırıcılık suçu için, başkasına ait MSN hesabının ele geçirilerek, internet yoluyla o kişinin arkadaş listesindeki kişilerle kendisini hesabın gerçek sahibi gibi tanıtarak, bu kişilerin kendisine ait bir hesaba havale yapmalarını sağlaması örneği verilebilir[71].

Yargıtay Ceza Genel Kurulunun vermiş olduğu kararın gerekçesine bakılacak olursa, somut olayın değerlendirmesinde Yargıtay'ın, failin kastı noktasından hareket ettiği görülmektedir[72]. Yargıtay'a göre, failin daha önce haksız bir şekilde

---

70 *"Dolandırıcılık suçunda unsur olan hileli davranışların gerçek kişiye yönelmesi ve bunun sonunda onun veya başkasının malvarlığı aleyhine sanığın veya başkasının yararına haksız bir menfaat sağlanması gerekeceği, somut olayda ise, sanığın bilgisayara virüs bulaştırmak suretiyle ele geçirdiği şifreleri kullanarak şikayetçinin G. Bankası Bergama Şubesi'nde bulunan yatırım hesabına girip hesaptaki paradan 21.400TYL.yi G. Bankası Galata Şubesine Ö. K. adına havale ettirmek ve sahte kimlikle parayı çekmekten ibaret eyleminde, gerçek kişiye yönelen hileli bir hareket bulunmaması nedeniyle dolandırıcılık suçunun unsurlarının oluşmadığı, fiilin TCK.nun 244/4.maddesinde öngörülen "bilişim sistemini bozma suretiyle haksız çıkar sağlama" suçunu oluşturduğu gözetilmeden.."* Yargıtay 11. Ceza Dairesi E. 2009/3019, K. 2009/6644, T. 28.5.2009 (www.kazanci.com.tr); benzer yönde bkz. 11. CD., E. 2009/1616, K. 2009/11328, T. 7.10.2009, 11. CD. E. 2006/6653 K. 2006/9374 T. 22.11.2006 (www.kazanci.com.tr).

71 **Özbek/ Kanbur/ Doğan/ Bacaksız/ Tepe,** Özel Hükümler, s. 924; aynı şekilde Yargıtay bir kararında (11.CD, 24.10.2007 tarih 7300/7063 sayılı kararı), internet aracılığıyla elde ettiği bir başkasına ait e-posta adresini kullanarak, o kişinin arkadaşlarına mesaj çekerek kontör istemesinin mağdur sayısınca bilişim sistemlerinin kullanılması suretiyle dolandırıcılık suçunu oluşturduğuna karar vermiştir. **Bakıcı** Sedat, 5237 sayılı Yasa Kapsamında Ceza Hukuku Özel Hükümler 1, Ankara, 2008, s. 459.

72 *"...Sanık Volkan'ın; firari Saim ile birlikte hareket ederek, daha önceden haksız bir şekilde ele geçirdikleri katılan firmanın internet bankacılık şifresini kullanmak suretiyle, katılanın Ş bank Ankara K. .. Şubesindeki hesabından 10.750 YTL'yi Ş ... bank-İstanbul Z Şubesinde sanık Volkan adına açtırdıkları hesaba havale edip, aynı gün banka şubesinden çekmek şeklinde gerçekleştirdiği eylemdeki kastı, katılan firmanın banka hesabında bulunan, taşınır nitelikteki parayı bilişim sistemini kullanmak sure-*

CamScanner ile tarandı

elde etmiş olduğu internet bankacılığı şifresini kullanarak, katılana ait hesaptan, kendi adına açtırmış olduğu hesaba havale yapması eylemindeki kastı, katılanın hesabındaki verilerin temsil ettiği parayı mal edinmektir. Yine Yargıtay'a göre, failin bu eylemdeki kastı varolan verilerin başka bir yere gönderilmesi değildir. Bu husus hakkında hemen belirtmek gerekecektir ki, TCK m. 244/4'de yer alan bilişim sisteminin işleyişine veya sistemdeki verilere müdahale yoluyla haksız çıkar sağlamak suçunda, TCK m. 244/1 ve 2'de olduğu gibi failin kastı sadece bilişim sistemin işleyişine veya verilere müdahale etmek değildir. Failde eylemi gerçekleştirirken, haksız çıkar sağlama yönünde özel kastının bulunması gerekmektedir. Bu bağlamda failin, başkasına ait hesaplar üzerinden kendi hesabına para transferi yapması eylemindeki kastı, sadece var olan veriyi başka bir yere göndermek değil, aynı zamanda haksız çıkar sağlanmasına da yöneliktir. Bu değerlendirme ile Yargıtay aslında TCK m. 142/2-e ile TCK m. 244/2 arasındaki ilişkiyi ortaya koymuştur. Ancak TCK m. 244/4'de yer alan suç bakımından da failin kastı verilerin temsil ettiği paraları mal edinmek suretiyle yarar sağlamak olabilecektir. Ancak fail bu durumda, kastını gerçekleştirebilmek için banka bilişim sisteminde yer alan verileri göndermektedir. Burada önem arz eden husus, m. 244/4'ün tali norm olma özelliği nedeniyle, m. 244/4'deki suçu oluşturan söz konusu eylemin, m. 142/2-e'de düzenlenen suç tipine uyup uymaması, yani eylemin bu suçun kanuni tanımındaki unsurları gerçekleştirip gerçekleştirememesidir. Bu durum ise ceza kanunlarının güvence işlevini sağlayan, ceza hukukunun temel ilkesi suçta ve cezada kanunilik ilkesinin doğal bir sonucudur.

Failin gerçekleştirmiş olduğu eyleme bakılacak olursa bu eylemlerin banka bilişim sisteminde var olan veriler üzerinde gerçekleştiği görülecektir. Zira bilişim sistemi üzerindeki her soyut unsur veri olarak kabul edilmektedir. Bu açıdan transfer edilen şey taşınabilir bir mal olarak para değil, veridir. Bu nedenlerle Yargıtay Ceza Genel Kurulu Kararına (CGK., 17.11.2009 Tarih, K:2009/268, E:2009/11-193, YKD., S. 4, C. 36, Nisan 2010, s. 705-725) katılmıyoruz.

---

tiyle 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..." Yargıtay Ceza Genel Kurulu, E. 2009/11-193, K. 2009/268, T. 17.11.2009(YKD., S. 4, C. 36, Nisan 2010, s. 714-715).

CamScanner ile tarandı

KAYNAKÇA

Bakıcı Sedat, 5237 sayılı Yasa Kapsamında Ceza Hukuku Özel Hükümler 1, Ankara, 2008.

Çeker Mustafa, "İnternet Bankacılığı ve Bankaların Sorumluluğu", Prof. Dr. Hüseyin Ülgen'e Armağan, İstanbul, 2007.

Dülger Murat Volkan, Bilişim Suçları, Ankara, 2004.

Eker Ö. Umut, "Türk Ceza Kanunu'nda Bilişim Suçları, Eski TCK Bağlamında Hukukumuzda Yer Alan İlk Düzenlemeler ve 5237 sayılı Yeni Türk Ceza Kanunu'nun İlgili Hükümlerinin Yorumu", TBBD, S. 62, 2006.

Hafızoğulları Zeki/**Özen** Muharrem, "Hırsızlık", Gazi Üniversitesi HFD ,S. 1-2, C. XII, 2008.

Hafızoğulları Zeki/**Özen** Muharrem, Türk Ceza Hukuku Özel Hükümler Kişilere Karşı Suçlar, Ankara, 2010.

Kaya Taner, "İnternet Bankacılığı", Bilişim ve Hukuk Dergisi(Ankara Barosu), S. 9, 2008.

Ketizmen Muammer, Türk Ceza Hukukunda Bilişim Suçları, Ankara, 2008.

Koca Mahmut, "Hukukumuzda TCK'nın 244. Maddesi Kapsamında Bilişim Sistemini Engelleme, Bozma, Verileri Yok Etme veya Değiştirme Suçu" , Yargıtay Bilişim Hukuku Konferansı, 09-10 Ekim, 2008.

Kurt Levent, Açıklamalı-İçtihatlı Tüm Yönleriyle Bilişim Suçları ve Türk Ceza Kanunundaki Uygulaması, Ankara, 2005.

Lale Muktedir, "İnternet Bankacılığında Hukuki Sorumluluk", Terazi Hukuk Dergisi, S. 42, Şubat 2010.

Özbek Veli Özer/**Kanbur** M. Nihat/ **Bacaksız** Pınar/**Doğan** Koray/ **Tepe** İlker, Türk Ceza Hukuku Genel Hükümler, Ankara, 2010.

Özbek Veli Özer/**Kanbur** M. Nihat/**Doğan** Koray/**Bacaksız** Pınar/**Tepe** İlker, Türk Ceza Hukuku Özel Hükümler, Ankara, 2010.

Özdamar Naci, "İnternet Bankacılığı ve Banka Kartları", Bilişim ve Hukuk, Ankara Barosu Uluslar arası Hukuk Kurultayı, C. II, 2008.

Taşkın Şaban Cankat, Bilişim Suçları, İstanbul, 2008.

Türkiye Bankalar Birliği İnternet Bankacılığı İstatistikleri, Aralık 2009.

Yazıcıoğlu Yılmaz, "Yeni Türk Ceza Kanunundaki Suçların Genel Değerlendirmesi", Yeditepe ÜHFD, S. 2, 2005, C. II.

Yılmaz Süleyman, "Hukuki Açıdan İnternet Bankacılığı", Ankara Üniversitesi Sosyal Bilimler Enstitüsü Doktora Tezi, Ankara, 2007.

Zevkliler Aydın / Aydoğdu Murat; Tüketicinin Korunması Hukuku, Ankara, 2004.

CamScanner ile tarandı