5237 SAYILI TCK'NIN 244. MADDESİNDE DÜZENLENEN BİLİŞİM ALANINDAKİ SUÇLAR

OFFENCES AGAINST INFORMATION SYSTEMS PRESCRIBED UNDER ARTICLE 244 OF THE TURKISH CRIMINAL CODE

Sacit YILMAZ*

Özet: Bilişim teknolojileri eğitimden ticarete, ulaşımdan iletişime, kamu hizmetlerinden özel sektöre kadar hayatın hemen her alanında köklü değişiklikler yapmıştır. Bilişim teknolojilerinin bu olumlu yönlerine karşı, kötüye kullanılması da kaçınılmazdır. Bu sebeple pek çok ülke bilişim alanında yasal düzenlemelere gitmiş, mevzuatlarını teknolojinin gerektirdiği biçimde değiştirme çabasına girmişlerdir.

Mukayeseli hukuktaki son gelişmelere paralel olarak, Yeni Türk Ceza Kanunu'nda Bilişim Suçları bölümünde TCK'nın 244. maddesi ile bilişim sistemini engelleme, bozma, verileri yok etme veya değiştirme suçu kabul edilmiştir. Makalede TCK'nın 244. maddesi tüm yönleriyle açıklanmaya çalışılacaktır.

Anahtar Sözcükler: Bilişim, sistem, veri, suç, yok etme, engelleme, sözleşme, zarar, yasa.

Abstract: Having made fundamental changes in all areas, such as education, trade, transportation, communication, public service, private sector, information technology, has affected our lives seriously. Besides its positive impacts, it is inevitable that it can be abused. Consequently, many states have enacted new laws on information technology and have made efforts for amendments in their legislation.

In line with the recent developments in comparative law, blocking, breaking of an information system, and deleting or altering of data was enacted as a crime in article 244 of the Turkish Criminal Code. In this essay article 244 will be explained in detail.

Keywords: Information, system, data, crime, delete, block, act, damage, law.

* Dr., Yargıtay Cumhuriyet Savcısı.

I. Bilişim Sistemini Engelleme, Bozma, Verileri Yok Etme veya Değiştirme Suçu

a. Giriş

Bilişim kelimesi; "*insanların teknik, ekonomik ve toplumsal alanlardaki iletişimde kullandığı ve bilimin dayanağı olan bilginin, özellikle elektronik makineler aracılığıyla düzenli ve akılcı biçimde işlenmesi, bilginin elektronik cihazlarda toplanması ve işlenmesi bilimi*" olarak açıklanmaktadır.[1]

Bilişim; bilginin aktarılması, organize edilmesi, saklanması, tekrar elde edilmesi, değerlendirilmesi ve dağıtımı için gerekli kuram ve yöntemlerdir. Bilişim sistemi ise, 5237 sayılı TCK'nın 243. maddesinin gerekçesinde; verileri toplayıp yerleştirdikten sonra bunları otomatik işlemlere tâbi tutma olanağını veren manyetik sistemler olarak tanımlanmıştır.[2] Avrupa Konseyi Siber Suç Sözleşmesi'nin "*Tanımlar*" başlıklı birinci maddesine göre ise bilişim sistemi; bir veya birçok unsuru, bir programın işleyişi aracılığıyla verilerin otomatik olarak işleme tabi tutulmasını sağlayan, birbirine bağlanmış veya benzeşen tek veya toplu tertibatı ifade etmektedir.[3]

Bilişim sistemlerinin en yaygın unsuru, verilerin saklanması, işlenmesi ve aktarılmasını sağlaması bakımından bilgisayarlardır. Ancak bilgisayarlar dışında da, bilişim sistemi olarak nitelendirilebilecek aygıtlar mevcuttur. Bu itibarla, bilişim suçu olarak isimlendirilen fiiller, bir bilgisayarda ya da bilgisayar olarak nitelendirilmemesine rağmen, veri iletişimi sağladığı için bilişim alanına dahil unsurlardan sayılması gereken diğer elektronik, manyetik, mekanik araçlar üzerinde (örneğin, WAP uyumlu, girilen verileri saklayabilen, işleyebilen, aktarabilen cep telefonları ile üzerindeki WEB paneli sayesinde ağa bağlanıp veri aktarımı yapabilen elektronik ev aletleri) veya bunları veri iletişimi için birbirine bağlayan soyut veya somut ağlar üzerinde işlenebilir.[4]

---

1 Cevat Özel, Bilişim-İnternet Suçları, http://www.hukukcu.com/bilimsel/kitaplar/bilisim_internetsucları.html, s. 1 Kontrol Tarihi: 16.11.2010; Berrin Bozdoğan Akbulut, "Bilişim Suçları", *Selçuk Üniversitesi Hukuk Fakültesi Dergisi*, C. 8, S. 1-2, Y. 2000, s. 546.

2 www.ceza-bb.adalet.gov.tr/mevzuat/maddegerekce.doc Kont. Tarihi: 16.08.2010.

3 Yeşim Atamer, İnternet ve Hukuk, *İstanbul Bilgi Üniversitesi Yayınları*, İstanbul, 2004, s. 703.

4 Caner Yenidünya, "Bilişim Sistemine Hukuka Aykırı Erişim Suçu", *Legal Fikri ve*

Bilişim teknolojilerinin eğitimden ticarete, ulaşımdan iletişime, kamu hizmetlerinden özel sektöre kadar hemen her alanda köklü değişiklikler yaparak, hayatı ciddi anlamda etkiler hale gelmesi, bilişim teknolojilerinin kanunları ihlal etme fırsatı veren ve ortaya yeni suç fiilleri çıkartan bir etkiye sahip olmasını da beraberinde getirmiştir.[5] Bu sebeple, özellikle bu teknolojilerin kaynağını oluşturan ülkeler başta olmak üzere, pek çok devlet bilişim alanında yasal düzenlemelere gitmiş, mevzuatlarını teknolojinin gerektirdiği biçimde değiştirme çabasına girmişlerdir.[6]

Bilişim alanındaki suçların düzenlenmesi bakımından mukayeseli hukuka bakıldığında iki temel sistemin uygulandığı görülmektedir: Kanun koyucular bu alandaki suçları karşılamak için mevzuatlarında ya ayrı özel bir kanun yapmakta, ya da mevcut ceza kanunları içinde düzenleme gerçekleştirmektedirler.[7] Yeni Türk Ceza Kanunu'nda ise, bu alandaki suçlar hem *"Bilişim Alanında Suçlar"* adı altında bir bölümde düzenlenmiş, hem de hırsızlık, dolandırıcılık gibi suçlar içerisinde yer almışlardır.

Mukayeseli hukuktan bahsetmişken birkaç örnek vermek konunun öneminin anlaşılması bakımından yerinde olacaktır. Avrupa Siber Suçlar Sözleşmesi'nin 2 ila 10. maddeleri arasında suç olarak tanımlanan fiiller sıralanırken, Sözleşme'nin 4 ve 5. maddeleri konumuzla ilgilidir. Şöyle ki, Sözleşme'nin dördüncü maddesinde, kasten ve haksız olarak, bilgisayar verilerini tahrip etme, silme, bozma, değiştirme veya erişilmez kılma suç olarak tanımlanmış; Sözleşme'nin 5. maddesinde ise, bilgisayar verilerine yeni veriler girmek, bunları başka yerle-

---

Sınaî Haklar Dergisi, İstanbul, Nisan 2005, s. 758.

5 Akbulut, a. g. m., s. 547; Ümit Kardaş, "Bilişim Dünyası ve Hukuk", *Karizma Dergisi*, S. 13, Y. 2003, s. 7, Yüksel Ersoy, "Genel Hukuki Koruma Çerçevesinde Bilişim Suçları", *Ankara Üniversitesi Siyasal Bilgiler Fakültesi*, C. 49, S. 3-4, Haziran 1994, s. 152, Olgun Değirmenci, "Bilişim Suçları Alanında Yapılan Çalışmalar ve Bu Suçların Mukayeseli Hukukta Düzenlenişi", *Legal Hukuk Dergisi*, S. 11, Kasım 2003, s. 2750

6 Hatice Akıncı/A.Emre Alıç/Cüneyd Er, "Türk Ceza Kanunu ve Bilişim Suçları", İnternet ve Hukuk, *İstanbul Bilgi Üniversitesi Yay,* Ocak 2004, İstanbul, s. 158

7 Ayhan Önder, *Şahıslara ve Mala Karşı Cürümler ve Bilişim Alanında Suçlar*, Filiz Kitabevi, İstanbul, 1994, s. 505; R.Yılmaz Yazıcıoğlu, "Yeni Türk Ceza Kanunundaki Bilişim Suçlarının Genel Değerlendirilmesi", *Yeditepe Üniversitesi Hukuk Fakültesi Dergisi*, C. 2, S. 2, Y. 2005, s. 396

re iletmek, tahrip etmek, silmek, bozmak, değiştirmek ve erişilmez kılmak suretiyle, kasten ve haksız olarak, bir bilgisayar sisteminin işleyişini ciddi olarak engellemek suç olarak tanımlanmıştır.[8]

ABD'de, Federal Ceza Kanunu'nun 1030. maddesinde, ABD hükümetine zarar vermek veya başka bir ülkeye yarar sağlamak amacıyla savunma ve dışişlerine ait tasnif edilmiş ve gizlilik dereceli bilgiye izinsiz olarak erişmek, finansal bir kurumun finans kayıtlarına veya tüketici bilgilerine ulaşmak veya bunları kullanmak amacıyla bir bilgisayara hukuka aykırı olarak girmek cezalandırılan bir fiil olarak düzenlenmiştir. Ayrıca devlet kurum veya teşkilatlarınca veya hükümet tarafından kullanılan bir bilgisayara yetkisiz erişmek de suçtur.[9]

İtalya'da bilişim suçları alanındaki son yasal düzenleme 23 Aralık 1993 tarihinde 547 sayılı Kanun ile yapılmıştır. İtalyan Ceza Kanunu'nda bilişim veya telematik sistemine hukuka aykırı girme veya hak sahibinin açık veya rızası hilafına sistemde kalmaya devam etme fiilleri 615ter maddesinde suç olarak düzenlenmiştir. Düzenleme ile hüküm altına alınan sistemler; güvenlik tedbirleri ile koruma altına alınan bilişim veya telematik sistemleridir. Bilişim veya telematik sistemlerinin kullanıcısı; bilimsel veya fiziksel koruma araçlarını hazırlamak suretiyle sisteme girme ve sistemde kalmayı yalnızca kendisi tarafından yetkili kılınan kişilere bırakmak istediğini açıkça bildirmek zorundadır. Güvenlik sistemleriyle korunan bilişim veya telematik sistemlerine erişim kodlarının herhangi bir surette hukuka aykırı olarak elde etme ve yayma fiili, 615quarter maddesinde bilişim suçu olarak yer almaktadır. Suçun oluşabilmesi için özel kast aranmaktadır; bu kast, kendisine veya başkalarına yarar sağlamak veya başkalarına zarar vermek amacına yöneliktir. 615quinques maddesi ile kendisi veya başkası tarafından yazılarak bir bilişim veya telematik sistemine, içinde saklanan verilere veya programlara zarar verme veya sistemin işleyişini tamamen veya kısmen engelleme veya bozma amaçla-

---

8 http//www.conventions. coe.int, Kontrol Tarihi: 16.08.2010.

9 Hüseyin Çeken, "Amerika Birleşik Devletlerinde İnternet Yolu İle İşlenen Suçlara İlişkin Düzenlemeler", *Askeri Adalet Dergisi*, Yıl: 30, Sayı: 114, Mayıs 2002, s. 75; Schjolberg, Stein, The Legal Framework - Unauthorızed Access To Computer Systems, http//www.mosstingrett.no/info/legal.html Kontrol Tarihi: 17.08.2010

narak veya bunları sonuç olarak gerçekleştirerek bilişim programını bildiren veya veren kişinin fiilinin cezalandırılacağı belirtilmektedir.[10]

Alman Ceza Kanunu'nun 202a maddesinde verilerin depolandığı ve işlendiği bilişim sistemleri ağına girmek ve burada bulunan verileri ele geçirmek suçu düzenlenmiştir. Alman Ceza Kanunu hukuka aykırı olarak bilişim sistemlerine girmeyi suç oluşumu için yeterli görmemekte, verilerin ele geçirilmesi koşulunu da aramaktadır. Fiil; kendisi veya üçüncü bir kişi yararına, kendisine ait olmayan, başkalarının girişine açık bulunmayan ve emniyete alınmış verilerin yetkisiz olarak ele geçirilmesi durumunda suç haline gelmektedir.[11]

İngiltere'de bilişim suçları, 29 Ağustos 1990 tarihinde yürürlüğe giren 29 Haziran 1990 tarihli "*Computer Misuse Act*'' düzenleme altına alınmış; 3 bölüm ve 18 kısımdan oluşan "*Computer Misuse Act*''ta, bilgisayardaki program veya verilere yetkisiz olarak girilmesi, başka suçların işlenmesini kolaylaştırmak veya yardımcı olmak amacıyla bilgisayarlara yetkisiz olarak erişim ve bilgisayarlarda saklı tutulan program veya verilerin yetkisiz olarak değiştirilmesi fiilleri suç olarak düzenlenmiştir.[12]

Mukayeseli hukuktaki gelişmelere paralel olarak, Yeni Türk Ceza Kanunu'nda da "*Bilişim Alanında Suçlar*" bölümünde, TCK 244. madde ile bilişim sistemini engelleme, bozma, verileri yok etme veya değiştirme suçu kabul edilmiştir.

b. Suçla Korunan Hukuki Değer

5237 sayılı TCK'nin 244. maddesinde, sisteme ve veriye müdahale iki fıkra halinde düzenlenmiş, maddenin birinci fıkrasında sistemin işleyişine müdahale, ikinci fıkrasında ise sistem içerisindeki veriye yönelik fiiller düzenlenmiştir. TCK 244. maddenin 1. ve 2. fıkralarındaki suçlarla korunan hukuki değer konusunda görüş birliği bulunma-

---

[10] Carlo Sarzana, "Bilişim Alanındaki Yeni Teknolojilerin Hukuksal Yansıması İtalya'daki Durum", *İstanbul Hukuk Fakültesi Dergisi*, *Prof. Dr. Türkan Rado'ya Armağan*, İstanbul 1997, C.LV, S. 3, s. 399.

[11] Önder, *a. g. e.*, s. 505.

[12] Olgun Değirmenci, *Bilişim Suçları*, Marmara Üniversitesi Sosyal Bilimler Enstitüsü yayınlanmamış yüksek lisans tezi, İstanbul, 2002, s. 158.

maktadır. Bir görüşe göre, burada korunan hukuki değer karma niteliktedir ve bilişim sistemi ve/veya bilişim sisteminin içerdiği veriler üzerinde tasarruf yetkisi bulunan kişinin, verilerle oluşturulan yazılım, ekonomik bilgiler, bilimsel çalışma, bilgi vb. gibi değerlere herhangi bir engel, arıza ya da gecikme olmadan ulaşması ve kullanmasındaki çıkarıdır.[13]

Diğer bir görüşe göre, genel olarak TCK 244. maddede, bilişim sisteminin ve bu sistem içerisindeki verilerin dokunulmazlığı korunan hukuki değerdir. 1. fıkrada, bilişim sistemi sahibinin mülkiyet hakkı, zilyedinin bilişim sisteminin dokunulmazlığı, iletişim kurma, teknolojik gelişim özgürlüğü korunmaktadır. 2. fıkrada ise, bazen mülkiyet hakkı, bazen de verilerin içeriğine göre fikri mülkiyet hakkı, özel hayatın gizliliği, ticari sırlar korunmaktadır.[14]

Bir başka görüş, TCK 244. maddenin 1. ve 2. fıkralarında korunan hukuki değerin, madde gerekçesinde de belirtildiği üzere, sistemlere yöneltilen ızrar fiillerini özel bir suç haline getirme düşüncesiyle bağlantılıdır. Aslında burada hem bilişim sisteminin ve hem de bu sistem içerisinde yer alan veriler veya diğer unsurların zarar görmemesi amaçlanmaktadır.[15]

Düzenlemenin karşılığı olan 765 sayılı TCK'nin 525/b 1. fıkrasında yer alan sisteme ve veriye zarar verme suçu ile ilgili olarak Sulhi Dönmezer, bu maddede düzenlenen fiiller ile sisteme ve içeriğine karşı mala zarar verme fiillerinin işlendiğini ifade etmiştir.[16] Yılmaz Yazıcıoğlu da bu suçun klasik mala zarar verme suçunun özel bir sekli olduğunu, bu suçun sistem ve içeriğini esas alan mala zarar verme fiillerini kapsadığını ifade etmiştir.[17]

Ayhan Önder suçun koruduğu yararın tartışmalı olduğunu, bazı yazarların bu suç tipi ile bilgisayarda mevcut veriler ile ilgili olan kişi-

---

13 Murat Volkan Dülger, *Bilişim Suçları*, Seçkin Yay, Ankara, 2004, s. 231.

14 Levent Kurt, *Bilişim Suçları ve Türk Ceza Kanunundaki Uygulaması*, Seçkin Yay, Ankara 2005, s. 162.

15 Ali Karagülmez, *Bilişim Suçları ve Soruşturma-Kovuşturma Evreleri*, Seçkin Yay, Ankara, 2005. s. 186.

16 Sulhi Dönmezer, *Kişilere ve Mala Karşı Cürümler*, Beta Yayıncılık, İstanbul, Ekim 2004.

17 R.Yılmaz Yazıcıoğlu, *Bilgisayar Suçları*, Alfa Yay, İstanbul, 1997, s. 259.

nin yararının korunduğunu, bazı yazarların ise mevcut verilerin ülke ekonomisinde ve idarede gerçekleştirildiği fonksiyon gereği, bu suçun ekonomik yaşama karşı işlenmiş bir suç olduğunu ifade ettiklerini belirtmiştir.[18] Yüksel Ersoy ise bu suç ile kişinin malvarlığının korunduğunu belirtmiştir.[19]

TCK'nın gerekçesi incelendiğinde, sisteme ve veriye yönelik müdahale fiillerinin, mala zarar verme suçuna göre özel bir düzenlemeye tabi tutulduğunun belirtildiği görülmektedir. Nitekim sisteme ve veriye müdahale ile ilgili olarak madde gerekçesinde "*...sistemlere yöneltilen ızrar fülleri özel bir suç hâline getirilmiştir. Aracın fizik varlığı ve işlemesini sağlayan bütün diğer unsurları, söz konusu suçun konusunu oluşturmaktadır. Fıkrada seçimlik hareketli bir suç meydana getirilmiştir*" denmektedir.[20]

Aktarılan bu hususlar incelendiğinde 5237 sayılı TCK ve 765 sayılı TCK bakımından, sistem ve veriye müdahalenin genel olarak mala zarar verme suçu kapsamında değerlendirildiği ve genel olarak 765 sayılı Kanun'un 525/b 1. fıkrasında ve TCK'nın 244/1-2. fıkralarında düzenlenen sistem ve veriye müdahalenin mala zarar vermenin özel bir şekli olarak kabul gördüğü görülmektedir.[21]

Madde gerekçesi ve doktrindeki görüşler doğrultusunda, kanaatimizce bu suçun hukuki konusu, mala zarar verme suçunun hukuki konusuyla örtüştüğü yönündedir. Bilindiği üzere mala zarar verme suçunda korunan hukuki değer, iktisaptan farklı olarak, kullanılırlık veya yararlılık değerini azaltan, yok eden fiillere karşı, mülkiyeti korumaya ilişkin toplumsal menfaattir.[22] Yapılan düzenleme ile bilişim sistemi veya verileri üzerinde sahibi veya zilyedinin her türlü mülkiyet hakkı ve buna bağlı olarak toplum menfaati korunmak istenmiştir.

---

18 Önder, *a. g. e.*, s. 508.

19 Ersoy, *a. g. e.*, s. 166.

20 www.ceza-bb.adalet.gov.tr/mevzuat/maddegerekce.doc Kontrol Tarihi: 17.08.2010.

21 Muammer Ketizmen, *Türk Ceza Hukukunda Bilişim Suçları*, Adalet Yay, Ankara, 2008, s. 128.

22 Zeki Hafızoğulları /Muharrem Özen, *Türk Ceza Hukuku Özel Hükümler Kişilere Karşı Suçlar*, Usa Yay, Ankara, 2010, s. 342; Nevzat Toroslu, *Ceza Hukuku Özel Kısım*, Savaş Yay, Ankara, 2009, s. 155; Sulhi Dönmezer, *Kişilere ve Mala Karşı Cürümler*, Filiz Kitabevi, 12. Baskı, s. 474.

Kanun sistematiği bakımından, suçla korunan hukuki değerin mala zarar verme suçu ile aynı amaca hizmet ettiği gözetildiğinde, şu husus önemli bir eksiklik olarak ortaya çıkmaktadır. Şöyle ki, mala zarar verme suçu Ceza Kanunu'nun İkinci Kısım Onuncu Bölüm'ünde yer alırken; TCK'nın 244 maddesi Üçüncü Kısım Onuncu Bölüm'de yer almaktadır. Mala zarar verme suçunu işleyenler, aynı bölüm içerisinde yer alan TCK 167 maddesinde yazılı şahsi cezasızlık sebepleri ile TCK'nın 168 maddesinde yazılı etkin pişmanlık hükümlerinden yararlanma olanağına sahiptir.

Bilindiği üzere, TCK, 167. maddesinde bu bölümde yer alan suçların; haklarında ayrılık kararı verilmemiş eşlerden birinin; üstsoy veya altsoyunun veya bu derecede kayın hısımlarından birinin veya evlat edinen veya evlâtlığın; aynı konutta beraber yaşayan kardeşlerden birinin zararına olarak işlenmesi hâlinde, ilgili akraba hakkında cezaya hükmolunmayacağı; ayrıca, haklarında ayrılık kararı verilmiş olan eşlerden birinin, aynı konutta beraber yaşamayan kardeşlerden birinin, aynı konutta beraber yaşamakta olan amca, dayı, hala, teyze, yeğen veya ikinci derecede kayın hısımlarının zararına olarak işlenmesi hâlinde cezada indirime gidileceği belirtilmiştir.

TCK'nın 168. maddesinde, hırsızlık, mala zarar verme, güveni kötüye kullanma, dolandırıcılık, hileli iflâs, taksirli iflâs ve karşılıksız yararlanma suçları tamamlandıktan sonra ve fakat bu nedenle hakkında kovuşturma başlamadan önce veya sonra, failin, azmettirenin veya yardım edenin bizzat pişmanlık göstererek mağdurun uğradığı zararı aynen geri verme veya tazmin suretiyle tamamen gidermesi halinde cezada indirime gidileceği kabul edilmiştir.

Mala zarar verme suçu ile aynı hukuki değeri koruyan TCK'nın 244. maddesi, kanun sistematiğinde İkinci Kısım Onuncu Bölüm'de yer alsa idi, TCK'nın 244. maddesinde yazılı suçu işleyenler yukarıda yazılı yasal olanaklardan yararlanabilecekti. Benzer bir eleştiri TCK'nın 245. maddesi için de geçerli idi. Ancak 5377 sayılı Kanun'un 27. maddesi ve 5360 sayılı Kanun'un 11. maddesi ile bu eksiklikler giderilerek, TCK'nın 245. maddesi için faile etkin pişmanlık ve şahsi cezasızlık sebeplerinden yararlanma olanağı getirilmiştir. Kanaatimizce benzer bir düzenlemenin TCK'nın 244. maddesi için de yürürlüğe konması gereklidir.

c. Maddi Unsurlar

c.1. Suçun Fail ve Mağduru

Kanun maddesinde bir özellik belirtilmediğinden herkes bu suçun faili olabilir. Suçta failin belirlenebilmesi için, suçun bilişim sisteminin hangi unsuruna yöneldiğinin tespit edilmesi gerekmektedir. Fiil eğer bilişim sisteminin kendisine yöneltilmişse, sistemin kendisi üzerinde; verilere yöneltilmişse veriler üzerinde; hem bilişim sistemine hem de verilere yöneltilmişse her ikisinin de üzerinde kullanım, mülkiyet ve tasarruf yetkisinin kimde olduğunun ortaya konması gereklidir.[23] Yargıtay kararları da bu yöndedir.[24]

Madde metninde mağdur bakımından da bir özellik öngörülmemiştir. Herkesin mağdur olabilmesi mümkündür. Dolayısıyla, söz konusu suçun oluşmasına yol açan eylemler nedeniyle, bilişim sistemindeki verilere ulaşamayan, geç ulaşan ya da sistemi kullanamayan ve sistem üzerinde tasarruf yetkisi bulunan kimse, çıkarları zedelendiği için suçun mağduru olacaktır.

c.2. Suçun Konusu

Bilişim sisteminin işleyişinin engellenmesi, bozulması, verilerin yok edilmesi veya değiştirilmesi suçunun konusunu, bilişim sistemleri ve verileri oluşturmaktadır. Bilişim sistemi, Avrupa Konseyi Siber Suç Sözleşmesi'nin *"Tanımlar"* başlıklı birinci maddesine göre, bir veya birçok unsuru, bir programın işleyişi aracılığıyla verilerin otomatik olarak işleme tabi tutulmasını sağlayan, birbirine bağlanmış veya benzeşen tek veya toplu tertibatı ifade etmektedir.[25] Türk Ceza Kanunu'nun

---

23 Dülger, *a. g. e.,* s. 232.

24 Yarg. 11.CD, 28.01.2009 gün, 2008/16570 Esas, 2009/101 Karar: Sanığın savunması ve tüm dosya kapsamı dikkate alındığında, dosyada mevcut Türk Telekomünikasyon A.Ş.'nin yazısından hesaplara gelen paraların internette 85.97.000.000 IP numarası kullanılarak aktarıldığının anlaşılması karşısında, bu numaranın kullanım bilgileri istenerek EFT'nin yapıldığı anda anılan numaranın bu şirket tarafından hangi kullanıcıya atandığının ilgili kurumdan araştırılıp tespit edildiğinde sanık ile irtibatı olup olmadığının saptanması gerektiğinin gözetilmemesi sonucu eksik soruşturmaya dayanarak yazılı şekilde hüküm kurulması nedeniyle hükmün bozulması.

25 Atamer, a. g. m., s. 703

243. maddesinin gerekçesinde bilişim sistemi, verileri toplayıp yerleştirdikten sonra bunları otomatik işlemlere tabi tutma olanağını veren manyetik sistemler şeklinde tanımlanmıştır.

Veri ise, depolamak, işlemek ve kullanmak üzere kurulmuş bir bilişim sisteminin üzerinde işlev gerçekleştirdiği temel unsurdur. Madde, bilişim sisteminin işleyişinde ve verilerde meydana getirilen zararları cezalandırmaktır.

c.3. Hareket

c.3.1. Genel Olarak

5237 sayılı TCK'nın 244/1-2. fıkralarındaki suçlar, 765 sayılı TCK'nın 525/b.1 maddesinde düzenlenen suç ile örtüşmektedir.[26] 5237 sayılı TCK'nın 244. maddesinde, sisteme ve veriye müdahale iki fıkra halinde düzenlenmiş, maddenin birinci fıkrasında sistemin işleyişine müdahale, ikinci fıkrasında ise sistem içerisindeki veriye yönelik fiiller düzenlenmiştir. 765 sayılı TCK'nın 525/b maddesinden farklı olarak, sisteme ve veriye müdahale fiilleri için farklı cezalar öngörülmüştür. Bu açıdan sistemin isleyişinin engellenmesi ve bozulması, daha ağır cezayı gerektiren fiiller olarak ele alınmıştır.

Maddenin üçüncü fıkrasında, birinci ve ikinci fıkrada düzenlenen fiillerin banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinde işlenmesi hali ağırlatıcı neden olarak düzenlenmiştir.[27] Maddenin son fıkrasında, birinci ve ikinci fıkralarda tanımlanan fiillerin işlenmesi suretiyle kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlamasının başka bir suç oluşturmaması hâlinde cezalandırılması kabul edilmiştir.

c.3.2. Sistemin İşleyişini Engelleme ve Bozma

Bilişim sisteminin işlemesini engellemek, sistemin geçici veya sürekli olarak çalışmasının herhangi bir şekilde kesintiye uğratılmasıdır.[28]

---

26 Dülger, *a. g. e.*, s. 251.

27 Ketizmen, *a. g. e.*, s. 118.

28 R. Yılmaz Yazıcıoğlu, Bilişim Suçları Konusunda 2001 Türk Ceza Kanunu Tasarı-

Burada sistemin işleyişi bozulmamakta, fakat işlemesi bir şekilde engellenmektedir. Yasa koyucu bu ifade ile kavramı çok geniş tutarak ve nasıl olduğu aramaksızın, sistemin işleyişini bozmak dışında, sistemin işlemesini engelleyen her türlü eylemi buraya dahil etmiştir. Bilişim sisteminin işlemesine sürekli veya geçici olarak engel olunması suçun oluşması açısından önem taşımamaktadır. 5237 sayılı TCK'nın 244/1. maddesi gereğince her iki durumda da bu suç işlenmiş olacaktır.

Bilişim sisteminin işleyişinin engellenmesi halinde, sistemin bozulması söz konusu olmayıp, sistemin normalde yerine getirdiği fonksiyonlarını ifa etmesi engellenmektedir. Örneğin, sistem eskisi kadar hızlı çalışmamakta, veri alışverişi yapamamakta, çeşitli programları hiç veya gereği gibi çalıştıramamakta, kısacası normal şartlarda yerine getirebildiği işlevlerini gereği gibi yerine getirememektedir. Sistem bozulmuş olmasa da, fail bir kısım eylemlerle işleyişi engellemektedir.[29]

Bilişim sisteminin bozulması halinde ise, sistemin tamamen çalışamaz hale gelmesi söz konusudur. Çalışamaz hale getirilmesi; sistemin çökertilmesi, program akışının bozulması, virüsler vasıtasıyla sistem yazılımlarının işlemez hale getirilmesi şekillerinde gerçekleştirilebilir. Bozulmada tamamıyla devre dışı bırakılma söz konusudur. Bilişim sisteminin işleyişinin bozulmasının ne şekilde gerçekleştiği suç açısından önem arz etmemektedir.

c.3.3. Sistemdeki Verileri Bozma, Yok Etme, Değiştirme, Verileri Başka Yere Gönderme

Konuyu açmadan önce maddede belirtilen veri kavramını tanımlamak gerekmektedir. Avrupa Siber Suç Sözleşmesi'nde veri, belirli durumların, bilgilerin kaydı ya da bir bilgisayarın bir işlemi gerçekleştirmesini sağlayacak biçimleri de içeren bilgisayar sistemince icra edilebilecek bir işlemler bütünü olarak tanımlanmıştır. Belirli konulardaki gerçeklerin sembolik ifadesi olan veri, bilgisayara girilen işlenmemiş durumdaki bilgileri ifade eder.[30] Veri, programlar gibi sistemin so-

sının Değerlendirilmesi, *Hukuk ve Adalet: Eleştirel Hukuk Dergisi*, İstanbul, Y. 1, S. 1, Ocak-Mart 2004, s. 179.

29 Kurt, *a. g. e.*, s. 164.

30 Hasan Çebi Bal, *Bilgisayar ve İnternet*, Akademi Yayınevi, Rize, 2001, s. 29.

yut yanına ilişkindir ve bir yandan sistemin istenilen doğrultuda çalışmasını sağlayan programları oluşturan temel birim, bir yandan da sistemin varlık nedenidir. Diğer bir ifadeyle veri, depolamak, işlemek ve kullanmak üzere kurulmuş bir bilişim sisteminin üzerinde işlev gerçekleştirdiği temel unsurdur.[31]

Maddede yer alan seçimlik hareketlerden ilki, bilişim sistemi içerisindeki verinin yok edilmesidir. Bilişim sistemi içerisindeki verinin yok edilmesi, verinin varlığına son verilmesi, ortadan kaldırılması, hak sahibinin tekrar elde edemeyeceği ya da büyük güçlükler sonucu elde edebileceği şekilde tasarrufundan çıkarılması olarak tanımlanabilir.

Bilişim sistemlerinde iki tip yok etme şekli vardır. Birinci işlemde verilerin depolama üzerindeki varlığına tamamen son verilerek, o veriye ilişkin hiçbir iz depolama ünitesi üzerinde bırakılmamakta; ikinci tip yok etme işleminde ise, veriler depolama ünitesi üzerinden silinmemekte, sadece o verilere erişimi sağlayan anahtar veriler silinmektedir. Bu durumda, işletim sistemi o verilere ulaşamamaktadır. Veriler fiziksel olarak silinmediği için özel işlemler aracılığı ile silinmiş gözüken veriler tekrar kurtarılabilir. Depolama ünitesinden fiziksel olarak silinmiş olan veriler ise asla kurtarılamaz. Kanun koyucunun verilerin yok edilmesinden kastı, verilerin her iki tip yok etme işleminden her hangi birisine maruz kalmasıdır.

Maddede yer alan diğer seçimlik hareket, bilişim sisteminin içindeki verinin bozulmasıdır. Verinin bozulması verinin içeriğine ya da yapısına müdahale suretiyle verinin kısmen ya da tamamen kullanılamayacak hale gelmesi olarak tanımlanabilir.[32] Burada özellikle verinin içeriğine müdahalenin, var olan verinin içerdiği bilgi ya da enformasyona olumsuz müdahaleyi kapsadığını belirtmek gerekir. Verinin yok edilmesinden farklı olarak burada, verinin tasarruf alanından çıkartılmaması ya da ortadan kaldırılmaması söz konusudur.[33]

---

31 Yazıcıoğlu, *a. g. e.,* s. 227; Mustafa Topaloğlu, *Bilişim Hukuku,* Karahan Kitabevi, Adana 2005, s. 67.

32 Necati Meran, *Sahtecilik, Malvarlığı, Bilişim Suçları*, Seçkin Yay, Ankara 2005, s. 372.

33 Ketizmen, *a. g. e.,* s. 139.

Bir diğer seçimlik hareket olan verilerin değiştirilmesi durumunda, bir verinin bir başka veriyle değiştirilmesi veya verilerin orijinal halinden başka bir hale dönüştürülmesi söz konusudur. Suçun oluşumu açısından failin amacının önemi bulunmamaktadır. Bir bilişim sisteminde bulunan dosyaların ya da resimlerin bir başkasıyla değiştirilmesi de bu suç tipine girmektedir. Verilerin değiştirilmesinde amaç, veriyi yok etmek veya erişilmez kılmak demek değil, veriye ulaşıldığında yanlış bilgilere erişilmesini sağlamaktır. Bu nedenle veri değiştirildiğinde sistem işleyişine devam etmektedir. Virüs, truva atı gibi kötü amaçlı kodların sisteme sokulması ve bu nedenle verilerin farklı bir hale gelmesi de verilerin değiştirilmesi başlığı altında düşünülmelidir.[34]

Maddede yazılı bir diğer seçimlik hareket olan verilerin erişilmez kılınması, verilerin malikinin ya da ilgilisinin istediği zaman, istediği verilere ulaşmasının engellenmesi anlamına gelmektedir. Bu durumda veriler yok edilmemekte, tahrif edilmemekte sadece sahibinin erişimi engellenmektedir. Veriye erişilmesi bakımından erişimin engellenmesinin geçici veya daimi olması arasında fark yoktur.[35]

Son seçimlik hareket olarak kabul edilen sistem içerisindeki verinin başka bir yere gönderilmesi, bilişim sisteminde yer alan verilerin, sahibinin ya da ilgilisinin izni olmaksızın orijinal konumundan başka bir yere aktarılması, taşınması, gönderilmesi, kaydedilmesi ya da kopyalanması fiilidir.[36] Verilerin gönderilmesi fiili, bir bilişim ağı üzerinden gerçekleştirilebileceği gibi, bir veri depolama aracı ile sistemden verilerin kopyalanarak taşınması şeklinde de gerçekleşebilir. Verilerin gönderilmesi fiili genellikle internet üzerinde sisteme yerleştirilen *"Truva atı"*, *"key logger"* ve *"virüsler"* gibi bir takım küçük programcıklar aracılığıyla gerçekleşmektedir. Bu tür programlar aracılığı ile faile çeşitli kullanıcı adları ve parolalar veya sisteme ilişkin veriler gönderilmekte ve sistem hakkında failin bilgilendirilmesi sağlanmaktadır. Verilerin nereye kopyalandığının önemi bulunmamaktadır. Eylem, ticari verilerin, askeri verilerin veya kamuya ait gizli verilerin, bir başka

---

34 Umut Eker, "Türk Ceza Hukuku'nda Bilişim Suçları", *Türkiye Barolar Birliği Dergisi*, S: 62, Ocak-Şubat 2006, Ankara, s. 124.

35 Dülger, *a. g. e.*, s. 237.

36 Eker, a. g. m., s. 125.

sisteme gönderilmesi gibi failin işine yarayabilecek veriler hakkında gerçekleşebileceği gibi, failin işine yaramayan verilerin transferi veya gönderilmesi şeklinde de gerçekleştirilebilir.[37]

Suçun maddi unsurları anlatılırken, suçun işlenme şekillerine de değinmek gerekecektir. Çünkü bilişim suçlarını, klasik suçlardan ayıran özellik, bu suçların maddi hareketinin tespitinin zorluğudur. Suçun işlenmesinden sonra arkada herhangi bir iz bırakılmaması ve çok kısa bir zaman dilimi içerisinde suçun gerçekleşmesi bu zorluğu doğurmaktadır. Teknolojik gelişmeler sayesinde, bilinen suç işleme yöntemlerinin yerine daha farklı yöntemler kurgulanabilmektedir. Konunun anlaşılması bakımından en çok bilinen ve uygulanan suç işleme yöntemleri sıralanırsa şu yöntemlerle karşılaşılır.[38]

Truva Atı: Truva atı, görünüşte yararlı bir işlevi yerine getirdiği düşünülen ancak bunun dışında bilişim sistemine zarar verecek gizli kod da içeren bir programdır. Genellikle internette ücretsiz yazılım sağlayan web sitelerinde ya da elektronik posta yoluyla kullanıcılara ulaştırılmaktadır. Truva atı; sisteme bulaştıktan sonra, sistemin açılması ile beraber kendisini belleğe yükler ve sistem ağlarının açıklarını kullanarak, programı yerleştiren tarafın isteklerine cevap verir.

Salam Tekniği: Bu teknik çok fazla sayıda kaynaktan, çok az sayıda değerlerin transferini esas alır. Genel olarak, tekniğin uygulanmasında Truva atı programları kullanılır. Bu yöntem özellikle bankacılık alanında kullanılır. Bilişim sistemleri ile hesap edilen bankacılık alanındaki değerlerin çarpımları sonucu ortaya çıkan değerler çok basamaklı olmasına karşın, bu değerler uygun bir basamağa kadar yuvarlanır. Yuvarlama sonucu çıkan rakam, belli bir hesaba gönderilir. Bu sayede hesaplarda fark edilemeyecek değişiklikler olur. Ancak bir hesap için çok değersiz görünen bu değerlerin, alternatif bir hesaba aktarılması durumunda toplanan miktarlar büyük yekun oluşturmaktadır.

Ağ Solucanları: Ağ solucanları, herhangi bir kullanıcı müdahalesine ihtiyaç duymadan kendi kendini çalıştırabilen ve kendisi bir kopyasını ağa bağlı olan diğer bilişim sistemlerine de kopyalayabilen bir programdır. Ağ solucanları çoğunlukla bilgisayar virüsleri ile karıştı-

---

37 Kurt, *a. g. e.*, s. 170.

38 Yazıcıoğlu, *a. g. e.*, s. 150.

rılmaktadır. Fakat ağ solucanları, bilgisayar virüsleri gibi sisteme zarar verme zorunluluğu olmadan da sistemin içinde dolaşabilmektedir. Ağ solucanları bilişim ağında ulaştıkları bir sistemin güvenlik duvarıyla karşılaştıklarında, tahmin edilmesi kolay şifreleri ve verileri kullanarak, genellikle kullanılan şifrelerden oluşan bir sözlükten anahtarları deneyerek, duvarı aşmaya çalışırlar. Genellikle iyi oluşturulmamış güvenlik duvarlarını aşarak sistemlere girmekte ve eylemlerine başlamaktadırlar.[39]

Bilgisayar Virüsleri: Bilgisayar virüsleri işletim sisteminin ve makine dilinin verdiği olanaklar kullanılarak yazılan, kendi kendisini çoğaltabilen, kopyalarını çeşitli yöntemlerle başka bilişim sistemlerine ulaştırarak bu sistemleri de etkileyebilen yazılımlardır. Bilgisayar virüsleri, yazılımdan yazılıma, dosyadan dosyaya, sistemden sisteme kolaylıkla kopyalanabilmektedirler. Bu kopyalanma işlemine günlük kullanımda *"virüs bulaşması"* denilmektedir. Sistemleri veri depolama üniteleri başta olmak üzere kullanılamaz hale getirebilen bilgisayar virüsleri, bulaştıkları bilişim sisteminde bulunan yazılımları çökerterek, sisteme olası en fazla zararı verecek şekilde tasarlanmışlardır.

İstem Dışı Alınan Elektronik İletiler (Spam): Spam teknik olarak, internet üzerinde aynı mesajın yüksek sayıdaki kopyasının, bu tip bir mesajı alma talebinde bulunmamış kişilere, zorlayıcı nitelikte gönderilmesi olarak ifade edilebilir. Spam, genellikle bir ürünün reklâmı, pazarlanması veya sosyal içerikli bir mesajın dünya çapında kitlelere ulaştırılması amacı ile kullanılır. Bu tür mesajlar bünyesinde çok sayıda elektronik posta adreslerinin veri tabanlarını bulunduran kuruluşların, bu veri tabanlarını bedel karşılığında satması sonucu artmıştır. Son yıllarda spam sorununun dünya çapında yaygınlık kazanması ve önemli ölçüde ekonomik zarara sebebiyet vermesi dolayısıyla başta ABD ve Avustralya olmak üzere pek çok devlet bu konuda yasal düzenlemeler yapmak zorunda kalmıştır.[40]

Mantık Bombaları: Mantık bombaları, bilişim sistemlerinde veya ağlarında, daha önceden belirlenmiş özel durumların gerçekleşmesi

---

[39] Burak Çekiç, İnternet Aracılığıyla İşlenen Suçlar, Marmara Üniversitesi Sosyal Bilimler Enstitüsü yayınlanmamış yüksek lisans tezi, İstanbul, 2005, s. 9.

[40] Topaloğlu, *a. g. e.*, s. 182; Tekin Memiş, Hukuki Açıdan Kitlelere E-Posta Gönderilmesi, *AÜEHFD*, Erzincan, C. V S. 1–4, 2001, s. 440.

durumunda zarar verici sonuçlar yaratan programlardır. Bir mantık bombası, belirlenmiş özel durum gerçekleşene kadar truva atı programı gibi davranır. Ancak özel durumun gerçekleşmesinden sonra bilişim sistemlerinde zararlı etkisini meydana getirir ve bu noktada her zaman kendisini gizli tutmaya çalışan truva atı programından ayrılır. Mantık bombalarının tek amacı içine girdikleri sisteme zarar vermek olduğundan dolayı harekete geçtiklerinde sistem için yıkıcı olmaktadırlar.

Yukarıda vermiş olduğumuz örnekler haricinde; sistem güvenliğinin kırılıp içeri girilmesi (hacking), tavşanlar (rabbits), bukalemunlar (chameleon), çöpe dalma, gizlice dinleme, veri aldatmacası, tarama, gizli kapılar, eşzamanlı saldırılar, sırtlama, yerine geçme, sahte ileti (fake mail), kurtlar, web sayfası hırsızlığı ve yönlendirmesi gibi yöntemler de kullanılmaktadır.

c.4. Netice

5237 sayılı TCK'nın 244. maddesinde "*engelleyen, bozan, yerleştiren, gönderen, erişilmez kılan, değiştiren, yok eden*" şeklinde eylemlerin meydana gelmesi ile bir sonucun ortaya çıkması aranmıştır. Bu nedenle bu suç neticeli suçtur. Neticeli suç, salt fiilin icra edilmesinden ayrı olarak kanuni tarifte belirtilen neticenin meydana gelmesi demektir.[41] TCK 244 maddesinde failin yaptığı hareketler neticesinde bir zarar meydana gelmesi aranmaktadır. Zaten bu eylemler neticesinde zararın meydana gelmemesi hayatın olağan akışına aykırıdır.

d. Manevi Unsur

Manevi unsur, işlenen fiil ile kişi arasındaki manevi bağdır. Bu bağ olmadığı müddetçe, gerçekleştirilen davranış fiil niteliğini taşımaz ve bir suçun varlığından söz edilemez.[42] Hukuka aykırı olarak bilişim sistemine girme ve sistemde kalma suçunun manevi unsuru kasttır. Bilindiği üzere kast, suçun kanuni tanımındaki unsurların bilerek ve is-

---

41 İzzet Özgenç, *Türk Ceza Hukuku Genel Hükümler*, Seçkin Yay, Ankara 2008, s. 180.

42 Özgenç, *a. g. e.*, s. 225.

teyerek gerçekleştirilmesidir.[43] Suç işleme kastının varlığı için failin, bir bilişim sistemine izinsiz olarak girmeye hakkının olmadığını, bilişim sistemine izinsiz olarak girerken hukuka aykırı şekilde hareket ettiğini bilmesi ve sonuçlarını istemesi gereklidir. Fail, bilişim sistemine girmek için mağdurun rızasını almış olsa bile, sistem içerisinde rızayı aşacak şekilde işlemler yapmış ise, yine suç işleme kastından bahsedilecektir.

Bu suç tipinin taksirle işlenmesi mümkün değildir.

e. Hukuka Aykırılık Unsuru

Hukuka aykırılık unsuru, işlenen fiile hukuk düzeni tarafından cevaz verilmemesi, fiilin bütün hukuk düzeni ile çelişki ve çatışma halinde bulunması anlamına gelmektedir. Hukuka aykırılık, suçun genel bir unsuru olup, tüm hukuk düzeninin fiil hakkındaki değersizlik yargısını ifade eder. Bir fiilin hukuka aykırı olması, onun bütün hukuk sistemine aykırı olması sonucunu doğurur.[44]

Suçun hukuka aykırılık unsurunu ortadan kaldıran ve dolayısıyla fiili tüm hukuk düzeni bakımından hukuka uygun hale getiren sebeplere ise hukuka uygunluk sebepleri denir. Ceza kanunumuzda hukuka uygunluk sebepleri sınırlandırılmıştır. 5237 sayılı Türk Ceza Kanunu'nun 24/1, 25/1, 26/1-2. maddelerine göre hukuka uygunluk sebepleri, kanunun hükmünü yerine getirme, meşru savunma, hakkın kullanılması ve ilgilinin rızasıdır.[45]

Bilişim sistemini engellemek, bozmak, verileri değiştirmek veya yok etmek fiillerinde, her olay için hukuka uygunluk sebeplerinin varlığı araştırılmalıdır. Uygulamada sıkça karşılaşılabilmesi bakımından özellikle ilgilinin rızası konusunu açmakta yarar var. Şöyle ki, TCK'nın 26/2. maddesinde, "*Kişinin üzerinde mutlak surette tasarruf edebileceği bir*

---

43 Timur Demirbaş, *Ceza Hukuku Genel Hükümler*, Seçkin Yay, Ankara 2009, s. 341; Hakan Hakeri, *Ceza Hukuku Genel Hükümler,* Seçkin Yay, Ankara, 2009, s. 177; Zeki Hafızoğulları /Muharrem Özen, *Türk Ceza Hukuku Genel Hükümler*, Usa Yay, Ankara 2010, s. 276.

44 Mahmut Koca/İlhan Üzülmez, *Türk Ceza Hukuku Genel Hükümler*, Seçkin Yay, Ankara 2009, s. 250.

45 Hafızoğulları / Özen, *a. g. e.,* s. 238.

hakkına ilişkin olmak üzere, açıkladığı rızası çerçevesinde işlenen fiilden dolayı kimseye ceza verilmez" demektedir. Burada mağdurun rızası, hareketi hukuka uygun hale getirmektedir. Teorik olarak, rızanın fiili hukuka uygun hale getirmesi bakımından belli şartları taşıması gerekir. Bunlar, kişinin üzerinde mutlak surette tasarrufta bulunulabilecek bir hakkın varlığının olması; rıza gösterenin rızasının kapsamını ve önemini algılayacak durumda olması ve rıza beyanının, mutlaka suçtan önce veya suçun icra hareketlerinin yapılması sırasında olmasıdır.[46]

Bilişim sistemine ilgilisinin rızası ve bilgisi dahilinde yapılan müdahaleler, bu kapsamda suç oluşturmayacaktır. Rızayı aşan durumun varlığı halinde ise, suçun oluştuğu kabul edilmelidir. Bu nedenle ilgilinin rızasının kapsamı net olarak tespit edilmeli ve sonucuna göre hüküm verilmelidir.

f. Suçun Özel Görünüş Biçimleri

f.1. Teşebbüs

TCK'nın 35. maddesinde belirtilen teşebbüs, failin işlemeyi amaçladığı bir suçun elverişli hareketlerle doğrudan doğruya icraya başlayıp da elinde olmayan nedenlerle sonuca ulaşamaması halidir. TCK 244. maddede tanımlanan suçlar, teşebbüse elverişli olan suçlardandır. Fail sistemi engellemeye veya bozmaya yönelik herhangi bir eylemi gerçekleştirmesine rağmen, elinde olmayan nedenlerle netice gerçekleşmemişse, suç teşebbüs aşamasında kalmış demektir. Örneğin failin amaca elverişli bir virüsü sisteme sokup faal hale getirmesine karşın, anti virüs programı sayesinde sistemin işleyişi engellenmemiş veya bozulmamışsa, fail bu suça teşebbüsten cezalandırılmalıdır. Yargıtay kararları da teşebbüs konusunu açıklamaya yardımcı niteliktedir.[47]

---

[46] Hafızoğulları / Özen, *a. g. e.,* s. 267.

[47] Yrg. 11.CD.25.06.2007, 2007/2168-4372 E-K: Bilişim sistemindeki verileri değiştirmek suretiyle haksız menfaat elde edilmesi suçunun sanık tarafından EFT'nin şikayetçi şirketin hesabından sahte olarak açtırmış olduğu hesaba intikali anında tamamlandığı gözetilmeyerek eylemin teşebbüs aşamasında kaldığından bahisle eksik ceza tayini aleyhe temyiz olmadığından bozma sebebi sayılmamıştır.

Yrg.11.CD.12.05.2009, 2009/3700-6207 E-K: Sanıkların, mağdurların bankalarda bulunan para hesaplarındaki var olan verileri (bilgileri) sahte kimliklerle açtırdıkları hesaba bilişim sistemi aracılığıyla göndererek yine sahte kimliklerle çek-

f.2. İştirak

Bilindiği üzere 5237 sayılı TCK'da iştirak konusu, 765 sayılı TCK'da yer alan iştirakten farklı düzenlenmiş ve asli fail - feri fail ayrımı terk edilmiştir. Yeni yapılan düzenlemeyle, fiilin işlenişi üzerinde kurulan hakimiyet ölçü olarak belirlenmiş, iştirak şekilleri ise, faillik, azmettirme ve yardım etme olarak sayılmıştır.[48] TCK 244. maddedeki suçlar bakımından suça iştirakte herhangi bir özellik bulunmamaktadır. TCK'nın 37, 38, 39 ve 40.maddelerindeki iştirake ilişkin genel kurallar burada da uygulanacaktır.[49]

f.3. İçtima

5237 sayılı TCK'da, *"kaç tane fiil varsa o kadar suç, kaç tane suç varsa o kadar ceza vardır"* ilkesi benimsenmiş; bu ilkenin istisnaları ise, Kanun'un Birinci Kitap İkinci Kısım Beşinci Bölüm'de bileşik suç (m. 42), zincirleme suç (m. 43) ve fikri içtima (m. 44) olarak belirtilmiştir.

TCK 244. maddede tanımlanan suçlar bileşik suç tanımına girmemektedir. Şöyle ki; bileşik suçlar, birden fazla hukuki konusu olan ya da başka bir deyişle çok ihlalli[50] suçlardır. Dolayısıyla bu suçların işlenmesiyle birden çok hukuki değerin ihlal ediliyor olması, haklı olarak kanun koyucuyu bileşik suçları, bu suçların unsurunu ya da ağırlaştırıcı nedeni oluşturan suçlara oranla daha ağır bir şekilde cezalandırmaya itmektedir. Çünkü bileşik suçta failin ahlaki kötülüğü, bileşenleri oluşturan suçlara göre çok daha fazladır. Yağma suçu bileşik suça örnek olarak verilebilir. Bundan başka, birleşik suçta kanunun suç saydığı bir fiil, kimi zaman başka bir suçun ağırlatıcı nedeni olabilmektedir. Bu halde, temel suçun ismi, kimliği bir değişikliğe uğramamakta, sadece suçun cezası artırılmaktadır. Böylece, bir suçun ağır-

---

mek istemesinden ibaret eylemlerinin paranın açılan hesaplara transferiyle suçun tamamlanacağı gözetilmeden paranın çekilmemesi nedeniyle teşebbüs aşamasında kaldığından bahisle eksik ceza tayini isabetsizliği karşı temyiz olmadığından bozma nedeni yapılmamıştır.

48 Kurt, *a. g. e.,* s. 266.

49 Dülger, *a. g. e.,* s. 241.

50 Zeki Hafızoğulları, *Ceza Hukuku Ders Notları*, Ankara 2008. http://www.zekihafizogullari.com/CezaHukuku%20Ders%20Notlari.pdf, s. 305. Kontrol Tarihi: 29.08.2010.

latıcı nedeni olan diğer bir suç, artık kendi kimliğini yitirmekte ve her suçta ağırlatıcı nedenler hangi kurallara tabi ise, bu da o kurallara tabi olmaktadır. TCK 244. maddede ise böyle bir düzenleme bulunmamaktadır.

TCK 244. maddedeki suçların zincirleme şekilde işlenmesi mümkündür.[51] TCK 43. maddeye göre, bir suçun aynı kişilere karşı farklı zamanlarda işlenmesi halinde zincirleme suçtan bahsedilebilecektir.[52] Başka bir deyişle, zincirleme suçun söz konusu olabilmesi için kural olarak aynı suç en az iki kez işlenmelidir. Bu suçlardan biri tamamlanmış, diğeri teşebbüs halinde kalmış olabileceği gibi; her iki eylem de teşebbüs halinde kalmış olabilir. Ancak fail, uzun süreli aralıklarla suçları işlemişse, ayrı ayrı suçların varlığını kabul etmek gerekecektir.

Fikri içtima konusunda, mala zarar verme suçu ile TCK'nın 244 maddesindeki suçların ilişkisine değinmek gerekmektedir. Şöyle ki, doktrinde bu konuda farklı görüşler ortaya konmaktadır. Özgenç'e göre sistemin somut unsuru olan donanım kısmına yönelik saldırılar mala zarar verme suçu olarak değerlendirilmelidir[53]. Yani sistemin fiziki varlığına zarar vermeksizin, elektronik ortamda verilen talimatlarla sisteme zarar verilmişse bilişim suçuna göre, şayet fiziki unsurlara zarar verilmişse klasik mala zarar verme suçuna göre hüküm kurulmalıdır. Burada bu sonuca ulaşılmasının sebebi, bilişim suçu kapsamındaki zarar vermelerin konusunu oluşturan mal varlığı ile klasik mala zarar vermenin konusu olan mal varlığı değerlerinin farklılık göstermesidir.

---

51 TCK 43: (1) Bir suç işleme kararının icrası kapsamında, değişik zamanlarda bir kişiye karşı aynı suçun birden fazla işlenmesi durumunda, bir cezaya hükmedilir. Ancak bu ceza, dörtte birinden dörtte üçüne kadar artırılır. Bir suçun temel şekli ile daha ağır veya daha az cezayı gerektiren nitelikli şekilleri, aynı suç sayılır. Mağduru belli bir kişi olmayan suçlarda da bu fıkra hükmü uygulanır.

(2) Aynı suçun birden fazla kişiye karşı tek bir fiille işlenmesi durumunda da, birinci fıkra hükmü uygulanır.

(3) Kasten öldürme, kasten yaralama, işkence ve yağma suçlarında bu madde hükümleri uygulanmaz.

52 Kubilay Taşdemir, *Bilişim, Banka ve Kredi Kartlarının Kötüye Kullanılması ve Dolandırıcılık Suçları*, Ankara 2009, s. 324.

53 İzzet Özgenç, *Türk Ceza Kanunu Gazi Şerhi*, Ankara, 2005, s. 989.

Bir başka görüşe göre, bozmak eylemi fiziki saldırı şeklinde olduğu durumda aslında klasik mala zarar verme suçu oluşmaktadır. Bunun yanında fiziki saldırı sonucunda, örneğin bilgisayarın kırılması halinde, aynı zamanda bilişim sisteminin işleyişi de bozulmaktadır. Tek bir fiil ile kanunun birden fazla hükmünün ihlâl edilmesi nedeniyle de, fikri içtima hali uygulanmalı ve en ağır cezayı gerektiren hükme göre ceza verilmelidir.[54]

Bir başka görüşe göre, mala zarar verme suçunun konusunu, başkasının taşınır veya taşınmaz malı oluşturmaktadır. Bahse konu suç tipinde suçun konusunu, bilişim sistemi yanında veriler de oluşturmaktadır. Ancak burada bilişim sisteminden kastedilen, bir mal olarak duran eşyanın değil, işlerliği olan, bilişim sistemi olarak kullanılan ve fayda sağlayan bir araçtır. Bu nedenle her iki hüküm birbirinden tamamen farklı iki suç tipini düzenlemekte ve suç politikasıyla belirlenen iki farklı hukuksal değeri koruma altına almaktadır. Dolayısıyla iki madde arasında özel-genel hüküm ilişkisi bulunmadığı gibi salt mala zarar verme kastıyla yapılan bir eyleme, TCK'nın 244. maddesinde düzenlenen hüküm uygulanmamalıdır.[55]

Kanaatimizce, bilişim sistemleri ve özellikle bilgisayar sistemleri esas alındığında, bunların karakteristik özelliklerini donanım yani fiziksel yapıdan çok yazılım unsuru belirlemektedir. Bu açıdan bir aygıt olarak bilgisayar sistemlerini diğer aygıtlardan ayıran unsur, yazılım kapsamında belirli komutlar aracılığıyla veri işleme faaliyetini yapabilmesi ya da daha genel bir ifade ile işlem yapabilmesidir. Bu nedenle suç işleyen kişinin kastı önem kazanmaktadır. Bir cihazın bilişim sistemi olduğunu bilerek ve sisteme zarar vermek amacıyla eylemde bulunan kişinin eylemi bilişim suçu kapsamında değerlendirilmelidir. Sistem fiziksel olarak ayrı unsurlar barındırıp da, bu unsurlara yönelik saldırılar da şayet sistemin işleyişini sağlayan unsurlardansa, yine bilişim suçu kapsamında değerlendirilmelidir. Bu değerlendirme, bilgisayara yapılan her eylemin bilişim suçunu ihlal edeceği anlamına gelmemelidir. Donanıma yapılan müdahale sonrası sistemin işleyişi bozulmamışsa mala zarar verme suçundan cezalandırma yoluna gidilmelidir. Ayrıca sistemin işleyişine etkisi olmayan sisteme bağlı olan

---

54 Kurt, *a. g. e.*, s. 165.

55 Dülger, *a. g. e.*, s. 242.

veya öylesine sistemin yanında duran bir bilgisayar parçasına verilen zarar evleviyetle genel mala zarar verme suçu kapsamında değerlendirilmelidir. Bir iş yerine zarar vermek amacıyla işyerindeki malzemelerde tahribat yaratıldığında, bilgisayarlara da zarar verilmiş ve sistem zarara uğratılmışsa, burada suç kastı nedeniyle, mala zarar verme suçundan cezalandırma yoluna gidilmelidir.

Türk Ceza Kanunu'nda içtima konusunda, sınırlı ve sayılı düzenlemeye gidilmişse de, doktrinde suçların görünüşte içtima ettikleri çeşitli hallerin varlığı da kabul edilmektedir. Buna göre, görünüşte içtima halinde suçların çokluğu sadece görünüşte olup, gerçekte ortada fiile uygulanacak tek bir norm bulunmaktadır.[56] Görünüşte içtimaının çeşitleri özel-genel norm ilişkisi yönünden; tüketen-tüketilen norm ilişkisi yönünden ve asli-tali norm ilişkisi yönünden görünüşte içtima olarak kabul edilmektedir. Asli-tali norm ilişkisi yönünden görünüşte içtima konusuna aşağıda TCK'nın 244/4 maddesi anlatılınca değinilecektir. Burada değinilecek konu, TCK'nın 244. maddesinin birinci ve ikinci fıkralarındaki tüketen-tüketilen norm ilişkisi yönünden görünüşte içtima halidir.

Bir normun, diğer bazı normlar tarafından korunan hukuki değerlerin tümünü ortak bir şekilde koruduğu durumlarda tüketen-tüketilen norm ilişkisi (geçitli suç) ortaya çıkar. Bu şekilde bir normun diğer bir normu bünyesine alması halinde, artık o norm varlığını kaybettiğinden, onun uygulanma olanağı yoktur.[57] TCK'nın 244. maddesinin birinci fıkrasında bilişim sistemine karşı düzenlenen fiillerin, sistemdeki veriler aracılığıyla gerçekleştirilmesi halinde, her iki fıkradaki suçlar da ihlal edilmiş olacaksa da, ikinci fıkradaki suç, birinci fıkradaki suç tarafından yutulur ve sadece birinci fıkradaki suç nedeniyle cezalandırma yoluna gidilir. Bu durumda her iki fıkrayı ihlal eden eylemler bağımsız eylemler olarak kabul edilmezler.

---

56 Koca / Üzülmez, *a. g. e.*, s. 462.

57 Veli Özer Özbek, *Türk Ceza Hukuku Genel Hükümler*, Seçkin Yay, Ankara, 2010, s. 532; Demirbaş, *a. g. e.*, s. 486.

g. Suça Etki Eden Nedenler

TCK'nın 244. maddesinin 3. ve 4. fıkralarında suça etki eden nedenler açısından iki düzenlemeye yer verildiği görülmektedir. Üçüncü fıkrada, TCK'nın 244. maddesinin 1. ve 2 fıkrasında düzenlenen fiillerin bir kamu kurum ya da kuruluşuna ya da banka veya kredi kurumuna ait bilişim sistemi üzerinde işlenmesi halidir. Son fıkrada yer alan hüküm ise, genel olarak bilişim ya da bilgisayar sistemleri aracılığıyla yarar sağlama fiillerinin cezalandırılmasına yönelik bir düzenlemedir ve aşağıda ayrı bir başlık altında incelenecektir.

TCK'nın 244. maddesinin 3. fıkrasında suçun ağırlaştırıcı nedeni düzenlenmiştir. Buna göre, bilişim sisteminin işleyişinin engellenmesi, bozulması, verilerin yok edilmesi veya değiştirilmesi suçunun bir banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinde işlenmesi halinde verilecek ceza arttırılacaktır. Tüm kamu kurum veya kuruluşlarına ait bilişim sistemleri üç numaralı fıkra kapsamında değerlendirilebilecektir. Özel kurumlardan ise banka veya kredi kurumu niteliği olan tüm özel kurum veya şirketler TCK 244/3 kapsamında değerlendirilecektir. TCK 158/1.j'de kredi kurumunun ne olduğu söyle tanımlanmaktadır: "*Kredi kurumu deyiminden, banka olmamasına karşın, kanunen borç para vermeye yetkili kılınan kurumlar anlaşılır.*" Şu halde, özel finans kurumları da kredi kurumu olarak kabul edilmelidir.[58]

TCK'nın 244. maddesinin üçüncü fıkrası ile maddenin 765 sayılı TCK'daki karşılığı olan 525 b.1'deki önemli bir eksiklik giderilmiş ve zarar verilen sistemin bankaya, kredi kurumuna ya da bir kurum ve kuruluşa ait bilişim sistemi olması ağırlaştırıcı neden sayılmıştır. Nitekim bir kişisel bilgisayarın işleyişinin engellenmesinden doğacak zarar ile bir bankanın bilgisayarının işlemesinin engellenmesinden doğacak zarar arasında ciddi fark vardır. Bu nedenle bankanın sistemine verilen zarar nedeniyle failin daha ağır bir cezaya çarptırılması da hakkaniyetle bağdaşmaktadır.[59]

---

[58] Şaban Cankat Taşkın, *Bilişim Suçları*, Beta Yay, Bursa, 2008, s. 65.

[59] Dülger, *a. g. e.*, s. 243.

h. Yaptırım ve Usul Hükümleri

5237 sayılı TCK'nın 244. maddesinin 1. fıkrasında düzenlenen eylemler açısından bir yıldan beş yıla kadar hapis cezası, 2. fıkrasında düzenlenen eylemler açısından ise altı aydan üç yıla kadar hapis cezası öngörülmüştür.

5237 sayılı TCK'nın 244. maddesinin 3. fıkrasında düzenlenen durumun gerçekleşmesi halinde, yukarıda belirtilen cezalar yarı oranında arttırılacaktır.

TCK'nın 244. maddesinde düzenlenen suçlar şikayete bağlı olmayıp, C. Başsavcılığı tarafından doğrudan soruşturma yapılır. Yargılama yetkisi ise asliye ceza mahkemelerine aittir.

II. Bilişim Sistemleri Aracılığıyla Yarar Sağlama Suçu

a. Giriş

Özellikle bilişim sistemi aracılığıyla hileli ya da aldatıcı hareketler yapılarak haksız çıkar sağlanmasında, hileli ya da aldatıcı hareketlerin kişiye karşı yapılmaması, fiillerin bilgisayar sistemi içerisinde yapılması ve bilişim sisteminde somut olmayan veriler üzerinden suçun işlenebilmesi nedeniyle, mukayeseli hukukta klasik dolandırıcılık ve hırsızlık suçlarından farklı olarak bilişim sistemleri aracılığıyla yarar sağlama hali yeni bir suç tipi olarak kabul edilmiştir.[60]

Bu tarz bir düzenlemenin İtalyan Ceza Kanunu'nda klasik dolandırıcılık suçundan sonra gelmek üzere Kanun'un 640ter maddesinde düzenlendiği görülmektedir. 640ter maddesinde, dolandırıcılığa ilişkin diğer unsurlar korunmuş, hile ve desise ile kişinin hataya düşürülmesi unsuru yerine genel olarak veri işleme faaliyetine ya da verinin kendisine müdahale edilmesi suçun unsuru haline getirilmiştir.

Alman Ceza Kanunu'nda da benzer bir yaklaşım sergilenmiş, Ceza Kanunu'nun dolandırıcılık suçunun düzenlendiği 263. maddesinden sonra gelmek üzere, 263a maddesinde, failin kendisine veya üçüncü kişiye hukuka aykırı yarar sağlaması amacıyla veriye ve veri işleme faaliyetine müdahale etmesi suç olarak düzenlenmiştir. Bu ka-

60 Akıncı/ Alıç/ Er, a. g. m., s. 188.

nunda 263. maddede düzenlenen dolandırıcılık suçunun unsurunu oluşturan hileli hareketlerle kişinin hataya düşürülmesi ya da var olan hatadan yararlanılması şartı bilgisayar dolandırıcılığı bakımından aranmamıştır.[61]

Benzeri bir düzenleme Siber Suç Sözleşmesi m. 8'de de yer almaktadır. Buna göre, bilgisayarlarla ilişkili sahtecilik fiilleri, bir diğer kişinin malvarlığında doğrudan bir zarara yol açmış ve suçu işleyen kimse kasıtlı olarak kendisi veya bir başkası için yasadışı ekonomik yarar sağlamak amacıyla hareket etmişse suçun oluşacağı kabul edilmiştir.[62]

Mukayeseli hukuktaki gelişmelere paralel olarak, TCK'nın 244. maddesinin son fıkrasında bilişim sistemi aracılığıyla haksız yarar sağlamaya ilişkin bir düzenlemeye yer verilmiştir. TCK'nın 244. maddesinin 4. fıkrasında düzenlenen bu suç, maddenin 1 ve 2. fıkralarına göndermede bulunmaktadır. Bu fıkrada, bir bilişim sisteminin işleyişinin engellenmesi, bozulması, sistemdeki verilerin bozulması, yok edilmesi, değiştirilmesi, başka yere gönderilmesi, erişilmez kılınması, sisteme veri yerleştirilmesi suretiyle kişinin kendisinin veya başkasının yararına haksız çıkar sağlaması, bu sayılan fiiller *"başka bir suç oluşturmadığı"* takdirde cezalandırılmaktadır. Bu suç tipi 765 sayılı TCK'nın 525/b.2'deki suç tipinin karşılığıdır. Ancak yeni düzenlemenin eski düzenlemeden temel farkı, yeni düzenlemede suçu oluşturan fillerin açıkça gösterilmesi ve suçun sınırlarının iyi çizilmesidir.[63]

Maddedeki "*başka bir suç oluşturmama*" düzenlemesi nedeniyle, TCK'nın 244/4 maddesi asli norm-tali norm ilişkisi kapsamında incelenmelidir. Bilindiği üzere asli norm-tali norm ilişkisinin bulunduğu hallerde olaya uygulanacak tek norm asli normdur. Zira yardımcı normun sonralığı ilkesine göre, asli normun bulunduğu hallerde yardımcı normun fiile uygulanması mümkün değildir. Bu tür normlar, çoğunlukla kanunda bulunabilecek boşlukları tamamlama görevini gören normlardır.[64] Bu bağlamda, TCK'nın 244/4 maddesi tali normdur

---

61 Ketizmen, *a. g. e.,* 149.

62 Aslı Deniz Helvacıoğlu, "Avrupa Konseyi Siber Suç Sözleşmesi Temel Hükümlerinin İncelenmesi", İnternet ve Hukuk**,** Derleyen: Yeşim M. Atamer, *Bilgi Üniversitesi Yayınları*, 1.Baskı, İstanbul, Ocak 2004, s. 286-287.

63 Dülger, *a. g. e.,* s. 244.

64 Koca / Üzülmez, *a. g. e.,* s. 467; Özbek, *a. g. e.,* s. 533.

ve bu hükmün uygulanabilmesi için, fiilin başka bir suç oluşturmaması gerekir. Maddenin gerekçesinde, *"fiilin daha ağır cezayı gerektiren başka bir suç oluşturmaması gerekir"* denilmiş ise de, bu ifade madde metni ile çelişki halindedir. Gerekçe, cezanın belirlenmesinde belirleyici olmadığından, madde metnine bağlı kalmak ve cezanın ağırlığı ne olursa olsun, eğer fiil başka bir suçu oluşturuyorsa, faile o suçtan ceza vermek gereklidir.

b. Suçla Korunan Hukuki Değer

Bu suç tipinin yasa maddesindeki tanımına göre, failin bilişim sistemi aracılığıyla gerçekleştirdiği eylemler sonucunda suçun oluşması için mağdurda bir zararın meydana gelmesi gerekmektedir. Ancak bu zararın maddi veya manevi zarar olup olmayacağı açıklanmamıştır. Zararın türü bakımından bir ayrım yapılmadığına göre, fail tarafından zarara uğratılan maddi veya manevi hak, suçla korunan hukuksal değeri oluşturmaktadır.[65]

c. Maddi Unsurlar

c.1. Suçun Fail ve Mağduru

5237 sayılı TCK'nın 244. maddesinin 4. fıkrasında düzenlenen bu suç tipinde fail için bir özellik aranmamıştır. Bu sebeple bu suçun faili herkes olabilir. Ancak tüzel kişiler suçun faili olamazlar.

Madde metninde mağdur bakımından da bir özellik öngörülmemiştir. Dolayısıyla, herkesin mağdur olabilmesi mümkündür. Söz konusu suçun oluşmasına yol açan eylemler nedeniyle zarara uğrayan kişiler, çıkarları zedelendiği için suçun mağduru olacaktır. Tüzel kişiler ise, suçtan zarar görendir. Suçun mağduru ile suçtan zarar gören kavramları birbirlerinden farklıdır. Şöyle ki, suçun mağduru suçtan doğan ceza ilişkisinin tarafı olduğu halde; suçtan zarar gören, hukuk ilişkisinin tarafıdır ve iddiası esas itibariyle hukuksal nitelik taşımaktadır.[66]

---

65 Dülger, *a. g. e.*, s. 244.

66 Bahri Öztürk / Mustafa Ruhan Erdem / Özge Sırma / Yasemin Saygılar, *Ceza Muhakemesi Hukuku Temel Kavramlar,* Turhan Kitabevi, Ankara, 2006, s. 200.

c.2. Suçun Konusu

TCK 244. maddenin 1. ve 2. fıkrasında düzenlenen suç tiplerinin konusu ile maddenin 4. fıkrasında düzenlenen suç tipinin konusu aynıdır. Buna göre, bu suçun konusu da bir bilişim sisteminin işleyişi veya bir bilişim sistemindeki verilerdir.

c.3. Hareket

Maddede 1 ve 2. fıkralara atıf yapıldığı için, bu fıkralarda düzenlenen bilişim sisteminin işleyişinin engellenmesi, bozulması, verilerin yok edilmesi, değiştirilmesi suçlarının maddi unsurunu oluşturan eylemler, bu suçun da maddi unsurunu oluşturmaktadır. Yukarıda bu konular anlatıldığı için tekrara girilmeyecektir. Ancak bu konuyla ilgili şu hususa dikkat çekilmelidir ki, bilişim sistemi aracılığıyla yarar sağlama suçunu oluşturabilecek fiiller, genel olarak iki başlık altında toplanmaktadır.

Birincisi verilere veya programlara müdahale aracılığıyla işlenen yarar sağlama halleridir. Verilere müdahale yoluyla yarar sağlama, bilgisayar sistemi içerisinde yer alan verilerin değiştirilmesi, erişilmez kılınması, silinmesi veya sisteme yeni verilerin eklenmesi seklinde ortaya çıkmaktadır. İkinci başlık olan programlara müdahale yoluyla yarar sağlama ise, bilgisayar sistemleri içerisinde var olan bir programa müdahale edilmesi ya da yeni bir program eklenmesi suretiyle gerçekleştirilebilir. Programlara müdahale yoluyla dolandırıcılık suçuna "*salam tekniği*" adı verilen yöntemi örnek göstermek mümkündür.[67] Yukarıda kısaca bu teknikten bahsedilmişti.

c.4. Netice

5237 sayılı TCK'nın 244/4. maddesinde yazılı eylemin meydana gelmesi ile haksız bir çıkarın sağlanması aranmıştır. Bu nedenle bu suç neticeli suçtur.

---

[67] Ketizmen, *a. g. e.,* s. 148.

d. Manevi Unsur

Suçun manevi unsuru, özel kasttır. Failde, genel kastın yanında kendisine veya başkasına haksız bir çıkar sağlama kastı da bulunmalıdır.

e. Hukuka Aykırılık Unsuru

Yukarıda hukuka aykırılık unsuru hakkında yapılan açıklamalara paralel olarak, bu suç bakımından, rıza hukuka uygunluk nedeni olarak kabul edilmelidir. Ancak rıza gösterenin mutlaka malik olması şart değildir. Sistemin ilgilisi (kullanan ya da yararlanan) de rızayı vermeye ehil olabilir. Malik olmadığı halde sistemden yararlanan kişinin verdiği bir rıza yoksa sadece sistemin malikinin verdiği rıza fiili suç olmaktan çıkarmayacaktır. Çünkü sistemden fiilen yararlanan malik olmayıp, sistemi kullanandır. Dolayısıyla, her somut olayda rızanın varlığı araştırılırken, rızayı verenin bu rızayı vermeye yetkisi olup olmadığına da bakılmalıdır.

f. Suçun Özel Görünüş Biçimleri

f.1. Teşebbüs ve İştirak

Suç, teşebbüs ve iştirak bakımından bir özellik taşımamaktadır. Genel hükümler uygulanacaktır.

f.2. İçtima

Maddede yazılı suç, fikri içtima bakımından özellik göstermektedir. Maddede açıkça *"kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlamasının başka bir suç oluşturmaması halinde"* ifadesine yer verildiğinden, söz konusu eylemlerin başka bir suç oluşturması halinde diğer suç tipleri olaya uygulanacaktır. Sorun da burada yatmaktadır. Şöyle ki, TCK'nın 142/2-e maddesinde yazılı hırsızlık suçunun bilişim sistemlerinin kullanılması suretiyle işlenmesi hükmü ve TCK'nın 158/1-f maddesinde yazılı, dolandırıcılık suçunun bilişim sistemlerinin kullanılması suretiyle işlenmesi hükmünün varlığı karşısında, so-

run TCK 244/4 maddesinin hangi hallerde uygulanacağı hususudur. Bu konuyla ilgili olarak Yargıtay çeşitli kararlar vermiştir.[68]

---

[68] Yrg. 11. CD, 26/09/2007, 2007/6122-5897 E-K**:** Sanığın, evrakı tefrik edilen suç ortaklarıyla birlikte fikir ve eylem birliği içinde Hasdağ Tekstil Sanayi ve Ticaret Limited Şirketi adına Akbank Kayseri Ticari Şubesinde bulunan 888-843-184019 nolu YTL hesabına internet üzerinden girerek, mevduatta bulunan 7.250.00 YTL. parayı, aynı bankanın Konya Truva Şubesinde kendi fotoğrafının yapıştırıldığı ve Veysel Tekin'e ait kimlik bilgilerini içeren sahte nüfus cüzdanı ile açtırdığı 888-773-0009847 nolu banka hesabına havale edip, bu şekilde hesaba yatan paradan 5000 YTL yi bankadan çektikten ve bakiye parayı çekmek isterken yakalandığı oluşa uygun şekilde kabul edilmiş olmasına göre, eylemin 5237 sayılı TCK'nın 244/4. maddesinde öngörülen bilişim suçunu oluşturduğu gözetilmeden suçun nitelendirilmesinde yanılgıya düşülerek hırsızlık suçundan yazılı şekilde hüküm kurulması.

Yrg. 11. CD, 28/01/2008, 2007/8337 E, 2008/269K: Dolandırıcılık suçundan 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, sanıkların açık kimlikleri tespit edilemediği için evrakı tefrik edilen faillerle fikir ve eylem birliği yaparak, İstanbul'da bulunan bir bilgisayardan katılanın Vakıfbank Ankara Şubesindeki hesabına ait internet şifresi kırılarak hesapta bulunan 41.500 YTL'nin, sanık Yaşar Aslan'ın Vakıfbank Gaziantep Şubesindeki hesabına EFT yoluyla havale etmeleri ve buradan da sanıklar Yaşar ile Eren'in parayı çekmelerinden ibaret eylemlerinde, gerçek kişiye yönelen hileli bir hareket bulunmaması nedeniyle dolandırıcılık suçunun unsurlarını oluşmadığı, fiilin 5237 sayılı TCK'nın 244/4 maddesine uygun "bilişim sistemini engelleme, bozma, verileri yok etme veya değiştirme suretiyle haksız çıkar sağlama" suçunu oluşturduğu gözetilmeden, suç vasfında hataya düşülerek yazılı şekilde bilişim sistemlerinin aracı olarak kullanılması suretiyle dolandırıcılık suçundan mahkumiyetlerine karar verilmesi.

Yrg. 11.CD, 24/03/2008, 2007/9407 E, 2008/1807 K: Sanığın, Denizbank A.Ş. Antalya Şubesi'nde kendi adına hesap açtırdıktan sonra, katılan F.A'ya ait aynı bankanın Karadeniz Ereğli Şubesi'ndeki banka hesabından, ele geçirdiği "interaktif bankacılık şifresini" kullanarak internet aracılığı ile banka hesabına para transferi yapmaktan ibaret eyleminin, gerçek kişiye yönelmiş bir hile bulunmadığı cihetle, suç tarihinde yürürlükte bulunan 765 sayılı Yasanın 525/b-2. maddesinde öngörülen "bilişim" suçunu oluşturduğu ve sonradan yürürlüğe giren 5237 sayılı Yasanın 244/4. maddesi ile karşılaştırma yapılması gerektiği gözetilmeden yazılı şekilde hüküm kurulması.

Yrg. 11.CD, 27/01/2009, 2008/15441 E, 2009/80 K: Dolandırıcılık suçunda unsur olan hileli davranışların gerçek kişiye yönelmesi ve bunun sonucunda onun veya başkasının malvarlığı aleyhine sanığın veya başkasının yararına haksız bir menfaat sağlanması gerekeceği, somut olayda ise; sanığın katılanın Şekerbank Uludağ Şubesinde mevcut şirket hesabına internet bankacılığı yoluyla girip hesaptaki paradan 7300.00 YTL'yı Yapı Kredi Bankası Adana Baraj Yolu Şubesinde Barış Güven sahte kimliğiyle açtırmış olduğu hesaba havale edip çekmeye çalıştığının iddia ve dosya içeriğine uygun gerekçelerle kabul edilmesi karşısında; Gerçek kişiye yönelen hile oluşturacak nitelikte bir hareketin bulunmaması nedeniyle dolan-

Yrg. 11.CD, 01/07/2008, 2006/1800 E,2008/7126 K: 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 katılan Türk Telekom A.Ş. tarafından üretilen ve ankesörlü telefonlardan konuşma yapmaya yarayan telefon kartlarının manyetik şeritlerine teyp bandı ile dolum yapmak suretiyle kaçak görüşme yaptığının iddia ve kabul olunması karşısında; gerçek kişiye yönelen hile oluşturacak nitelikte bir hareketin bulunmaması nedeniyle dolandırıcılık suçunun unsurlarının bulunmadığı, ayrıntıları Ceza Genel Kurulu'nun 19.06.2007 gün ve 136-150 sayılı kararında belirtil-

---

dırıcılık suçunun unsurlarının bulunmadığı, fiilin 5237 sayılı TCK'nın 244/4 maddesinde öngörülen bilişim suçunu oluşturduğu gözetilmeden, suç vasfında hataya düşülerek yazılı şekilde bilişim sistemlerinin aracı olarak kullanılması suretiyle dolandırıcılık suçundan mahkumiyetine karar verilmesi.

Yrg. 11.CD, 07/10/2009, 2009/1616-11328 E-K: Dolandırıcılık suçu; hileli davranışlarla bir kişinin aldatılıp onun veya bir başkasının zararına, failin kendisine veya bir başkasına yarar sağlaması suretiyle oluşur. Suçun maddi unsurunu oluşturan hareketlerin, gerçek bir kişiye yöneltilmiş olması, onun kandırılarak çıkar sağlanması gerekir. Bilişim sistemlerinin araç olarak kullanılması suretiyle dolandırıcılık suçunda ise, verileri toplayıp yerleştirdikten sonra bunları otomatik işlemlere tabi tutma olanağını veren manyetik sistemler araç olarak kullanılıp gerçek kişiler aldatılarak çıkar sağlanmaktadır. Bankaların etkin işlevi bulunan çek, hesap cüzdanı, dekont gibi maddi varlıklarının kullanılması halinde ise, banka vasıta kılınarak dolandırıcılık suçu oluşacaktır.

Gerçek bir kişiyle karşı karşıya gelmeden, yüz yüze veya telefon, bilgisayar, bilgi geçer gibi bir başka vasıta kullanılarak görüşmeden, konuşmadan, kişilere yönelik hileli davranışlarla aldatılmadan sadece bilişim sistemi kullanılarak doğrudan doğruya çıkar sağlanması halinde "bilişim sistemine girerek haksız çıkar sağlama suçu" gerçekleşecektir.

Somut olayda ise; sanığın, katılanın Garanti Bankası 1. Levent Şubesinde bulunan hesabına internet bankacılığı yoluyla girip hesaptaki paradan 3.200.00 TL'yı Garanti Bankası Osmanbey Şubesindeki kendi hesabına internet yoluyla havale ettikten sonra parayı çekerek haksız menfaat sağladığı iddia ve dosya içeriğine uygun kabul edilmesi karşısında; gerçek kişiye yönelen hile oluşturacak nitelikte bir hareketin bulunmaması ve tamamen bilişim sistemi içinde gerçekleştirilmesi nedeniyle dolandırıcılık suçunun unsurlarının bulunmadığı "veri"nin taşınabilir bir mal olarak kabul edilmesinin olanaklı olmaması nedeniyle hırsızlık suçunun unsurlarının da gerçekleşmediği eylemin, suç tarihinde yürürlükte bulunan 765 sayılı TCK'nın 525/b. (5237 sayılı TCK'nın 244/4. maddesine uygun "bilişim sistemini engelleme, bozma verileri yok etme veya değiştirme suretiyle haksız çıkar sağlama") maddesinde öngörülen bilişim suçunu oluşturduğu gözetilmeden, suçun nitelendirilmesinde yanılgıya düşülerek bilişim sistemlerinin aracı olarak kullanılması suretiyle dolandırıcılık suçundan mahkumiyetine karar verilmesi.

diği üzere sanığın fiilinin kül halinde suç tarihinde yürürlükte bulunan 765 sayılı TCK'nın 525/b-2 (5237 sayılı TCK'nın 244/4 maddesine uygun *"bilişim sistemini engelleme, bozma, verileri yok etme veya değiştirme suretiyle haksız çıkar sağlama"*) madde ve fıkrası kapsamında bilişim suçunu oluşturduğu gözetilmeden, suç vasfında hataya düşülerek yazılı şekilde karar verilmesi bozmayı gerektirmiştir.

Görüldüğü üzere, Yargıtay Ceza Dairesi ilk uygulamalarında TCK'nın 244/4 maddesinin sıkça uygulanmasına yol açacak bir yoruma girmişken, aşağıda anlatılacak Yargıtay Ceza Genel Kurulu kararı sonrası, bu görüşten vazgeçmiştir. Konumuz bakımından önemli olması nedeniyle Ceza Genel Kurulu kararının önemli kısımlarının aynen aktarılmasında fayda görülmüştür.

Yargıtay Ceza Genel Kurulu 17/11/2009 gün, 2009/11-293 Esas, 2009/268 karar sayılı kararı: "*Sanık V.E. ile firari S.T. birlikte hareket ederek, daha önceden haksız bir şekilde ele geçirdikleri katılan firmanın internet bankacılık şifresini kullanmak suretiyle, katılanın Şekerbank Ankara Küçükesat Şubesindeki hesabından 10.750 YTL'yı internet kanalı ile Şekerbank-İstanbul Zeytinburnu Şubesinde sanık V. adına açtırdıkları hesaba havale ettikleri ve aynı gün banka şubesinden çektikleri olayda, Yargıtay Ceza Genel Kurulunca çözümü gereken uyuşmazlık, sanığın 765 sayılı TCK'nın 525/b-2 maddesine uyan eyleminin, suç tarihinden sonra yürürlüğe giren 5237 sayılı TCK'nın 244/4 maddesine mi, yoksa 142/2-e maddesine mi, uyan suçu oluşturduğuna ilişkindir.*

244. maddenin 4. fıkrasında yer alan; "Yukarıdaki fıkralarda tanımlanan fiillerin işlenmesi suretiyle kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlamasının başka bir suç oluşturmaması halinde…" biçimdeki ifadeden bu fıkradaki düzenlemenin tali norm niteliğinde olduğu anlaşılmaktadır. Buna göre, bilişim sistemleri aracılığıyla haksız çıkar sağlanmış olması halinde öncelikle Yasada düzenlenmiş olan bilişim sistemlerinin kullanılması suretiyle işlenebilen diğer suçların oluşup oluşmadığı değerlendirilmeli, şayet gerçekleştirilen eylem bu suçlardan hiçbirisinin tanımına uygun değilse, o zaman 244. maddenin 4. fıkrası hükmü uyarınca uygulama yapılmalıdır. …

Bu konu öğretide de tartışmalı olup, bir kısım yazarlar bilişim sistemiyle hukuka aykırı yarar sağlama eylemlerinin, genellikle bilişim suçları veya dolandırıcılık suçu 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 kapsayacağının açıkça belirlenmesi gerektiğini, bilişim sistemini kullanmak suretiyle hırsızlık suçunu düzenleyen hükmün uygulanmasının bir iki örnek dışında olanaksız olduğunu ileri sürmüş; bir kısım yazarlar 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 gerçekleşmediği tartışılmalıdır şeklinde görüş bildirmektedirler…

Bu bilgiler ışığında somut olay değerlendirildiğinde;

"*Sanık V.nin; firari S.T. ile birlikte hareket ederek, daha önceden haksız bir şekilde ele geçirdikleri katılan firmanın internet bankacılık şifresini kullanmak suretiyle, katılanın Şekerbank Ankara Küçükesat Şubesi'ndeki hesabından 10.750 YTL'yı Şekerbank İstanbul Zeytinburnu Şubesi'nde sanık V. adına açtırdıkları hesaba havale edip, aynı gün banka şubesinden çekmek şeklinde gerçekleştirdiği eylemdeki kastı, katılan firmanın banka hesabında bulunan, taşınır nitelikteki parayı bilişim sistemini kullanmak suretiyle kendi banka hesaplarına geçirmeye, katılanın rızasına aykırı olarak malvarlığında azalmaya neden olmaya; başka bir anlatımla var olan veriyi başka bir yere göndermekten 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.*" denmiştir. Yargıtay Ceza Genel Kurulu'nun bu kararı ilgili ceza dairesi tarafından da benimsenmiş ve uygulamada bu görüş üzerinde birlik sağlandığı gözlemlenmiştir.[69]

---

[69] Yrg. 11 CD, 29/03/2010, 2009/23625, 2010/3600 K**:** Katılanın internet bankacılığı şifresini kırarak hesabında bulunan paraları kendisinin ve yakınlarının hesaplarına aktarmak suretiyle haksız menfaat temin eden sanığın eyleminin, ayrıntıları Yargıtay Ceza Genel Kurulu'nun 17.11.2009 gün 193/268 sayılı kararında da açıklandığı üzere TCK'nın 142/2-e maddesindeki bilişim sisteminin kullanılması sure-

Bu konu hakkında tartışılması gereken husus, verinin taşınabilir mal olup olmadığı hususudur. Bir görüşe göre, hırsızlık suçunun konusu taşınır, menkul bir mal olmalıdır. Yani taşınır mal, mevcut ve maddi varlığı olan bir cisim olmalıdır. Verinin sahibinin rızası olmaksızın bilişim sisteminden başka bir yere gönderilmesinde hırsızlık suçunun oluştuğunu söyleyebilmek için verinin taşınır bir mal olarak kabulü zorunludur. Veri ise, 5237 sayılı TCK'nın hiçbir maddesinde taşınabilir bir mal olarak düzenlenmemiş ve tanımlanmamıştır. Bu nedenle veri üzerinden işlenen suçlarda TCK'nın 244/4 maddesi uygulanmalıdır denilmektedir.[70]

Bir başka görüşe göre ise, sisteme ve veriye müdahalenin yapılmış olması sonrasında doğrudan bir yarar sağlanmıyor ve yararın sağlanmasına ilişkin işlem başka bir kişi tarafından gerçekleştiriliyor ise, bu durumda eylemin klasik dolandırıcılık suçu kapsamında değerlendirilmesi gerektiği belirtilmiştir.[71]

Kanaatimizce, sisteme veya veriye yapılan müdahale sonucu doğrudan bir zarar meydana gelmiyorsa, müdahale sonucu veriye bağlı değerler zarar görüyorsa veya zararın doğması için bir kişinin aldatılması gerekiyorsa artık klasik dolandırıcılık veya hırsızlık suçlarının işlendiği kabul edilmelidir. Bu anlamda Yargıtay Ceza Genel Kurulu kararının yerinde olduğunu düşünmekteyiz.

Yargıtay'da oluşan görüş birliği sayesinde, TCK'nın 244/4 maddesinin uygulamada uygulanabilir bir madde olmaktan çıktığı anlaşılmaktadır. Zira TCK'nın 244/4 maddesindeki suçun gerçekleşme şartı olan haksız çıkar sağlanması için, verilere bağlı değerlere müdahale edilmesi gerekmektedir. Uygulamada görülmüştür ki, bilişim sistemleri yoluyla yarar sağlama suçu çoğunlukla, kişilere ait internet bankacılığı şifrelerinin ele geçirilmesinden sonra banka hesaplarının boşaltılması suretiyle işlenmektedir. Yukarıdaki kararda görüldüğü üzere Yargıtay Ceza Genel Kurulu tarafından verinin temsil ettiği değer esas alınıp, bu yolla işlenen suçların TCK'nın 142/2-e maddesi kapsamın-

---

tiyle hırsızlık suçunu oluşturacağı gözetilmeden ve suçun zincirleme biçimde işlenip işlenmediği de tartışılmadan, yazılı şekilde hüküm kurulması.

70 Kubilay Taşdemir, Adı geçen kararda muhalefet görüşü.

71 Ketizmen, *a. g. e.,* s. 179.

da değerlendirilmesi karşısında, TCK'nın 244/4 maddesinin uygulanma imkanının çok sınırlı kaldığı görüşündeyiz.

g. Yaptırım ve Usul Hükümleri

5237 sayılı TCK'nın 244. maddesinin 4. fıkrasında düzenlenen eylemler açısından iki yıldan altı yıla kadar hapis cezası ve beş bin güne kadar adli para cezası öngörülmüştür. Görüldüğü üzere, bu suçu isleyen failler açısından hem adli para cezası hem de hürriyeti bağlayıcı ceza öngörülmüştür. Zira fail, işlediği suç neticesinde haksız bir çıkar sağlamaktadır. Bu sebeple madde metnine göre, hapis cezası ile birlikte adli para cezasına da hükmedilecektir.

Maddede işlenen suç şikâyete bağlı olmayıp, C. Başsavcılığı tarafından doğrudan soruşturma yapılır. Yargılama yapma yetkisi ise asliye ceza mahkemelerine aittir.

SONUÇ

Bilişim ve iletişim teknolojilerinin her ülkenin gelişimi için sunduğu benzersiz olanaklar her geçen gün akıl almaz bir hızla yayılmakta ve artmaktadır. Kısa süreli veri akış kesintilerinin yarattığı olumsuzluklar bile, bilişim sektörünün ne kadar hayatın içerisinde olduğunu göstermektedir. Bilişim sektöründeki gelişmeye paralel olarak, bilişim suçlarında göz ardı edilemeyecek oranda artışların olması, bu suçların doğurduğu zararların da, pek çok adi suçtan daha yıkıcı etkiye neden olmasını sağlamaktadır.

Yıkıcı etkiye sahip bilişim alanında işlenen suçlarla mücadele edebilmek için kabul edilen TCK'nın 244. maddesinin içeriği yukarıda her yönüyle açıklanmaya çalışıldı. Belirtildiği üzere, günümüz şartları ve mukayeseli hukuktaki gelişmelere paralel olarak ayrı bir başlık altında bu düzenlemenin kabul edilmesi önemlidir. Maddenin 1. ve 2. fıkraları, 765 sayılı TCK ile kıyaslandığında, bu düzenlemenin daha açık, kapsayıcı ve isabetli olduğu görülmektedir. Ayrıca bu fıkraların içerdiği cezalar kendi içerisinde bir dengeye sahiptir. Kişilere karşı işlenen suçlar ile banka veya kredi kurumlarına ve kamu kurumlarına yönelik işlenen suçların cezaları arasında ayrıma gidilmesi anlamlıdır.

TCK'nın 244/4 maddesinin uygulaması ise halen tartışılmaya devam edilmektedir. Yargıtay Ceza Genel Kurulu'nun vermiş olduğu kararın yerindeliği sorgulanmaya devam ederken, verilen karar sonrası TCK'nın 244/4 maddesinin uygulanma alanının daraldığının ve TCK'nın 142/2-e ve TCK'nın 158/1-f maddelerinin öncelikle tartışılıp uygulanacakları kanaatinde isek de; gelişen ve değişen teknoloji dünyasında, suçla mücadele için böylesi bir ek maddenin varlığının önemli olduğu düşüncesindeyiz.

TCK'nın 244. maddesinin varlığı pek çok açıdan yerinde olmasına karşın, kanaatimizce TCK'nın 244 maddesi tümüyle Ceza Kanunu'nun *"Malvarlığına Karşı Suçlar"*ın düzenlendiği İkinci Kısım Onuncu Bölüm'de yer almalıydı. Yukarıda anlatıldığı üzere, maddede yazılı suçların koruduğu hukuki yararlar dikkate alındığında, İkinci Kısım Onuncu Bölüm'deki suçlarla örtüştüğü açıktır. Özellikle sanık hakları bakımından, TCK'nın 167, 168 maddelerindeki olanaklardan sanıkların yararlandırılmaması nedeniyle oluşan eşitsiz durumların giderilmesi gerekmektedir.

Bu arada bilişim suçlarıyla mücadele etmek amacıyla yasal düzenleme yapılırken, bu suçların uluslararası boyutları da unutulmamalıdır. Teknolojinin sağladığı olanaklar sayesinde, ülkeler arasında bu suçlar seri şekilde ve iz bırakmadan işlenebilmektedir. Suç örgütlerinin aksine, ülkeler arası işbirliğinin istenen seviyede olmaması, bürokratik kısıtlamalar ve diğer etkenler nedeniyle, suçla tam anlamıyla mücadele edilememektedir. Bu durum ceza kanunundaki maddeleri de işlevsiz kılmaktadır.

Bilişim suçlarıyla uluslar arası alanda mücadele derken ilk akla gelen sözleşme olan Siber Suç Sözleşmesi 2001 yılında yürürlüğe girmiş ise de, o tarihten beri Türkiye bu sözleşmeyi imzalamamış ve sözleşmeye taraf olmamıştır. Dolayısıyla Ceza Kanunu'na 243, 244, 245, 246. maddelerinde yazılı bilişim suçlarına yönelik hükümleri koymak, bu suçlarla her anlamda mücadele edildiğini göstermeye yetmemektedir. Bilişim suçuyla mücadelede samimiyetin ve siyasi iradenin ortaya konması bakımında acilen *"Siber Suç Sözleşmesi"* imzalanmalıdır.

Bilişim suçlarıyla mücadelede uluslar arası alandaki tavır bir tarafa, ülke içindeki sorunlar da ayrıca değerlendirilmelidir. Kolluk güçleri bünyelerinde bilişim suçlarıyla mücadele etmek için özel birimler

kurmuşlarsa da, uygulamada teknik ve fiziki altyapı eksiklikleri nedeniyle faillerin yakalanmasında sorunlar yaşanmaktadır. Bu amaçla kolluk güçlerinin bilişim suçlarıyla ilgili birimleri güçlendirilmeli, teknolojik altyapıları geliştirilmelidir.

Yakalanan şüphelilerin yargılanıp cezalandırılmasında ise, ülkemizin yargı sistemine dair temel yapısal sorunlarla karşılaşılmaktadır. Bu suçları işleyen şüphelileri yargılama yetkisine sahip asliye ceza mahkemeleri, Adalet Bakanlığı Adli Sicil İstatistik Genel Müdürlüğü verilerine göre,[72] 2008 yılında toplam 1.228.068 adet dava dosyasını incelemek zorunda kalmış ve yıl içerisinde 623.436 adet dava dosyasını karara bağlamış, 604.632 adet dava dosyasını ise bir sonraki yıla devretmiştir. Yine 2008 yılı istatistiklerin göre, asliye ceza mahkemelerinde ortalama yargılama süresi 321 gün olup, bu süreye temyiz süreci dahil değildir.

Açıktır ki, bilişim suçlarının mahiyetleri ve yarattıkları olumsuz etkiler nedeniyle daha hızlı bir yargılama sürecine ihtiyaç vardır. Dolayısıyla bu suçları yargılamakla görevli ihtisas mahkemeleri oluşturulmalı, konunun uzmanları ile mahkemeler donatılmalı, mahkemelerin oluşumu için gerekli sayıda hakim ve C. Savcısı ataması yapılmalıdır. Çünkü kolluk güçleri uzmanlaşsa bile, yargılama makamında aynı uzmanlaşma olmazsa, istenen sonuca ulaşmak mümkün olmayacaktır.

KAYNAKLAR

Akbulut, Berrin Bozdoğan, Bilişim Suçları, *Selçuk Üniversitesi Hukuk Fakültesi Dergisi,* C:8, S:1-2,Y:2000.

Akıncı, Hatice/Alıç, A.Emre/Er,Cüneyd "Türk Ceza Kanunu ve Bilişim Suçları", *İnternet ve Hukuk,* İstanbul Bilgi Üniversitesi Yay., Ocak 2004, İstanbul.

Atamer, Yeşim, *İnternet ve Hukuk,* İstanbul Bilgi Üniversitesi Yayınları, İstanbul, 2004.

Bal, Hasan Çebi, *Bilgisayar ve İnternet,* Akademi Yayınevi, Rize, 2001.

[72] http://www.adlisicil.adalet.gov.tr/istatistik_2008/ist_tab.htm Kontrol Tarihi: 01/09/2010.

Çeken, Hüseyin, "Amerika Birleşik Devletlerinde İnternet Yolu İle İşlenen Suçlara İlişkin Düzenlemeler", *Askeri Adalet Dergisi*, Yıl: 30, Sayı: 114, Mayıs 2002.

Çekiç, Burak, "İnternet Aracılığıyla İşlenen Suçlar", Marmara Üniversitesi Sosyal Bilimler Enstitüsü Yayınlanmamış Yüksek Lisans Tezi, İstanbul, 2005.

Değirmenci, Olgun, Bilişim Suçları Alanında Yapılan Çalışmalar ve Bu Suçların Mukayeseli Hukukta Düzenlenişi, *Legal Hukuk Dergisi,* S.11,Y:Kasım 2003.

Değirmenci, Olgun, Bilişim Suçları, Marmara Üniversitesi Sosyal Bilimler Enstitüsü Yayınlanmamış Yüksek Lisans Tezi, İstanbul, 2002.

Demirbaş, Timur, *Ceza Hukuku Genel Hükümler,* Seçkin Yay, Ankara, 2009.

Dönmezer, Sulhi, *Kişilere ve Mala Karşı Cürümler,* İstanbul, Filiz Kitabevi, 12. Baskı.

Dönmezer,Sulhi/Erman,Sahir, *Nazari ve Tatbiki Ceza Hukuku,* Genel Kısım, C: 2, Sulhi Garan matbaası, 1974, İstanbul.

Dülger, Murat Volkan, *Bilişim Suçları,* Seçkin Yay, Ankara, 2004.

Eker, Umut, Türk Ceza Hukuku'nda Bilişim Suçları, *Türkiye Barolar Birliği Dergisi,* S: 62, Ocak-Şubat 2006, Ankara.

Erol, Haydar, *İçtihatlı Türk Ceza Kanunu*, 2000.

Ersoy, Yüksel, Genel Hukuki Koruma Çerçevesinde Bilişim Suçları, *Ankara Üniversitesi Siyasal Bilgiler Fakültesi Dergisi*, C: 49,S:3-4,Y:Haziran 1994.

Hafızoğulları, Zeki, Ceza Hukuku Ders Notları, Ankara 2008, http://www.zekihafizogullari.com/CezaHukuku%20Ders%20Notlari.pdf, Kontrol Tarihi: 29/08/2010.

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

Hafızoğulları, Zeki/Özen, Muharrem, *Türk Ceza Hukuku Genel Hükümler,* Usa Yay, Ankara, 2010.

Hakeri, Hakan, *Ceza Hukuku Genel Hükümler,* Seçkin Yay, Ankara, 2009.

Helvacıoğlu, Aslı Deniz; "Avrupa Konseyi Siber Suç Sözleşmesi Temel Hükümlerinin İncelenmesi", *İnternet ve Hukuk,* Derleyen: Yeşim M. Atamer, Bilgi Üniversitesi Yayınları, 1.Baskı, İstanbul, Ocak 2004.

Karagülmez, Ali, *Bilişim Suçları ve Soruşturma-Kovuşturma Evreleri,* Seçkin Yay, Ankara, 2005.

Kardaş, Ümit, Bilişim Dünyası ve Hukuk, *Karizma Dergisi*, S:13,Y:2003.

Ketizmen, Muammer, *Türk Ceza Hukukunda Bilişim Suçları,* Adalet Yay, 2008, Ankara.

Koca, Mahmut/Üzülmez,İlhan, *Türk Ceza Hukuku Genel Hükümler,* Seçkin Yay, Ankara, 2009.

Kuntalp, Erden, *Kartlı Ödeme Sistemi Hakkında Genel Bilgiler, Kavramlar ve Taraflar Arasındaki Hukuki İlişkiler, Banka ve Kredi Kartları Sempozyumu* (08-10.10.1999), BKM Yay.

Kurt, Levent, *Bilişim Suçları,* Seçkin Yay, Ankara, 2005

Memiş, Tekin, Hukuki Açıdan Kitlelere E-Posta Gönderilmesi, *AÜ-EHFD,* Erzincan, C:V, S:1-4, 2001.

Meran, Necati, *Sahtecilik, Malvarlığı, Bilişim Suçları,* Seçkin Yay, Ankara, 2005.

Önder, Ayhan, *Şahıslara ve Mala Karşı Cürümler ve Bilişim Alanında Suçlar,* Filiz Kitabevi, İstanbul,1994.

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

Özel, Cevat, Bilişim-İnternet Suçları,
http://www.hukukcu.com/bilimsel/kitaplar/bilisim_internetsucları.html, Kontrol Tarihi: 15/08/2010.

Özgenç, İzzet, *Türk Ceza Hukuku Genel Hükümler,* Seçkin Yay, Ankara, 2008.

Özgenç, İzzet, *Türk Ceza Kanunu Gazi Şerhi, Genel Hükümler,* Ankara, 2005.

Öztürk, Bahri/ Erdem, Mustafa Ruhan /Sırma, Özge/ Saygılar, Yasemin, *Ceza Muhakemesi Hukuku Temel Kavramlar,* Turhan Kitabevi, Ankara, 2006.

Sarzana, Carlo, "Bilişim Alanındaki Yeni Teknolojilerin Hukuksal Yansıması İtalya'daki Durum", *İstanbul Hukuk Fakültesi Dergisi*, *Prof. Dr. Türkan Rado'ya Armağan* sayısı, İstanbul 1997, C.LV, S.3.

Schjolberg, Stein, The Legal Framework - Unauthorized Access To Computer Systems, http//www.mosstingrett.no/info/legal.html Kontrol Tarihi: 17/08/2010.

Taşdemir,Kubilay, Bilişim, *Banka ve Kredi Kartlarının Kötüye Kullanılması ve Dolandırıcılık Suçları,* Ankara, 2009.

Taşkın, Şaban Cankat, *Bilişim Suçları,* Beta Yay, Bursa, 2008.
Tezcan, Durmuş/Erdem, Mustafa Ruhan/Önok, Murat*, Teorik ve Pratik Ceza Özel Hukuku*, 5. Baskı, 2007.
Topaloğlu, Mustafa, *Bilişim Hukuku,* Karahan Kitabevi, Adana, 2005.
Toroslu,Nevzat, *Ceza Hukuku Özel Kısım,* Savaş Yay, Ankara, 2009.
Yazıcıoğlu, R. Yılmaz, Yeni Türk Ceza Kanunundaki Bilişim Suçlarının Genel Değerlendirilmesi, *Yeditepe Üniversitesi Hukuk Fakültesi Dergisi,* C:2,S:2,Y:2005.
Yazıcıoğlu, R. Yılmaz, *Bilgisayar Suçları,* Alfa Yay, İstanbul, 1997.
Yazıcıoğlu, R. Yılmaz, Bilişim Suçları Konusunda 2001 Türk Ceza Kanunu Tasarısının Değerlendirilmesi, *Hukuk ve Adalet: Eleştirel Hukuk Dergisi,* İstanbul, Y:1,S:1,Ocak-Mart 2004.
Yenidünya, Caner, "Bilişim Sistemine Hukuka Aykırı Erişim Suçu", *Legal Fikri ve Sınai Haklar Dergisi,* İstanbul, Nisan 2005.
http//www.conventions.coe.int, Kontrol Tarihi: 16/08/2010.
http://www.adlisicil.adalet.gov.tr/istatistik_2008/ist_tab.htm Kontrol Tarihi: 01/09/2010.