ÇANKAYA ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
KAMU HUKUKU ANABİLİM DALI
CEZA VE CEZA USUL HUKUKU BİLİM DALI

5237 SAYILI
TÜRK CEZA KANUNU'NDA BİLİŞİM SUÇLARI

YÜKSEKLİSANS TEZİ

HÜDAVERDİ UÇAR

ANKARA 2014

Tez Başlığı : **5237 sayılı Türk Ceza Kanunu'nda Bilişim Suçları**

Tezi Hazırlayan : **UÇAR, Hüdaverdi**

Sosyal Bilimler Enstitüsü Onayı:

Prof. Dr. Mehmet YAZICI
Sosyal Bilimler Enstitüsü Müdürü

Bu tezin yüksek lisans derecesi elde etmek için gerekli koşulları sağladığını onaylarım.

Prof.Dr. Hamdi MOLLAMAHMUTOĞLU
Kamu Hukuk Anabilim Dalı Başkanı

Bu tez, tarafımdan incelenmiş olup Yüksek Lisans Tezi olarak uygun bulunmuştur.

Prof. Dr. Doğan SOYASLAN
Tez Danışman

Tez sınav Tarihi: 26.06.2014

Tez Jüri Üyeleri :

Prof. Dr. Doğan SOYASLAN (Çankaya Üniv.) .....

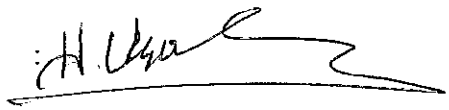
Doç. Dr. Devrim GÜNGÖR (Ankara Üniv.) .....

Yrd. Doç. Dr. Elvan KEÇELİOĞLU (Çankaya Üniv.) .....

ÇANKAYA ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ MÜDÜRLÜĞÜNE

Bu belge ile, bu tezdeki bütün bilgilerin akademik kurallara ve etik davranış ilkelerine uygun olarak toplanıp sunulduğunu beyan ederim. Bu kural ve ilkelerin gereği olarak, tez çalışmamda bana ait olmayan tüm veri, düşünce ve sonuçları bilimsel etik kurallar gözeterek ifade ettiğimi ve kaynağını gösterdiğimi ayrıca beyan ederim.

Adı Soyadı : Hüdaverdi UÇAR

İmza : 

Tarih : 26.06.2014

ÖZET

5237 SAYILI

Türk Ceza Kanunu'nda Bilişim Suçları

UÇAR, Hüdaverdi

Yüksek Lisans Tezi

Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı

Tez Danışmanı, Prof Dr. Doğan SOYASLAN

Haziran 2014, 139 sayfa

Günümüzde teknoloji çok ilerlemiştir, bu ilerleme teknolojinin dalları diyebileceğimiz bilgisayar ve iletişimde de kendini göstermiş, tarihi süreç içerisinde çok daha ileri ve geniş kapsamlı sonuçlar ortaya çıkmasına zemin hazırlamıştır. Özellikle internetin yaygın olarak kullanılmaya başlanması eğitimden sağlığa, ticaretten sanayiye, kamu sektöründen özel sektöre varıncaya kadar, iş ve sosyal hayatımızda, aynı şekilde özel hayatımızdaki ilişkilerimizde yeni bir çığır açmıştır.

Bu teknolojik gelişmelerin insanlar tarafından kullanılmaya başlanmasıyla toplumlara büyük yararlar sağlandığı gibi, beraberinde birtakım problemleri de getirdiği bilinmektedir. Bu problemlerin en büyüğü suç işlenmesinin kolaylaşması olmuştur. Çünkü İnsanlar suç işlerken teknolojik alanlardan yararlanma eğilimine girmeye başlamışlardır. Böylelikle teknolojinin bir nimeti olan bilişim sistemleri insanların hizmetine sunulunca kötü kullanımlarla beraber yeni suç tipleri olan 'bilişim suçları' ortaya çıkmaya başlamıştır. Bu suçların yanında mevcut bazı suç tipleri de bilişim sistemlerinin kullanılması suretiyle işlenmeye başlanmıştır. Çalışmamızda Türk hukukunda ilk kez 5237 sayılı Türk Ceza Kanunu ile düzenlenen bilişim suçları incelenmiştir.

Yüksek lisans tezi olarak hazırladığım bu çalışmada tez danışmanlığımı yapan, yardım ve desteklerini esirgemeyen, değerli görüş ve önerileri ile katkıda

bulunup beni yönlendiren, saygıdeğer hocam Prof. Dr. Doğan SOYASLAN'a şükranlarımı sunarım.

Anahtar Kelimeler: Bilgisayar, bilişim, suç, ceza, veri, kişisel veri, haberleşme,

ABSTRACT

5237 SAYILI

Türk Ceza Kanunu'nda Bilişim Suçları

UÇAR, Hüdaverdi

Master Thesis

The Institute of Social Sciences, Department of Public Law

Thesis Supervisor: Prof. Dr. Doğan SOYASLAN

June, 2014, 139 pages

At the present time, the technology has progressed a lot. This progress has shwn its impacts on computing and communnication leading much further and comprehensive consequences in the historical process. Especially, the beginning of vast usage of the Internet has pioneered new paths in our relations in business, social and private life in the areas from education to health, from trade, to industry, from public sector to private sectors.

İt is clearly known that starting to use these progresses provided a great benefit to society as well as it has caused certain problems. The biggest of these problems is that committing crimes has been easier. People have tended to make use of the technology while committing crimes. Hereby, the term "Cyber Crimes" has emerged after the abuse of information system which was submitted to the service of humanity as a part of technological developments. Alongside of this type of crime, other types of crimes have started to be commited with the use of İnformation Systems. In our study, Cyber Crimes have been examined which was orginezed by the Turkish Penal Code numbered 5237.

I would like to thank to my dear advisor, Prof. Dr. Doğan SOSYASLAN who supervised my studies in my MA. Thesis; supported and helped in my research; guided and contributed to me with his valuable ideas and suggestions.

Keywords: Computer, informatics, crime, penalty, data, private data, communications

İÇİNDEKİLER

İKİNCİ BÖLÜM

BİLİŞİM SUÇLARININ TEKNİK ANLAMDA İSLENME ŞEKİLLERİ

RESİMLER DİZİNİ

KISALTMALAR

AİHS	: Avrupa İnsan Hakları Sözleşmesi
Bkz.	: Bakınız
C	: Cilt
CD.	: Ceza Dairesi
E.	: Esas No
EİK	: Elektronik İmza Kanunu
f.	: fıkra
FSEK	: Fikir Ve Sanat Eserleri Kanunu
K.	: Karar No
m.	: madde
s	: sayfa
S	: Sayı
SSD	: Siber Suçlarla Mücadele Daire Başkanlığı
T.	: Tarih
T.C.K.	: Türk Ceza Kanunu
TDK	: Türk Dil Kurumu
UYAP	: Ulusal Yargı Ağı Projesi
Vb.	: ve benzeri
Vd.	: ve devamı
Y.	: Yargıtay
YCGK	: Yargıtay Ceza Genel Kurulu
Y.T.C.K.	: Yeni Türk Ceza Kanunu

GİRİŞ

Günümüzde teknoloji çok ilerlemiştir, bu ilerleme teknolojinin dalları diyebileceğimiz bilgisayar ve iletişimde de kendini göstermiş, tarihi süreç içerisinde çok daha ileri ve geniş kapsamlı sonuçlar ortaya çıkmasına zemin hazırlamıştır. Özellikle internetin yaygın olarak kullanılmaya başlanması eğitimden sağlığa, ticaretten sanayiye, kamu sektöründen özel sektöre varıncaya kadar, iş ve sosyal hayatımızda, keza özel hayatımızdaki ilişkilerimizde yeni bir çığır açmıştır.

Bu teknolojik gelişmelerin insanlar tarafından kullanılmaya başlanmasıyla toplumlara büyük yararlar sağlandığı gibi, beraberinde birtakım problemleri de getirdiği bilinmektedir. Bu problemlerin en büyüğü suç işlenmesinin kolaylaşması olmuştur. Çünkü İnsanlar suç işlerken teknolojik alanlardan yararlanma eğilimine girmeye başlamışlardır. Böylelikle teknolojinin bir nimeti olan bilişim sistemleri insanların hizmetine sunulunca kötü kullanımlarla beraber yeni suç tipleri olan 'bilişim suçları' ortaya çıkmaya başlamıştır. Bu suçların yanında mevcut suç tipleri olan hakaret, hırsızlık, dolandırıcılık, özel hayatın gizliliği ve müstehcenlik gibi suçlar da bilişim sistemlerinin kullanılması suretiyle işlenmeye başlanmıştır.

İşte bu nedenlerle, Türk Ceza Kanunumuz (T.C.K.) bu gelişmelere kayıtsız kalamamıştır. Bilindiği gibi 5237 sayılı T.C.K.'da bilişim suçlarına ayrı bir bölüm ayrılmakla birlikte, klasik suç tiplerinin yer aldığı bölümlerde de (hırsızlık ve dolandırıcılık suçlarında olduğu gibi) bilişim suçlarına ilişkin bazı düzenlemelere yer verilmiştir.

Bilişim suçları faili çok zor belirlenen suçlardır. Fail çoğu zaman hep bir adım öndedir. Faili bulmak büyük uğraş ve uzun zaman gerektirir. Bu nedenle bu suçlar sayesinde birçok insana leke vurmak kolaydır. Görüntü ve ses kayıtları gerçek dahi olsa hukuka aykırı şekilde kullanıldığında insanın özel hayatını örseleyebilmektedir. Hiç kimsenin bir başkasını özel hayatını gayri ahlaki göstermeye hakkı yoktur. Son dönemlerde ülkemizde siyasetçilere özel görüntü ve ses kayıtlarının internette yayınlanarak saldırılarda bulunulduğuna da şahit oluyoruz. Yani bu suçlar sayesinde ülkelerin hatta dünyanın gündemi değişebilmektedir. Kim olursa olsun herkesin özel hayatı kutsaldır, insanın özelini ihlal eden kişiler

cezalandırılmalıdır. Bu suçlarla ilgili araştırmalara daha çok önem verilmeli ve üzerinde durulmalıdır. Bu nedenlerle araştırmamızın konusunu "Türk Ceza Kanunu'nda Düzenlenen Bilişim Suçları" olarak seçmiş bulunmaktayız.

Çalışmamızın birinci bölümünde, bilişim, bilişim sistemi, adli bilişim ve bunların ceza hukuku ile olan ilişkisi hakkında temel bilgiler verilecek, ikinci bölümünde ise bilişim suçlarında fail ve mağdur yapısı ve suçun işlenme şekillerine değinilecektir.

Üçüncü bölüme geldiğimizde, asıl konumuz olan 5237 sayılı Türk Ceza Kanunu'ndaki bilişim suçlarına geçmeden, 765 sayılı Türk Ceza Kanunu'nda düzenlenen bilişim suçlarına değinmeye çalışacağız. Çünkü, bilişim suçları açısından ceza kanunlarındaki lehe ve aleyhe kanunun belirlenebilmesi için ve 5237 sayılı Türk Ceza Kanunu'nun bilişim suçlarına ilişkin düzenlemeleri daha iyi anlayabilmek için 765 sayılı Türk Ceza Kanunu'ndaki bilişim suçlarına ilişkin mülga düzenlemeleri bilmek gerekir. Ardından da asıl çalışma konumuz olan 5237 sayılı Türk Ceza Kanunu'ndaki bilişim suçlarına ayrıntılı olarak değinilecektir.

5237 sayılı Türk Ceza Kanunu'ndaki bilişim suçları da çalışmamız da aynı bölüm içerisinde üçe bölünerek incelenecektir. 5237 sayılı T.C.K.'da Onuncu Bölümde "Bilişim Alanında Suçlar" başlığı altında bulunan bilişim suçlarına, Dokuzuncu Bölümde "Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar" başlığı altında düzenlenen bilişim suçlarına ve T.C.K.'da bilişim sistemleri aracılığıyla işlenebilecek diğer suç tipleri olan; bilişim sisteminin kullanılması yoluyla işlenen hırsızlık, bilişim sistemlerinin kullanılması yoluyla işlenen dolandırıcılık, haberleşmenin engellenmesi, hakaret, müstehcenlik suçu kumar oynanması için yer ve imkân sağlama suçlarına ayrı ayrı değinilecektir.

Çalışmamızda, doktrindeki görüşler, Yargıtay kararları ile görüşlerimizle tüm konular açıklanmaya çalışılacaktır.

BİRİNCİ BÖLÜM

BİLİŞİM, BİLİŞİM SİSTEMİ VE HUKUK İLİŞKİSİ HAKKINDA TEMEL BİLGİLER

I. BİLGİSAYAR

Türkçe'de "bilgi" ve "sayar" kelimelerinin birleştirilmesiyle meydana getirilen bilgisayar kelimesi Güncel Türkçe Sözlüğü'nde, çok sayıda aritmetiksel veya mantıksal işlemlerden oluşan bir işi, önceden verilmiş bir programa göre yapıp sonuçlandıran elektronik araç, elektronik beyin[1] anlamına; Bilişim Terimleri Sözlüğü'nde ise, çok sayıda aritmetiksel ya da mantıksal işlemlerden oluşan bir işi, çalışması sırasında bir işletmenin işe karışması gerekmeksizin, önceden verilmiş bir izlenceye göre, özdevimli olarak yürüten bir veri işleyici bir bilgisayar dizgesi elektronik ve mekanik birimlerden oluşan donanım ile bu donanım birimlerini ya da kaynakları istenen işlere yöneltip verimli bir çalışma düzeni içerisinde kullanabilmek için gerekli tüm izlencelerden ve veri yapılarından oluşan yazılım öğeleri[2] anlamına gelmektedir. Basit bir tanım yapmamız gerekirse kendisine verdiğimiz bilgileri istediğimizde saklayabilen, istediğimizde geri verebilen cihaza bilgisayar denir. Bir başka tanımla ise bilgisayar; belleğindeki programa uygun olarak aritmetik ve mantıksal işlemleri yapabilen, karar verebilen, yürüteceği programı ve işleyeceği verileri ezberinde tutabilen, çevresiyle etkileşimde bulunabilen araçları ifade etmektedir[3].

Computer kelimesini "bilgisayar" olarak dilimize yerleştiren ise Prof. Dr. Aydın Köksal'dır. Yaptığımız araştırmalara göre bilgisayar kelimesi 1970'e kadar çok yaygın olmayan bu kelime 1960'ların sonlarına doğru bilgisayar olarak kullanmaya ve yaygınlaşmaya başlamıştır. Çoğu ülke computer kelimesi kullanırken bizim bu denli güzel ve tanımına uygun kelimeyi bulmamız ülkemiz ve dilimiz için bir değerdir diyebiliriz.

1 Güncel Türkçe Sözlük, http://tdkterim.gov.tr/bts/

2 Bilişim Terimleri Sözlüğü, http://tdkterim.gov.tr/bts/

3 http://www.adalı.net/?page_id=1229 ; (Erişim tarihi: 01.08.2013)

A. Bilgisayarın Yapısı

Bilgisayarlar, onları diğer tüm teknolojik araçlara üstün kılan iki özelliğe sahiptir. Birincisi, yazılım programlarının; ikincisi ise donanım birimlerinin (çevre birimleri) ilâve edilebilme özeliğine sahip olmasıdır. Anlaşılmaktadır ki bilgisayar; donanım (hardware) ve yazılım (software) olmak üzere iki bileşenden oluşmaktadır. Bilgisayarda bu bileşenler kullanılarak hayal edilen her şey gerçekleştirilebilmesi teknik olarak mümkündür diyebiliriz. Şimdi donanım ve yazılım kavramlarını kısa kısa açıklamaya çalışarak araştırmamıza devam edelim.

a. Donanım

Donanım, bilgisayarın fiziki bileşenlerine verilen isimdir.

1. Donanım Birimleri

- Giriş birimi; bilgisayara dış ortamdan veri girilmesini sağlayan birimlerdir.
- Çıkış birimi; bilgisayar ortamında işlenen verilerin dış ortama aktarılmasını sağlayan birimlerdir.
- Merkezi işlem birimi (CPU); bilgisayarın beynidir. Bilgisayar içindeki bütün işlemler CPU'da yapılır. Yani giriş biriminden girilen veriler CPU içinde işlenir ve çıkış birimine aktarılır.
- Bellek; bilgilerin kalıcı ya da geçici olarak saklandığı ortamlardır.
- RAM (Random Access Memory) bellek; rastgele erişilebilir bellektir. Bu belleğe kalıcı olmayan bellek de denir. Elektrik kesildiğinde ya da bilgisayar kapatıldığında ram bellekteki veriler silinir. Ram bellek, ana bellek olarak da isimlendirilir.
- ROM (Read Only Memory) bellek; sadece okunabilir bellektir. Bu bellek üzerindeki bilgiler üretici firma tarafından yazılır. Kullanıcı tarafından üzerinde bulunan bilgiler değiştirilemez. Üzerinde bilgisayarın açılması için gerekli olan program vardır. Bu program bilgisayar açılırken temel giriş, çıkış birimlerini kontrol eder.
- Depolama birimi (Yan Bellek); kalıcı bellektir. Üzerine kaydedilen bilgiler elektrik kesildiğinde ya da bilgisayar kapatıldığında silinmez. Sabit disk (Harddisk) , disket, CD, data kartuşları depolama birimine örnek olarak gösterilebilir.

- Kontrol birimi; bilgisayarda yapılan tüm işlemleri kontrol eden birimdir. Yapılan işlemlerin sağlıklı ve düzgün bir şekilde yapılmasından sorumludur. Kontrol Birimi (CU-Control Unit) bir şirketteki müdür olarak düşünülebilir.
- Aritmetik ve mantık birimi (ALU-Aritmetical Logical Unit); 4 işlem ve mantıksal karşılaştırma işlemleri ALU tarafından yapılır.

2. Bilgisayarın Ana Donanım Birimleri

- Ana kart; ana kart (Mainboard), diğer bütün kartların üzerine takıldığı karttır. Bilgisayar içindeki diğer bütün donanım birimleri ana kart üzerinde toplanır ve ana kart üzerindeki veri yolları vasıtasıyla haberleşir. Ana kart üzerinde her donanım biriminin takılabileceği bir yer mevcuttur.
- İşlemci (CPU); bilgisayar içindeki tüm aritmetiksel ve mantıksal işlemlerinin yapıldığı ve tüm işlemlerin kontrol edildiği bölümdür. Bilgisayarın asıl yükünü çeken beyin olarak düşünülebilir. Bilgisayarın hızını etkileyen en önemli parçadır. İşlemci hızı MHZ (Mega hertz) olarak ölçülür. 1 Mhz= 1.000.000 işlem/saniye"dir. Yani 1 Mhz hızındaki bir işlemci saniyede 1 milyon işlem yapar.
- RAM; bilgisayarın işlem yaparken kullandığı bellektir (hafıza). Bilgisayarın hızını etkileyen diğer bir parçadır.
- Sabit disk (Harddisk); bilgisayarın içindeki depolama birimidir. Sabit disk manyetik bir ortam olan plakalardan oluşur. Bu plakalar bir motora bağlıdır ve sürekli dönerler. Bu dönüş esnasında okuma yazma kafası bu plakalar üzerine veri yazar yada okur.
- Kapasite ölçüm birimleri; küçükten büyüğe Bit, Byte (Bayt), KB(Kilo Byte), MB (Mega Byte), GB (Giga Byte), TB (Tera Byte) şeklindedir. Bit; en küçük birim bit"tir. Bilgisayar içinde karakterler ikilik sayı siteminde 8 haneli bir sayıyla ifade edilir. İşte bu sayının her bir basamağına 1 byte denir. Byte (Bayt); bilgisayar içinde her karakter aynı zamanda 1 Byte'tır. 1024 byte=1 kilo byte; 1024 kilo byte=1 mega byte; 1024 mega byte=1 gbyte; 1024 giga byte=1 tera byte'tır
- Ekran kartı; bilgisayarın kasasıyla monitör arasında köprü vazifesi görür. Bilgisayar içinde yapılan işlemlerin sonucu monitöre ekran kartı vasıtasıyla aktarılır.

3. Çevre Birimleri

- Disket (Floppy) sürücü ve disket; disket sürücü disket üzerinde okuma ve yazma işlemi yapan birimdir. Disket ise kapasitesi düşük olan depolama birimidir. Disketler verilerin bir bilgisayarda başka bilgisayara taşınmasında kolaylık sağlar.

Ayrıca disketler üzerinde yazmaya karşı koruma (Protect) vardır. Günümüzde artık yok denecek kadar azalmıştır.

- CD-ROM; veri depolamak için kullanılan yan bellek birimidir. Disketlere göre kapasiteleri çok yüksektir. CD içindeki bilgiler CD-ROM sürücüler vasıtasıyla okunabilir. CD üzerine yazma işlemi CD-Writer aracılığıyla yapılır. CD üzerine bilgiler bir kereye mahsus olmak üzere yazılır ve kullanıcı CD-ROM sürücü vasıtasıyla bu bilgileri sadece okuyabilir.
- Modem; coğrafi olarak uzak mesafelerdeki bilgisayarlar arasında iletişim kurmak için kullanılır. İnternet'e bağlanmak için mutlaka modem gereklidir. Modem uzak mesafelerdeki bilgisayarları telefon hattı vasıtasıyla birbirine bağlar. İki tür modem vardır. Bunlar; dahili (Internal) ve harici (External)dir.
- Yazıcı (Printer); bilgisayar ortamındaki bilgileri kağıt üzerine aktarmak için kullanılır.
- Tarayıcı (Scanner); kağıt üzerindeki resim, grafik, tablo, yazı gibi bilgileri bilgisayar ortamına aktarmak için kullanılır.
- Güç Kaynağı (Power Supply); bilgisayara güç veren birimdir. Bilgisayar içindeki bütün parçalara elektrik verir.
- Fare (Mouse); ekran üzerinde simgelere daha kolay ulaşmamızı sağlayan klavyenin bazı görevlerini yapabilen kolaylaştırıcı bir aygıttır. Daha çok Windows İşletim Sisteminde kullanılan birimdir.
- Klavye; F ve Q olmak üzere iki tür klavye vardır. F klavye Türkçe (daktilo) klavyedir. Q klavyenin de Türkçe uyarlanmış hali vardır ve ülkemizde çoğunluk tarafından bu klavye tercih edilmektedir
- Monitör; bilgisayarda yapılan işlemlerin izlendiği birimdir. Monitörle bilgisayar arasındaki iletişimi ekran kartı sağlar. Yaygın olarak 12, 14, 15, 17, 19 ve 21 inçlik (1 inç = 2,54 cm) boyuta sahip renkli ekranlar kullanılmaktadır. Bu boyut ekranın bir köşesinde köşeden diğer köşesine olan uzaklıktır.

b. Yazılım

Yazılım; bilgisayar donanımının bazı işlevleri yerine getirebilmesi için belirli bir mantık çerçevesinde yazılmış komut topluluklarına yani programlara yazılım denmektedir. Sistem yazılımları ve uygulama yazılımları olmak üzere iki tür yazılım vardır.

1. Sistem Yazılımları

Sistem yazılımı (system software) olarak adlandırılan gruba, kullanıcıların veri hazırlama, uygulama yazılımı geliştirme ve çalıştırma amacıyla kullandıkları programlar girer. Bu gruptaki programlar genellikle konunun uzmanı olan yazılım şirketleri ya da bilgisayarı üreten şirket tarafından hazırlanmışlardır. En bilinen sistem yazılımı işletim sistemi (operating system) adı ile anılır. İşletim sistemi, bilgisayar donanımının verimli ve kolay kullanılmasını sağlamak amacıyla hazırlanan programlardan oluşur. Genellikle bilgisayar ilk açıldığında, işletim sistemini oluşturan programlar otomatik olarak çalışırlar[4].

Bilgisayar, işletim sistemi sayesinde açılır ve onun sayesinde dosya kopyalama, yazı yazma, resim yapma, dosya silme, yazıcıdan çıktı alma gibi işlemler yapılır. İşletim sistemi çekirdek yazılımdır. Diğer bütün programlar işletim sistemi üzerinde çalışır. İki tür işletim sistemi vardır: Çok kullanıcılı işletim sistemleri; aynı anda birden fazla kişinin bir ağ ortamında kullandığı işletim sistemleridir. Linux, Unix, Novel, Windows NT, Windows 2000 gibi işletim sistemleri çok kullanıcılıdır.

Tek kullanıcılı işletim sistemleri; aynı anda sadece bir kişinin kullanımına izin veren işletim sistemleridir. Dos, Windows 3.1, Win 95, Win 98, Win Me, Win XP Home Edition gibi işletim sistemleri tek kullanıcılı işletim sistemleridir.

2. Uygulama Yazılımları

Uygulama yazılımı (application software), kullanıcıların kendi özel işlerini bilgisayar donanımına yaptırmak amacıyla, sistem yazılımını kullanarak hazırlayıp çalıştırdıkları her türlü programı kapsar[5]. Örneğin; günlük hayatta yaptığımız yazı yazma, resim yapma, faks çekme, hesap işleri gibi işleri bilgisayar ortamında yapmanızı sağlayan ve işinizi kolaylaştıran programlardır.

c. Bilgisayar Ağları (Network)

Birden fazla bilgisayarın bir kablo aracılığıyla birbirine bağlanmasıyla oluşan yapıya bilgisayar ağı (network) denir. Bilgisayarların birbirine bağlanarak bir ağ oluşturmanın amacı yapılan işlemlerde hız, ekonomiklik ve kolaylık sağlamaktır. LAN (Local Area Network-Yerel alan agı) ile WAN (Wide Area Network-Geniş Alan Ağı) olmak üzere iki tür bilgisayar ağı vardır.

4 Aslan, Hüryaşa, "Bilgisayar Yazılımı,Ünite 3" s.39 http://w2.anadolu.edu.tr/aos/kitap/IOLTP/2276/unite03.pdf

5 Aslan, Hüryaşa, s.39

1. LAN (Local Area Network-Yerel alan ağı)

LAN (Local Area Network-Yerel Alan Ağı), birbirine yakın mesafedeki bilgisayarların bir kablo ve ağ kartı (Ethernet kartı) aracılığıyla bağlanmasıyla oluşan bilgisayar ağlarıdır.

2. WAN (Wide Area Network-Geniş Alan Ağı)

WAN (Wide Area Network-Geniş Alan Ağları), coğrafi olarak uzak mesafelerdeki bilgisayarları birbirine bağlamak için kullanılır.

B. Veri, Kişisel Veri Kavramları

Veri, İngilizcede "data" sözcüğünün karşılığı olarak dilimizde kullanılmaktadır. Veri, bilgilerin belirli bir formata dönüştürülmüş halidir. Başka bir ifade ile veri, olgu, kavram ya da komutların, iletişim, yorum ve işlem için elverişli biçimsel ve uzlaşımsal bir gösterimi, elverişlilik, kişiler ya da özdevimli makinelerle iletişim, yorum ya da işleme uygunluk biçiminde düşünülebilir[6]. Veri soyut bir kavramdır.

Veri, Avrupa Konseyi Siber Suç Sözleşmesinin 1. maddesine göre ise bir bilgisayar sisteminin belli bir işlevini yerine getirilmesini sağlayan yazılımlar da dahil olmak üzere, bir bilgisayar sisteminde işlenmeye uygun nitelikteki her türlü bilgiyi ifade eder. 5651 sayılı Kanun I-k bendinde ise veri bilgisayar tarafından üzerinde işlem yapılabilen her türlü değer olarak tanımlanmaktadır.[7]

Kişisel veri Avrupa Birliğince kabul edilen 24.10.1995 tarihli Avrupa Topluluğu Veri Koruma Yönergesinin 2. maddesinde, bir gerçek kişi hakkında olabilen ve belirleyici olabilecek her türlü bilgi şeklinde ifade edilmiştir[8].

C. Program

Program, bir bilgisayarın istenilen şekilde çalışmasına yardımcı olmak, kullanıcı ile bilgisayar arasında köprü vazifesi görmek, bilgisayarın fiziksel çalışmasının kullanıcı tarafından denetlenmesine ve istenilen şekilde çalışmasına, müdahale edilmesine olanak vermek, bilgisayarın çalışmasının sonuçlarından kullanıcının faydalanmasını sağlamak üzere sistematik olarak bir araya getirilmiş veri dizileridir[9].

6 Bilişim Terimleri Sözlüğü, http://tdkterim.gov.tr/bts/

7 Özen Muharrem/ Baştürk İhsan, "Bilişim – İnternet Ve Ceza Hukuku", Adalet Yayınevi, Ankara, 2011, s.132

8 Başalp Nilgün, "Kişisel Verilerin Korunması Ve Saklanması", Yetkin Yayınevi, Ankara, 2004

9 Yazicioglu Yılmaz, "Bilgisayar Suçları, Krimonolojik Sosyolojik ve Hukuki Boyutları ile", İstanbul, 1997, s. 30,31

II. İNTERNET

A. Genel Olarak

İnternet, bilgisayar ağlarının birbirine bağlanması sonucu ortaya çıkan, herhangi bir sınırlaması ve yöneticisi olmayan uluslararası bilgi iletişim ağı sistemini ifade etmektedir[10]. Amerikan Yüksek Mahkemeleri kararlarına göre, *"internet, birbirleri ile bağlı bulunan bilgisayarlardan oluşan uluslararası ağdır. İnternet, bireylerin dünya çapında haberleşmesi için tamamen yeni ve benzeri olmayan bir ortamdır[11]"*

İnternetin Türkçe kelime manası ise "genel ağ" dır. Bu ağ sistemi aracılığıyla milyonlarca bilgisayarın birbirleri ile ilişki kurması sonucu insanlar haberleşebilmekte ve bilgi alışverişinde bulunabilmektedir. Günümüzde internet, bilgiye en kolay ve en hızlı şekilde ulaşmanın yolu olmuştur.

Bilgisayarların birbirleriyle veri alışverişi ve ortak iş yapacak biçimde bağlanması ile oluşan bilgisayar ağları, bilgisayarların potansiyel gücünü inanılmaz boyutlara çıkarmıştır. Böyle ağların toplamından oluşan internet, bilgiye ve bilgisayar kaynaklarına dünya çapında erişimi sağlamaktadır. 1990 yılından itibaren dünya çapında yaygınlaşmaya başlayan internet, kısa sürede hızlı gelişme göstermiştir. İnternete bağlanma maliyeti düşerek, güçlü ve kullanımı kolay programlar internet vasıtasıyla iletişim kurmayı ve bilgi erişimini ve yayıncılığı herkese açık bir imkân haline getirmiştir. Bir internet uygulaması olan World Wide Web, multi-medya verilerin (metin, ses, resim, film) tek bir sistemle bütünleşik bir biçimde yayılmasına ve erişilmesine imkân vermesiyle, internet kullanıcı sayısında ve İnternette yayınlanan bilgi miktarında patlamaya yol açmıştır[12].

B. İnternetin Tarihsel Gelişimi

20. yüzyılda dünya çapında yeni bir yapı sağlayan internet, iletişimde yeni bir çığır açmıştır. Ancak pek tabiidir ki internet ağı içerisinde yer alan bilgisayarların sorunsuz veri iletişiminde bulunabilmeleri, bazı kurallara uyulması gerekmektedir. Bu kurallar dünyada geçerli olan TCP/IP (Transmission Control Protocol/Internet Protocol) ile belirlenmiştir. TCP/IP protokolü ile dünya üzerindeki milyonlarca bilgisayarın iletişim kurmalarını sağlanmıştır[13]. Ortak bir anlaşma dili olarak

10 Güncel Türkçe Sözlük http://tdkterim.gov.tr/bts/

11 Sirabaşi Volkan, "İnternet ve Radyo-Televizyon Aracılığıyla Kişilik Haklarına Tecavüz (İnternet Rejimi)", Adalet Yayınevi, Ankara, 2003 s.52

12 Yayci Esra, "Bilişim Suçları", Yayımlanmış Master Tezi, Gazi Üniversitesi Sosyal Bilimler Enstitüsü, Ankara, 2007 s.14

13 Sinar Hasan, "İnternet ve Ceza Hukuku", (İstanbul, 2001), s.24

tanımlanabilir. Günümüzde TCP/IP protokolü dışında da protokoller kullanılmakla birlikte pek de rağbet görmemektedirler. Bu sebeple internet ağında evrensel olarak benimsenmiş tek ve genel geçerliliği olan ortak anlaşma dili, TCP/IP protokolüdür[14].

İnternetin gelişmesindeki son aşama ise World-Wide-Web (www)'in geliştirilmesidir. Ses, görüntü ve metin gibi farklı formatta olan bilgilerin göz atıcı (browser) kullanılarak ulaşıldığı internet ortamıdır[15]. İnternet kullanıcılarının en çok kullandığı platformdur. İnternette her sayfanın bir adresi vardır. Örneğin http://www.cankaya.edu.tr Bu adreste iki kısım vardır *http* (Hypertext Transmission Protocol) ve *www* (World-Wide-Web). HTML adı verilen bu işaretleme dili sayesinde işlev kazanırlar. HTTP (Hyper Text Transfer Protocol) adı verilen protokol, internet üzerinde HTML işaret dili kullanılarak meydana getirilen web sayfalarının aktarılabilmesini sağlar[16]. Bir web adresinde o adresi kullanan kuruluşun adı genellikle yer alır. İnternete bağlı bulunan her bilgisayarın bir adresi olduğu gibi her kuruluşunda bir adresi vardır. Bunlar; *com, edu, gov, org, mil, net* olabilir.

Bu internet adreslerinin gruplandırılmasında kullanılan kısaltmaların anlamları aşağıdaki gibidir.

com : Ticari kuruluşlar
org : Sivil toplum kuruluşları
edu : Eğitim kuruluşları
ac : Akademik kuruluşlar
gov : Hükümet kuruluşları
int : Uluslar arası kuruluşlar
mil : Askeri kuruluşlar
net : Kendi özel ağları olan ve bunu dış kullanıma sunabilen gruplar

İnternet şu anda suçların işlendiği alan haline de gelmiştir. Birçok suç türü internet ortamında işlenilebilmektedir. Araştırmamızın ileriki bölümlerinde bu konu işlenecektir.

III. BİLİŞİM VE BİLİŞİM SİSTEMİ

Bilişim, kişilerin teknik, ekonomik, sosyal, kültürel alanlar başta olmak üzere her türlü alandaki iletişimlerinde kullandıkları ve bilimin temeli olan bilginin,

14 Karagülmez Ali, "Bilişim Suçları Ve Soruşturma – Kovuşturma Evreleri", Seçkin Yayınevi, Ankara, 2011, s.40

15 Özen Muharrem/ Baştürk İhsan, s.23,24

16 Özen Muharrem/ Baştürk İhsan, s.24

özellikle elektronik, elektromanyetik ve benzeri ortamları kullanılarak düzenli ve rasyonel bir biçimde işlenmesi bilimi olarak tarif edilmektedir[17].

Bilişim Terimleri Sözlüğünde ise bilişim kelimesi; "İnsanoğlunun teknik, ekonomik ve toplumsal alanlardaki iletişiminde kullandığı ve bilimin dayanağı olan bilginin, özellikle elektronik makineler aracılığıyla, düzenli ve ussal biçimde işlenmesi bilimi. Bilgi olgusunu, bilgi saklama, erişim dizgeleri, bilginin işlenmesi, aktarılması ve kullanılması yöntemlerini, toplum ve insanlık yararı gözeterek inceleyen uygulamalı bilim dalı."[18] olarak açıklanmaktadır.

Yargıtay bilişim sistemini; verileri toplayıp yerleştirdikten sonra bunları otomatik işlemlere tabi tutma olanağını veren manyetik sistemler olarak tanımlamıştır. [19]

Görülmektedir ki, bilişim, bilgisayardaki bilgileri akademik ve mesleki disipline sokan bir bili dalı olma özelliğiyle bilgisayardan üstün bir özellik taşımaktadır[20].

IV. BİLİŞİM SUÇLARI VE ADLİ BİLİŞİM

A. Genel Olarak

Bilişim ve bilişim suçlarının tanımlarını yukarıda belirtik. Bilişim suçları konusunda herkesin kabul ettiği bir tanım yoktur. Gelişen teknolojiyle beraber bilişim suçlarının işlenme şekillerinin değişmesi tanımı daha da güçleştirmektedir. Bilişim suçları konusunda herkesin ittifak ettiği bir tarif yoksa da en geniş kabul gören tarif Avrupa Ekonomik Topluluğu Uzmanlar Komisyonu'nun Mayıs 1983 tarihinde Paris Toplantısı"nda yaptığı tanımlamadır. Bu tanımlamaya göre bilişim suçları; "Bilgileri otomatik işleme tabi tutan veya verilerin nakline yarayan bir sistemde gayri kanuni, gayri ahlaki veya yetki dışı gerçekleştirilen her türlü davranış'tır. Üyesi bulunduğumuz Avrupa Ekonomik Topluluğu bir tavsiye kararında bu suçları beşe ayırmıştır. Bunlar sırası ile;

a. Bilgisayarda mevcut olan kaynağa veya herhangi bir değere gayri meşru şekilde ulaşarak transferini sağlamak için kasten bilgisayar verilerine girmek, bunları bozmak, silmek, yok etmek,

17 Tanrikulu Cengiz, "Hakimler Ve Savcılar Yüksek Kurulu (HSYK) Bilişim Hukuku Semineri 18-22 Mart 2013", www.hsyk.gov.tr Erişim Tarihi: 01.06.2013 s.7

18 Bilişim Terimleri Sözlüğü, http://tdkterim.gov.tr/bts/

19 Y. 11. C.D. 15.04.2008 T. 2008/792 E. , 2008/2826 K.

20 Özen Muharrem/ Baştürk İhsan, , s.11

b. Bir sahtekârlık yapmak için kasten bilgisayar verilerine veya programlarına girmek, bozmak, silmek, yok etmek,

c. Bilgisayar sistemlerinin çalışmasını engellemek için kasten bilgisayar verilerine veya programlarına girmek, bozmak, silmek, yok etmek,

d. Ticari anlamda yararlanmak amacı ile bir bilgisayar programının yasal sahibinin haklarını zarara uğratmak,

e. Bilgisayar sistemi sorumlusunun izni olmaksızın konulmuş olan emniyet tedbirlerini aşmak suretiyle sisteme kasten girerek müdahalede bulunmaktır.

Sonuç itibariyle bugün öğretide "bilişim suçu" kavramı üzerinde uzlaşmaya varıldığı ve bu kavramın tercih edildiği görülmektedir.

B. Bilişim Suçlarının Tarihsel Gelişimi

Bilişim suçlarının ortaya çıkışı, bilgisayarların yaygın olarak kullanılmaya başlanmasıyla olmuştur, bilişim suçlarının işlenme miktarının çok fazla sayılara ulaşması ve bu nedenle özellikle ceza hukuku açısından düzenleme yapılması ihtiyacının oluşması ise internetin ortaya çıkması ve bunun kişilerin kullanımına açılmasıyla gerçekleşmiştir[21]. 1966 yılına kadar bilişim ile ilgili suçların bilinmeyen bir olguydu. Zira bilgisayarların gelişimi ile birlikte diğer olumsuz sonuçlarının yanı sıra bilişim ile ilgili suçlar da ortaya çıkmış ve gün geçtikçe de bu suç tipleri çoğalmaya başlamıştır[22]. Bilinen ilk bilişim suçu, 18 Ekim 1966 tarihli Minneapolis Tribune'de yayınlanan "Bilgisayar uzmanı banka hesabında tahrifat yapmakla suçlanıyor" başlıklı makale ile kamuoyuna yansımıştır[23]. Bugün ise bilişim suçları geniş bir yelpazeye yayılmış durumdadır. Fakat ülkemizde bilişim suçları, terör, insan öldürme, yağma gibi suçların yanında çok ciddi bir suç olarak değerlendirilmemektedir.

İşlenen ve mağdurlarına ciddi zararlar veren ilk ve önemli bilişim suçlarından başka bir örnek vermek gerekirse, "Condor" kod adlı Kevin Mitnick adındaki genç, 1981 yılında Pasifik Bell anahtarlama istasyonuna ait verileri çalmakla suçlanmıştır. Mitnick 1982 yılında, Kuzey Amerika Hava Savunma Komutanlığı bilgisayarına girmiş, ayrıca Kaliforniya"daki tüm telefon anahtarlama merkezlerine erişerek, Manhattan'daki üç adet merkezi telefon şirketinin geçici olarak kontrolünü ele geçirmiştir. 1988'de 25 yaşında olan Mitnick, MCI ve Digital Equipment

21 Dülger M. Volkan, "Bilişim Suçları", İstanbul, 2004, s. 59

22 Yazicioglu Yılmaz, s. 50–51

23 Aydin Emin Doğan, "Bilişim Suçları ve Hukukuna Giriş", Ankara, 1992, s.13

şirketlerinin güvenlik çalışanlarının elektronik postalarını ele geçirmiştir. Bunun üzerine Digital Equipmant, Mitnick'i bilgisayar işlemlerine 4 milyon Amerikan Doları zarar vermekle ve 1 milyon Amerikan Doları değerindeki yazılımı çalmakla suçlamış ve yargılama neticesinde Mitnick 1 yıl hapse mahkûm edilmiştir. Yine 1993 yılında Mitnick, California Motorlu Araçlar Departmanı'nın veri tabanlarından sürücü belgelerini çalmakla suçlanmıştır. 1994 yılının ilk günü ise Mitnick, San Diego Supercomputer Center'da bulunan Tsutomu Shimomura'nın sistemine girmiştir. Bunun üzerine Shimomura da, Mitnick'in tutuklandığı 1995 yılına kadar internet üzerinden Mitnick'i kovalamıştır. Ve neticede Mitnick, yargılanarak suçlu bulunmuş, yaklaşık 5 yıl hüküm giydikten sonra, 21 Ocak 2000 tarihinde federal cezaevinden çıkmıştır[24].

Tarihsel gelişimi tarihten birkaç örnek vererek açıklamaya çalıştık ileriki bölümlerde bilişim suçlarına değindiğimiz de ise günümüzde bilişim suçlarının kısa sürede ne denli geliştiğini göreceğiz.

C.Adli Bilişim

Bu terim hukukumuzda bilişim sistemleri vasıtasıyla işlenen ve sayısal delil toplamanın gündeme geldiği durumlarda, bu delillerin hangi usuller ve araçlar vasıtasıyla toplanması gerektiği ve bu toplanan delillerin ne şekilde ilgili adli birimlere sunulacağı ve saklanacağı gibi hususları belirleyen disiplinin genel adı olarak kullanılmaktadır[25].

Adli bilişimi, esasen bilişim sistemlerinde meydana gelen olayların cereyanı sırasında işlenen suçlarda maddi gerçeğe ulaşmada soruşturmacılara yardımcı olmak amacıyla sayısal delillerin bulunması, elde edilmesi ve saklanması için geliştirilen yöntemleri ve araçları ortaya koyan bilim dalı olarak tanımlayabiliriz[26]. Adli bilişim, olay unsurlarını tanımlama, muhafaza etme, kurtarma, analiz etme ve olayla ilgili görüş sunma amacıyla adli olarak dijital ortamları inceler[27].

24 Özdilek Ali Osman, "Bilgisayar Suçları Ne Kadar Ciddi", Montreal, 2002 s. 2'den , Jonathan Littman: The Fugitive Game, Online With Kevin Mitnick

25 Yayla Mehmet, "Uluslararası Platformlarda ve Türkiye'de Bilişim Suçları, Ankara İl Jandarma Komutanlıuğında Alan Çalışması", Yayımlanmamış Yüksek Lisans Tezi, Ankara 2004, s.78

26 Tanrikulu Cengiz, s.37

27 Hakimler ve Savcılar için Siber Suçlar Eğitimine Giriş, Oturum 1.3.2 & 1.3.3, Elektronik Delil, www.hsyk.gov.tr. Slayt 44

V. TÜRKİYE'DE BİLİŞİM VE İNTERNET YÖNETİMİ

A. Ulaştırma Bakanlığı

Ülkemizde, bilişim ve bilgisayar denilince bakanlık bazında aklıma ilk akla gelen kuruluş Ulaştırma Bakanlığı'dır. 655 sayılı Ulaştırma, Denizcilik Ve Haberleşme Bakanlığının Teşkilat Ve Görevleri Hakkında Kanun Hükmünde Kararname ile Ulaştırma Bakanlığı bünyesinde Haberleşme Genel Müdürlüğü ve Bilgi İşlem Daire Başkanlığı Kurulmuş Kararnamenin 23 maddesinde Bilgi İşlem Dairesinin görevi: "Bilgi teknolojileri, bilişim, bilgi işlem ve bilgi güvenliğiyle ilgili her türlü yatırım, iş, işlem ve hizmetleri yapmak veya yaptırmak ve bunları Bakanlık merkez ve taşra teşkilatının kullanımına sunmak" şeklinde düzenlenmiştir. Açıklamalardan anlaşılacağı üzere bilişin alanı ile ilgili asli görev Ulaştırma Bakanlığı'dır. Diğer kuruluşlar ise bir şekilde Bakanlığın bağlı veya ilişkili kuruluşlarındandır.

B. İnternet Kurulu

5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi Ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun'un 10/5 maddesinde İnternet Kurulu'na yer verilmiştir.

İnternet Kurlu; Adalet Bakanlığı, İçişleri Bakanlığı, çocuk, kadın ve aileden sorumlu Devlet Bakanlığı ile Kurum ve ihtiyaç duyulan diğer bakanlık, kamu kurum ve kuruluşları ile internet servis sağlayıcıları ve ilgili sivil toplum kuruluşları arasından seçilecek bir temsilciden oluşur. 5561 sayılı kanun Telekomünikasyon iletişim Başkanlığı'na İnternet Kurulu ile gerekli işbirliği ve koordinasyonu sağlar; bu Kurulca izleme, filtreleme ve engelleme yapılacak içeriği haiz yayınların tespiti ve benzeri konularda yapılacak öneriler ile ilgili gerekli her türlü tedbir veya kararları alma hususlarını görev olarak yüklemiştir.

C. Bilgi Teknolojileri Ve İletişim Kurumu (BTK)

5809 sayılı Elektronik Haberleşme Kanunu ile Telekomünikasyon Kurumunun adı "Bilgi Teknolojileri Ve İletişim Kurumu" şeklinde değiştirilmiş görev ve yetkileri Kanunda düzenlenmiştir.

5809 sayılı Kanun'un 3/1-h maddesinde elektronik haberleşme; Elektronik haberleşme: "Elektriksel işaretlere dönüştürülebilen her türlü işaret, sembol, ses, görüntü ve verinin kablo, telsiz, optik, elektrik, manyetik, elektromanyetik, elektrokimyasal, elektromekanik ve diğer iletim sistemleri vasıtasıyla iletilmesini,

gönderilmesini ve alınmasını ifade eder" şeklinde tanımlanmıştır. Bu tanıma göre bilgisayar ve internet ağının elektronik haberleşme olarak değerlendirileceği sonucu çıkmaktadır.

D. Türkiye İletişim Başkanlığı (TİB)

23 Temmuz 2005 tarihinde 5397 sayılı Kanun ile Bilgi Teknolojileri ve İletişim Kurumu Bünyesinde, Telekomünikasyon İletişim Başkanlığı (TİB) kurulmuştur.

TİB'in ilk kuruluşunda bilgisayar ağlarına ilişkin hiçbir yetki ve görevi yoktu. Sadece telekomünikasyon yoluyla yapılan iletişim alanında yetkileri bulunan bir kuruluştu. Ancak 5651 sayılı Kanuna girmesi ile birlikte internet ortamında işlenen suçlarda mücadele anlamında tüm görevler TİB'e verilmiştir. Bunun içinde TİB bünyesinde İnternet Dairesi Başkanlığı kurulmuştur.

Konumuz esas olarak Türk Ceza Kanunu'nda yer alan bilişim suçları olduğu için TİB hakkında kısaca bilgi verilmiş ve TİB'in 5651 sayılı Kanundaki bilgisayar ağlarına ilişkin, 5651 sayılı Kanun dışındaki görev ve yetkilerine, TİB'in kuruluş olarak yapısına, kararlarının niteliğine savcılık ve mahkeme kararlarına karşı itiraz etme yetkisine uzun şekilde değinme cihetine gidilmemiştir. Ancak TİB bünyesinde kurulan ve konumuzla daha fazla ilgisi olduğunu düşündüğümüz İnternet Dairesi Başkanlığı'nın görev ve yetkilerine aşağıda değinilecektir.

E. İnternet Daire Başkanlığı

Yukarıda da belirttiğimiz üzere TİB bünyesinde bilgisayar ağları ile ilgili işlevleri yerine getirmek üzere görevlendirilmiş bir kuruluştur.

Bu kurumun görevleri, *Telekomünikasyon Yoluyla Yapılan İletişimin Tespiti, Dinlenmesi, Sinyal Bilgilerinin Değerlendirilmesi ve Kayda Alınmasına Dair Usul ve Esaslar ile Telekomünikasyon İletişim Başkanlığının Kuruluş, Görev ve Yetkileri Hakkında Yönetmelik"in* 22/A maddesinde belirlenmiştir. Maddeye göre İnternet Daire Başkanlığının görevleri şunlardır:

a) (Değişik:RG-9/9/2011-28049) 17 nci maddenin (j), (k), (1), (m), (o), (p), (r), (s), (t) ve (u) bentleri kapsamında sayılan görevleri yerine getirmek ve buna ilişkin iş ve işlemleri yürütmek,

b) (Değişik:RG-9/9/2011-28049) 5651 sayılı Kanunla verilen görevler kapsamındaki suçların internet ortamında işlenmesini önlemek için gerekli iş ve işlemleri yürütmek,

c) Erişim sağlayıcılar ve yer sağlayıcılar ile ilgili iş ve işlemleri yürütmek,

d) İnternet toplu kullanım sağlayıcılarıyla ilgili olarak mevzuatta Başkanlığa verilen görevleri yerine getirmek,

e) Başkanlığın bilişim ve internet alanındaki faaliyetleri ile ilgili yurt içi ve yurt dışı gelişmeleri takip etmek, bu kapsamda ulusal ve uluslararası kurum ve kuruluşlarla işbirliği ve koordinasyonu sağlamak ve gelişmelerin Başkanlık hizmetlerine yansıtılması için önerilerde bulunmak,

f) Başkan tarafından verilen diğer görevleri yerine getirmek.

F. Siber Suçlarla Mücadele Daire Başkanlığı

Bilişim teknolojileri kullanılarak işlenen suçların soruşturulması ve dijital delillerin incelenmesi için destek veren görevli daire başkanlıklarının ve taşra teşkilatındaki birimlerin dağınık yapısının tek bir çatı altında toplanması, mükerrer yatırımların önüne geçilmesi, siber suçlarla mücadelenin etkin ve verimli olarak yürütülmesini sağlamak amacıyla 2011/2025 sayılı Bakanlar Kurulu Kararı ile Emniyet Genel Müdürlüğü bünyesinde Bilişim Suçlarıyla Mücadele Daire Başkanlığı kurulmuştur.

28/02/2013 tarih ve B.05.1.EGM.0.65.35539/31772 sayılı Bakanlık Oluruna istinaden Bilişim Suçlarıyla Mücadele Daire Başkanlığının ismi Siber Suçlarla Mücadele Daire Başkanlığı (SSD) olarak değiştirilmiştir

SSD'nin sorumlu olduğu suçlar[28];

1.Bilişim Sistemlerine Yönelik Suçlar (T.C.K. madde 243 ve 244)

2.Banka ve Kredi Kartlarının Kötüye Kullanılması (T.C.K. madde 245/2-3)

3.Elektronik İmza (EİK madde 16. ve 17)

4.Bilişim Ve Banka Sistemleri Aracılığıyla; Dolandırıcılık (T.C.K. madde 158/1-f) ve Hırsızlık (T.C.K. madde 142/2-e)

5.Online Kumar (T.C.K. madde 228)

6.Çocuk Pornografisi (T.C.K. madde 226/3)

7.Haberleşmenin Engellenmesi (T.C.K. madde 124)

8.Özel Hayata Ve Hayatın Gizli Alanına Karşı İşlenen Suçlar (T.C.K. madde 132, 133, 134, 135 ve 136)

9.Ekonomi, Sanayi Ve Ticarete İlişkin Suçlar (T.C.K. madde 239/1-2)

28 Tataroğlu, Bahadır "Hakimler Ve Savcılar Yüksek Kurulu (HSYK) Bilişim Hukuku Semineri", 18-22 Mart 2013 www.hsyk.gov.tr Erişim Tarihi: 01.06.2013 s.8

10.Devlet Sırlarına Karşı Suçlar (T.C.K. madde 326/1, 327, 329, 330, 333, 334, 335, 336 ve 337)

İKİNCİ BÖLÜM

BİLİŞİM SUÇLARININ TEKNİK ANLAMDA İSLENME ŞEKİLLERİ

I. BİLİŞİM SUÇLARININ İŞLENME ŞEKİLLERİ

A. Genel Olarak

Bilişim suçlarında suçu işleyecek kişi açısından her hangi bir özellik belirtilmediği için bu suçların faili herkes olabilir

Bazı yazarlarca, bu suçun işlenebilmesi için belli bir bilgi birikimi olması gerektiği, bu nedenle bu suçların "beyaz yaka suçları" olarak değerlendirilmesini düşünen yazarlar vardır[29].

Bu suçu işleyen kişilere "hacker", "elektronik korsan", "siber terörist", "bilişim korsanı" gibi isimler verilmektedir.

Bilişim sistemlerinde araç olarak kullanılan bilgisayar, cep telefonu, tablet vb. kullanabilen herkes bu suçun faili olabilir. Bilişim suçu işleyen bir faili bulmak çok zor olabilir. Çünkü bu kişiler sanal bir ortamda kendi kimlik bilgilerini çoğu kez kullanmazlar. Hatta çoğu kez kendilerini karşı cins olarak tanıtmaktadırlar. Bu suçları işleyen failler gizemli olmayı çok sevmektedirler.

Bilişim suçlarıyla ilgili yapılan çalışmalar, çoğunlukla bilişim suçu faillerini; genç, eğitimli, teknik yeteneğe sahip ve genellikle agresif olarak nitelendirmektedirler[30].

Mağdur, suçu oluşturan fiilden doğrudan doğruya zarar gören kimsedir[31]. Bir başka görüşe göre ise, tecavüzün zarar verdiği değerin sahibi, zarar gören şahıstır[32]. Mağduru olmayan bir suç mümkün değildir. Ancak, mağdur kavramı ile suçtan zarar gören kavramlarını birbirine karıştırmamak gerekir. Suçtan zarar gören kişi her zaman suçun islenmesi dolayısı ile mağdur edilen kişi değildir. Mağdur ancak gerçek kişi olabilir. 5237 sayılı Türk Ceza Kanunu'nun 20. maddesine göre ancak gerçek

29 Dülger Murat Volkan, s.119'dan "İngilizce 'white-collar crime' teriminden Türkçe'ye çevrilen 'Beyaz yaka suçları'; kavram olarak oluşumunda şiddet içermeyen, ticari alanda dolandırıcılık, güveni kötüye kullanma gibi suç tipleri için kullanılan genel addır" Black's Law Dictionary s.1590

30 Karagülmez Ali, s.56

31 Toroslu Nevzat," Ceza Hukuku", 7. Baskı, Ankara, Savaş Yayınevi, Şubat 2005, s.67

32 Soyaslan, Doğan, "Ceza Hukuku, Genel Hükümler", 5. Baskı, Ankara, Yetkin Basımevi, 2005 s.224

kişiler suçun mağduru olabilmektedirler. Tüzel kişiler suçun mağduru olamazlar, suçtan zarar göreni olabilirler.

Mağdur bilişim sistemine bağlanan herkes olabileceği gibi bazı durumlarda bilişim sistemine bağlanmayan kişiler de mağdur olabilir. Mesela, fail başkasının kimlik ve kredi kartı bilgilerini kullanarak internetten ve bir mağazadan alışveriş yapmışsa bilgileri kullanılan kişi mağdur olmaktadır. Oysaki mağdurun verdiğimiz örnekte bilişim sistemiyle hiçbir bağlantısı olmamıştır.

Bilişim suçlarında faile ulaşmak zor olduğu için suçla mücadele sürekli mağdura dikkatli olması telkin edilmekte, hatta uyarı yazıları konularak mağduriyetlerin önüne geçilmeye çalışılmaktadır. Günümüzde Emniyet Genel Müdürlüğü cep telefonlarına bu konuda birçok ileti atmaktadır.

Bilişim suçlarının işlenme şekilleri klasik suç tiplerinden farklıdır. Klasik suç tiplerinde suçun maddi unsurlarından birini oluşturan eylemler, faillerin maddi hareketiyle meydana gelmektedir. Bu maddi hareket evrakta sahtecilik suçunda failin somut bir belgeyi değiştirmesi eylemidir. Bilişim suçlarında ise genellikle failin bir bilgisayar klavyesine dokunması dışında başkaca bir fiziki hareket olmamakta birlikte meydana gelecek zararlar çok daha fazla olmaktadır[33].

Bilişim teknolojisindeki hızlı gelişmesi ile bilişim suçlarının islenme şekilleri de gün geçtikçe artmaktadır. Sık görülen birkaç bilişim suçunun işlenme şekillerine aşağıda değineceğiz.

1. Truva Atı (Trojan Horse)

Resim 1.1. Truva Atı Örnek Resim

Bu tekniğin tarihteki, Truva atı efsanesine benzeyen yönleri bulunmaktadır[34]. Bilgisayar yazılımı bağlamında Truva atı zararlı program barındıran veya yükleyen programdır. Fail, bir bilgisayarda kullanılan programın istediği gibi çalışmasını sağlamak için bu programın içine gizli bir program ilave etmektedir. Bu şekilde fail yapmak istediği işlemleri gerçekleştirebilmektedir.

33Dülger M. Volkan, s.69

34 Aydin Emin Doğan, "Bilişim Suçları Ve Hukukuna Giriş", Ankara, Eylül 1992 s.48

Truva atları masum kullanıcıya kullanışlı veya ilginç programlar gibi görünebilir ancak yürütüldüklerinde zararlıdır[35].

Truva atı, bir virüs değildir. Kendi kendini çoğaltmaz, sadece sabit diskteki bilgilere zarar verir. Truva atı, kendisini zararsız bir program gibi (örneğin bir oyun ya da yardımcı program) gösterir. Görünümü ve ilk çalıştırıldığındaki aktivitesi zararsız bir program gibidir, ancak çalıştırıldığında verileri silebilir veya bozabilir[36]. Yani Truva atı yazılımı, kurulmuş olduğu bilgisayarın yazılımının açıklarından yararlanarak bütün sisteme hâkim olmakta ve failin bütün komutlarını yerine getirmektedir[37].

Truva atının en basit örneği yüklendiğinde bedava ekran koruyucu vaat eden Waterfalls.scr isimli programdır. Çalıştırıldığında uzaktan bilgisayara giriş sağlayabilecektir. Truva atı zararlı yükü (payload) çeşitli zararlar vermek için dizayn edilmiş olsa da zararsız da olabilir. Truva atları sistemde nasıl gedik açabildiğine ve nasıl tahribat yaptığına göre sınıflandırılır. 7 ana tür Truva atı zararlı yükü vardır[38]: Uzaktan Erişim, E-posta Gönderme, Veri yıkımı, Proxy Truva (zararlı bulaşmış sistemi saklama), Ftp Truva (zararlı bilgisayardan dosya ekleme ya da kopyalama), Güvenlik yazılımını devre dışı bırakma, hizmetin reddi servis saldırıları (Dos Saldırıları), URL Truva (zararlı bulaşmış bilgisayarı sadece pahalı bir telefon hattı üzerinden internete bağlama)

Bu virüs ile yapılan eylem, Türk Ceza Kanunu'nun 244. maddesinin 1. fıkrasında düzenlenen, bilişim sistemini bozma suçunu oluşturacaktır.

2. Salam Tekniği (Salami Teqniques)

Salam tekniği, genellikle bankalarda yaygın olarak gerçekleştirilen bir bilişim suçu metodudur. Fail, bu yöntemle banka hesaplarındaki küsuratların veya virgülden sonraki son bir ya da iki rakamı kendi belirlediği bir hesaba aktarmaktadır. Böylelikle banka çalışanları veya hesap sahipleri hesaplarda meydana gelen bu küçük miktarların yetkisiz hareketini fark edememektedir. Ancak bu küçük miktarların faile ait başka bir hesapta toplanması faile büyük miktarlarda hukuka

35 Vikipedi, Özgür Ansiklopedi, http://tr.wikipedia.org/wiki/K%C3%B6t%C3%BC_vir%C3%BCs , Erişim Tarihi: 23.8.2013

36 Yayci Esra, s.30

37 Değirmenci Olgun; "Bilişim Suçları", Yayımlanmamış Yüksek Lisans Tezi, Marmara Üniversitesi Sosyal Bilimler Enstitüsü, 2002 s.79

38 Vikipedi, Özgür Ansiklopedi, http://tr.wikipedia.org/wiki/K%C3%B6t%C3%BC_vir%C3%BCs , Erişim Tarihi: 23.8.2013

aykırı yarar sağlamaktadır[39]. Bu tekniğin gerçekleştirilmesi için de genellikle Truva atı yazılımının çeşitleri veya benzer işleve sahip yazılımlar kullanılmaktadır[40].

Bu virüs ile yapılan eylem, Türk Ceza Kanunu'nun 244. maddesinin 4. fıkrasında düzenlenen, bilişim sistemine müdahalede bulunarak haksız çıkar sağlama suçunu oluşturacaktır.

3. Sistem Güvenliğinin Kırılıp İçeri Girilmesi (Hacking)

Resim 1.2. Hacking Örnek Resim

"Hacking" eylemini gerçekleştiren kisilere "hacker" denilmektedir. "Hacker" ise, bilişim sistemlerinin isleyiş sistemlerini merak eden ve sisteme müdahale eden kişiye verilen isimdir. Ayrıca "crack" eylemi ve bunları gerçekleştiren kişiler olan "cracker"ler ise, sisteme müdahale edenler arasında üst seviyede teknik bilgi ve donanıma sahip, tecrübeli ve bu işte ileri düzeyde olanlar için kullanılmaktadır. Bunlar diğerlerine oranla daha kötü niyetli faaliyetlerde bulunmaktadır. Genel olarak bu kişileri ifade etmek için "bilişim korsanı" terimi kullanılabilir[41]. Failler bu yöntemle genellikle hukuka aykırı eylemler haberleşme özgürlüğünü, özel hayatın gizliliğini ihlal eder niteliktedir. Bu virüs ile düzenlenen eylem, Türk Ceza Kanunu'nun 244. maddesinin 1 ve 2. fıkralarında düzenlenen suçları oluşturur.

4. Mantık Bombaları (Logic Bombs)

Resim 1.3. Mantık Bombası Örnek Resim

Belirli çevresel değişkenlere bağlı olarak yıkıcı bilgisayar komutlarını meydana getiren programlardır. Örneğin bir mantık bombası yaratıcısının maaş kayıtlarının izleyebilir ve yaratıcısının maaşı belirli bir limitin altına düştüğünde, yükseltmek

39 Dülger M. Volkan, s.71

40 Değirmenci Olgun, s.84

41 Dülger M. Volkan, s.72

silmek veya formatlamak gibi bilişim suçu yapacak işlemlerde bulunabilir[42].

Bu virüs ile yapılan eylem, Türk Ceza Kanunu 244. maddesinin 2. fıkrasında düzenlenen, verileri bozma suçunu oluşturacaktır.

5. Bilişim Virüsleri

Resim 1.4. Virüs Alarmı Örnek Resim

Bu günümüzde en çok bilinen yöntemdir. Virüs, bir programa oradan da bütün programlara kendini kopyalayarak bilişim sistemlerini kullanılamayacak hale getirmektedirler. En belirgin özelliği kendini kopyalamasıdır. İnsanlar program ve bilgisayarları yavaşladığında "virüs bulaşması" terimini kullanırlar. Virüsten korunmanın yöntemi Anti virüs programları kullanmaktır. Ancak bazı virüsler kendini geliştirerek anti virüs programlarına takılmayarak yayılabilmektedir. Bu nedenle anti virüs programlarını sürekli güncellemek gerekir.

Mantık bombası gibi bu virüs ile yapılan eylem de Türk Ceza Kanunu 244. maddesinin 2. fıkrasında düzenlenen, verileri bozma suçunu oluşturacaktır.

6. Hukuka Aykırı İçerik Sunulması

Bu husus, çocuk pornografisi, şiddeti teşvik eden, ayrımcı ve kişilik haklarına tecavüz eden içerikler şeklinde olmaktadır.

7. Bilgi Aldatmacısı (Data Diddling)

Bilgi aldatmacası, bilgisayara yanlış veri girilmesi veya bazı verilerin kasten bırakılması anlamına gelmektedir. Böylece fail, bilgisayara girdiği veya bilgisayarda bıraktığı veriler ile mevcut veriler üzerinde istediği yönde değişiklik yapma veya cihazı istediği yönde kullanma olanağına kavuşmaktadır[43].

Mantık bombası gibi bu virüs ile yapılan eylem de Türk Ceza Kanunu 244. maddesinin 2. fıkrasında düzenlenen, verileri bozma suçunu oluşturacaktır.

42 Aydin Emin Doğan, s.52

43 Yazicioglu Yılmaz, s.152

8. Sistem Dışı Alınan Elektronik Postalar (Spam)

Resim 1.5. Spam E-posta Örnek Resim

Günümüzde istem dışı e-postalar önemli bir sorun haline gelmiştir. Bu tür elektronik postalara "spam" da denilmektedir. Bu e-postalar daha bizim gönderilmesini izin vermediğimiz, iznimiz dışında gönderilen reklâmlar şeklinde gelmektedirler. İstem dışı alınan elektronik postalara ilişkin mevzuatımızda özel bir düzenleme bulunmamaktadır. Ancak e-postaların içeriğine göre Türk Ceza Kanunu'ndaki suç türlerine girebilir. E-postanın içeriğinde tehdit var ise T.C.K. 106. maddesi, hakaret var ise T.C.K. 125. maddesi, terör örgütü propagandaları varsa Terörle Mücadele Kanunu uygulama alanı bulabilir. Bunun yanında istem dışı alınan elektronik postalar, sistemi engelleyecek boyuta ulaştığı takdirde bu, 5237 sayılı T.C.K.'nın 244. maddesinde düzenlenen "bilişim sisteminin engellenmesi" kapsamında değerlendirilebilecektir. Ayrıca, istemediğimiz halde aynı kişiden sürekli e-posta gelmesi T.C.K.'nın 123. maddesindeki kişilerin huzur ve sukününu bozma suçu kapsamında değerlendirilebilir diye düşünmekteyiz.

9. Ağ Solucanları (Network Worms)

Resim 1.6. Bilgisayar Solucanları Örnek Resim

Solucan virüsü genellikle e-posta, kaynağı belirsiz programlar, forum siteleri, korsan oyun dvd ve cd leri gibi farklı yollarla bilgisayarlara bulaşır. Solucan da, virüs gibi, kendisini bir bilgisayardan diğerine kopyalamak için tasarlanmıştır ancak bunu otomatik olarak yapar. İlk olarak, bilgisayarda dosya veya bilgi ileten özelliklerin denetimini ele geçirir. Solucan bir kez sisteminize girdikten sonra kendi başına ilerleyebilir. Solucanların en büyük tehlikesi, kendilerini büyük sayılarda çoğaltma becerileridir. Örneğin bir solucan, e-posta adres defterinizdeki herkese kopyalarını gönderebilir ve sonra aynı şeyi onların bilgisayarları da yapabilir. Bu, domino

etkisinin getirdiği yoğun ağ trafiği işyeri ağlarını ve Internet'in tümünü yavaşlatabilir. Yeni solucanlar ilk ortaya çıktıklarında çok hızlı yayılırlar. Ağları kilitlerler ve olasılıkla sizin ve başkalarının Internet'teki Web sayfalarını görüntülerken uzun süreler beklemenize yol açarlar. Solucan, Virüslerin bir alt sınıfıdır. Bir solucan genellikle kullanıcı eylemi olmaksızın yayılır ve kendisinin tam kopyalarını (olasılıkla değiştirilmiş) ağlardan ağlara dağıtır. Bir solucan bellek veya ağ bant genişliği tüketebilir, bu da bilgisayarın çökmesine yol açabilir. Solucanlar yayılmak için bir "taşıyıcı" programa veya dosyaya gereksinim duymadıklarından, sisteminizde bir tünel de açabilir ve başka birinin uzaktan bilgisayarınızın denetimini eline geçirmesini sağlayabilir[44].

Yakın geçmişteki solucanlara örnek olarak Sasser solucanı ve Blaster solucanı verilebilir. Solucanı Truva atından farklı kılan farklılıklar şunlardır[45];

1. Truva virüsü bilgisayara girdiğinde hangi programla girmişse o programın açılmasını bekler program açılmazsa truva at bilgisayarda aktifleşemez.
2. Truva atı direk bilgisayarın işletim sistemine zarar verir. Solucan ise zarar vermez sadece girdiğiniz siteleri, girdiğiniz kullanıcı adı ve şifreleri, indirdiğiniz programları, anlık ileti programlarında konuşmalarınızı yani bilgisayarda yaptığınız her şeyi programcısına rapor olarak bildirir.
3. Truvanın sahibi kendi bilgisayarından sizin bilgisayarınızın ekranını kapatabilir, klavyenizdeki tüm ışıkların yanıp sönmesini sağlayabilir, istediği programları açabilir, monitörünüzü kapatabilir kısacası tüm kontrolü eline alabilir ama solucanın böyle bir özelliği yoktur.

İnternetteki solucan örnekleri[46];

1. Tebrikler 250 sms kazandınız telefonunuza indirmek için tıklayınız.
2. Tebrikler Amerika'ya gitme hakkını yakalamak için ücretsiz çekiliş kazandınız.
3. Tebrikler Amerika kapınızda.
4. Visa kartınıza bonus kazandınız.
5. Sitemize giren 1.000.000. kişisiniz. Bizden hediye şarkı kazandınız.
6. Bugün şanslı gününüzdesiniz. Bizden para ödülü kazandınız.
7. Tebrikler bizden saat kazandınız.

44 Vikipedi, Özgür Ansiklopedi, http://tr.wikipedia.org/wiki/K%C3%B6t%C3%BC_vir%C3%BCs , Erişim Tarihi: 23.8.2013

45 Vikipedi, Özgür Ansiklopedi, http://tr.wikipedia.org/wiki/K%C3%B6t%C3%BC_vir%C3%BCs , Erişim Tarihi: 23.8.2013

46 Vikipedi, Özgür Ansiklopedi, http://tr.wikipedia.org/wiki/K%C3%B6t%C3%BC_vir%C3%BCs , Erişim Tarihi: 23.8.2013

E-postalarda solucan örnekleri[47];

1. Bin Ladin yakalandı.
2. Fidel Castro öldü.
3. İlk defa nükleer terör saldırısı gerçekleşti.
4. Üçüncü dünya savaşı çıktı.
5. 300$ bonus kazandınız.

10. Ağ Tavşanları (Network Rabbits)

Bilgisayar virüslerinden biridir. Adlarına yakışır şekilde çok hızlı ürerler. Hafıza depolarında alan tükeninceye kadar kolonileşirler. Burada amaç, özellikle çok kullanıcılı sistemlerin, iletişim ağ ortamlarında ana sistem bilgi isleme gücünü yitirinceye kadar sistemin kaynaklarını kurutmaktır.

Tavşanlar ile virüsler arasındaki en belirgin fark, tavşanların kullanıcı veri kütüklerinin sonuna eklenmemeleri, asalak özelliklere sahip olmamaları ve kendi kendilerine yetebilmeleridir[48].

Mantık bombası gibi bu virüs ile yapılan eylem de Türk Ceza Kanunu 244. maddesinin 1. fıkrasında düzenlenen, bilişim sistemini bozma suçunu oluşturacaktır.

11. Bukalemun (Chameleon)

Resim 1.7. Bukalemun Virüsü Örnek Resim

Truva atı özelliğine yakın olan bukalemun diğer alışılagelmiş, güvenilir programlar gibi davranmakla beraber, gerçek birtakım hile ve aldatmalar içerir. Uygun şekilde programlandığında yasalarla belirlenmiş yazılımların her hareketini taklit edebilir. Bukalemun, sisteme giren bütün kullanıcıların adlarını ve şifrelerini gizli bir dosyada kaydeder ve sistemin bakım için geçici bir süre kapatılacağına ilişkin mesaj verir. Daha sonra bukalemunun yaratıcısı, kendi yasa dışı amaçları için programlara istediği gibi girer, çıkar[49].

Bu virüs ile yapılan eylem Türk Ceza Kanunu'nun 244. Maddesinin 1. fıkrasında düzenlenen, bilişim sistemini bozma suçunu oluşturacaktır.

47 Vikipedi, Özgür Ansiklopedi, http://tr.wikipedia.org/wiki/K%C3%B6t%C3%BC_vir%C3%BCs , Erişim Tarihi: 23.8.2013

48 Aydin Emin Doğan, s.52-53

49 Aydin Emin Doğan,s.51

12. Süper Darbe (Super Zapping)

Süper Darbe bir uzmanlık programı olup aslında yararlıdır. Bu durumu açıklayacak olursak, bilgisayar sistemleri bazen çeşitli isletme hatalarından veya programların kendilerinden kaynaklanan sebepler ile çalışamaz hale gelmektedirler, diğer bir ifade ile kilitlenmektedir. Sistemin kilitlendiği bu gibi durumlarda, en kısa zaman içinde yeniden çalışıp işlevsel olabilmeleri için "super zap" programları kullanılmaktadır ki bu programlar bir yandan sistemdeki çeşitli emniyet tedbirlerini asarken, diğer yandan da meydana gelen sorunları süratli bir şekilde düzeltmektedir[50]. Bu yöntemin kötü niyetli kimseler tarafından kullanılması halinde güvenlik mekanizmalarının engeli olmaksızın sistem üzerinde istenen değişiklik yapılabilmekte ve bu şekilde tehlikeli hale gelebilmekte bilişim suçu işlenmesine sebebiyet verebilmektedir.

Bu virüs ile yapılan eylem de Türk Ceza Kanunu'nun 244. maddesinin 1. fıkrasında düzenlenen, bilişim sistemini bozma suçunu oluşturacaktır.

13. Gizli Kapı Veya Hile Kapısı (Trap Doors)

Resim 1.8. Gizli Kapı Örnek Resim

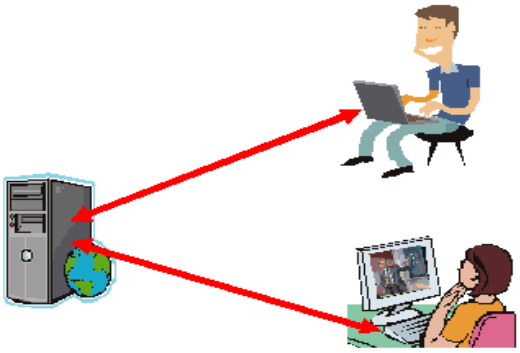
İşletim sistemleri veya çok işlevli ve kullanıcılı sistemleri hazırlayan bilgisayar programcılarının bunları meydana getirirken ileride ortaya çıkabilecek durumlara göre, sistem şifrelerinde değişiklik yapabilmeyi veya yeni şifreler girebilmeyi sağlamak üzere sisteme bıraktıkları çeşitli giriş olanaklarına denilmektedir. Bununla, değişikliğe kapalı olan şifreler üzerinde, ortaya çıkan yeni şartlara göre ayarlama yapabilme olanağı yaratılmak istenmektedir[51]. Bu yöntem kötü niyetle kullanılması durumunda bilişim suçu işlenmesine sebebiyet verebilmektedir.

Bu virüs ile yapılan eylem de Türk Ceza Kanunu'nun 244. Maddesinin 1. fıkrasında düzenlenen, bilişim sistemini bozma suçunu oluşturacaktır.

50 Yazicioglu Yılmaz, s.156

51 Yazicioglu Yılmaz, s.156-157

14. Eş Zamanlı Saldırılar (Asynchronous)



Resim 1.9. Eş Zamanlı Saldırı Örnek Resim

Çok işlevli program teknikleri, bilgisayarda mevcut bulunan birçok programın, bilgisayar kaynaklarını çeşitli usuller çerçevesinde kullanmak suretiyle sırayla işlem yapmalarına olanak sağlamaktadır. Birçok sistemin mevcut programları es zamanlı kullanamamasından hareket eden bazı failler, geliştirdikleri es zamanlı saldırı teknikleri ile bilgisayar işletim sistemlerinde, daha doğrusu programdaki veriler üzerinde çeşitli ihlâller meydana getirmektedirler[52].

Bu virüs ile yapılan eylem de Türk Ceza Kanunu'nun 244. maddesinin 1 ve 2. fıkralarında düzenlenen suçları oluşturabilecektir.

15. Artık Toplama (Scavening)

Adından da anlaşılacağı üzere, bir bilgisayar sisteminin çalışmasından geriye kalan veri ve bulguların toplanması işlemini ifade etmektedir. Bu işlem, yazıcıdan çıkan bir karbon kâğıdın veya bilgisayar çıktısının çevreden toplanması ile ilgili olabileceği gibi, bilgisayarda işlem görüp silinmiş, kayıtları yok edilmeye çalışılmış verilerin elde edilmesi seklinde de olabilmektedir[53].

Bu eylem Türk Ceza Kanunu'nun 244. Maddesinde düzenlenen sistemi engelleme, bozma, verileri yok etme veya değiştirme suçu oluşabilir.

16. Yetki Dışı Veya Gizlice Girme (Piggybacking – İmpersonation)

Resim 1.10. Yetkisiz Sisteme Girme Örnek Resim

Bir sisteme yetki dışı girme veya yetki dışı kullanım hem elektronik hem de nesnel usullerle gerçekleştirilebilmektedir. Nesnel olanı elektronik veya mekanik yöntemlerle kontrol edilen yerlere giriş imkânı yaratmak için kullanılan bir usul teskil

52 Yazicioglu Yılmaz, s.158

53 Yazicioglu Yılmaz, s.159

etmektedir. Örneğin, girişi kontrol altında bulunan bir alana giriş için, buraya giriş yetkisi bulunan bir kimsenin izlenmesi suretiyle gizlice girişin sağlanması gibi. Elektronik olanı ise, sistemin kullanıcıyı otomatik olarak tanıdığı online sistemlerde yani birçok kullanıcılı sistemlerde söz konusu olmaktadır. Zira bu tür bir sistemde terminalin devreye geçebilmesi için anahtar görevi yapan bir şifreye ihtiyaç bulunmakta ve ancak bu şifre girildikten sonra terminal üzerinden bilgisayarla ilgili istenilen faaliyetler gerçekleştirilebilmektedir[54]. Bu durumda Türk Ceza Kanunu 243. Maddesindeki bilişim sistemlerine girme suçu oluşabileceği gibi, kişinin sistemde yapmış olduğu eyleme göre aynı kanunun 244. maddesinde düzenlenen sistemi engelleme, bozma, verileri yok etme veya değiştirme suçu da oluşabilir.

17. Saatli Bombalar (Time Bombs)

Resim 1.11. Saatli Virüsler Örnek Resim

Nümerik veya zamana bağlı çevresel değişkenlerin aldıkları duruma göre koşulsal olarak, zararlı bilgisayar komutlarını yerine getiren programlardır. Genelde mantık bombaları ile aynı yapıya sahiptirler ve belirli bir sayıda çalıştırıldıktan sonra, belli bir tarihte patlayacak şekilde programlanabilirler[55]. Örneğin 01 Ocak patlama tarihi olarak belirlenerek eylem gerçekleştirilebilir.

Bu eylem Türk Ceza Kanunu'nun 244. maddesinde düzenlenen sistemi engelleme, bozma, verileri yok etme veya değiştirme suçu oluşabilir.

18. Yazılım Bombaları (Software Bombs)

Resim 1.12. Yazılımı Tahrip Etme Örnek Resim

Şimdiye kadar işlenmesi en kolay ve popüler bilişim suçu yazılımı, yazılım bombası olmuştur. Bu virüs çeşidi olan yazılım bombaları, kütük organizasyonunu tahrip etmek için kullanılır. Sisteme girdikleri anda adlarına yakışır

54 Yazicioglu Yılmaz, s.159

55 Aydin Emin Doğan, s.51

şekilde verilere çarparak yok ederler. Bu durumda ne bir uyarı, ne de önceden bir belirti söz konusudur[56].

Bu eylem T.C.K. 244'teki sistemi engelleme, bozma, verileri yok etme veya değiştirme suçu oluşabilir.

19. Bug – Ware

Resim 1.13. Bug-Ware Örnek Resim

Aslında tam anlamıyla bilişim suçu sayılamayacağı ileri sürülen bug-ware, belirli fonksiyon kümelerini düzenlemek için tasarlanan bilgisayar programlarını temsil eden bir terimdir. Ancak, uygun olmayan ve zor anlaşılır, karışık programlanmaları nedeniyle, sistem yazılımlarına ve donanımlarına zarar verebilirler. Yanlış mantık akışı ve program parçalarının, uygun olmayan bir şekilde bir araya getirilmesi nedeniyle, istemeyerek bile olsa donanımlara ve verilere zarar verebilirler[57].

Bu eylem Türk Ceza Kanunu'nun 244. Maddesinde düzenlenen sistemi engelleme, bozma, verileri yok etme veya değiştirme suçu oluşabilir.

20. Tarama (Scanning)

Resim 1.14. Tarama Yöntemi İle Virüs Örnek Resim

Bilişim sistemlerine değeri her seferinde değişen veriler, hızlı bir şekilde girilmek suretiyle, sistemin olumlu cevap verdiği durumların tespitine yönelik bir tekniktir. Tarama bilişim sistemlerinin telefon numaralarını veya internete bağlı sistemlerinin IP numaralarını bulmaya yönelik olabileceği gibi, numarası belli olan fakat şifre ile korunmuş

56 Aydin Emin Doğan, s.51

57 Aydin Emin Doğan, s.50

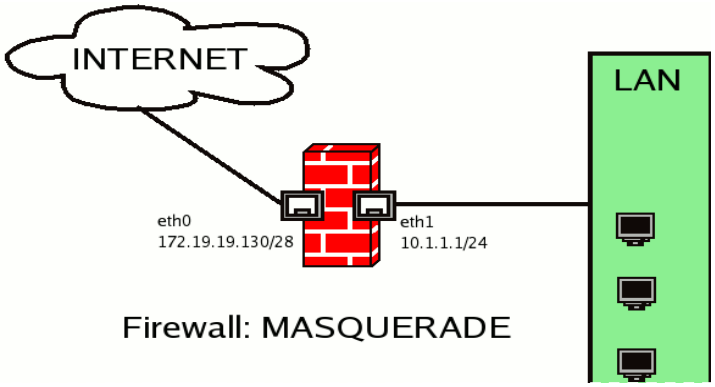
sistemlerin geçerli şifrelerini bulmaya yönelik de olabilir. Birinci durumda "port tarayıcı", ikinci durumda "password tarayıcı" söz konusu olacaktır[58].

21. Web Sayfası Hırsızlığı ve Web Sayfa Yönlendirme

Resim 1.15. Web Sayfası Çalma Örnek Resim

Amerika ve Almanya"da çok sık olarak görülen bu suç tipinde, kendisine internet adresi (domain name) almak isteyen kişinin, bir ISS"ye yaptığı müracaat, sisteme müdahale eden bilisim korsanı veya bu bilgiye ulasan çalışan tarafından kendileri veya üçüncü bir kisi adına daha hızlı davranılarak kaydettirilir. Daha sonra bu internet adresi yüksek ücretlerle satılır. Web sayfası yönlendirme ise, Avrupa, Orta dogu, Asya"nın bazı bölümleri ile Afrika'nın kuzey bölümlerinin internet adreslerini dağıtmaktan sorumlu olan "Reseaux IP Europeens Network Coordination Center" (RIPE) adlı organizasyonun veri bankasında bulunan web sayfalarına, internet üzerinden nasıl ulaşılacağına dair "routing" kurallarının yapılan müdahalelerle değiştirilerek internet kullanıcılarının farklı internet adreslerine çekilmesi suretiyle islenmektedir[59].

22. Yerine Geçme (Masquerading)



Resim 1.16. Hile ile Erişim Yetkisi Örnek Resim

Bir ağa bağlı olan bilişim sistemleri, erişim imkânları bakımından sınıflara ayrılırlar. Bazı bilişim sistemleri için daha geniş olan erişim imkânı, diğerleri için daha sınırlı tutulabilir. Sistem isleyişinde bu yetkiyi tanımlayabilmek için bir erişim kodu veya parola ister. Ancak

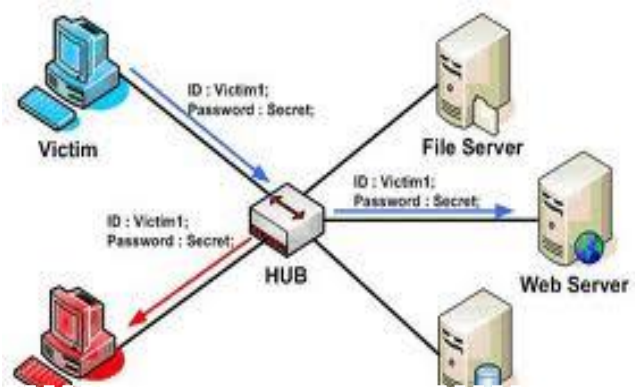
58 Degirmenci Olgun, s.82

59 Degirmenci Olgun, s.98-99

sistemlerde yapılan ufak hilelerle erişim yetkisi olmayan veya sınırlı erişim yetkisi olan kişilere erişim hakkı tanınabilmektedir. Eğer bu hile, erişim yetkisi olan bir kişinin/sistemin parola veya erişim kodunun yazılması veya ona özgü niteliklerin taklit edilmesi suretiyle yapılırsa yerine geçme olarak isimlendirilir[60].

Bu eylem Türk Ceza Kanunu'nun 244. Maddesinde düzenlenen sistemi engelleme, bozma, verileri yok etme veya değiştirme suçu oluşabilir.

23. Gizlice Dinleme (Eavesdropping)



Resim 1.17. Gizlice Dinleme Örnek Resim

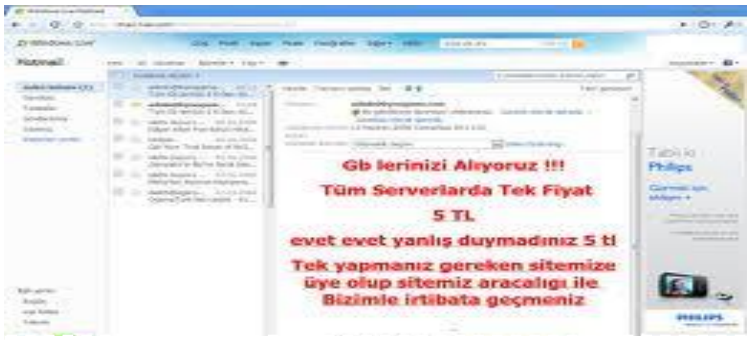
Gizlice dinleme, bilişim sistemlerinin veri taşımada kullandığı ağlara girilerek veya bilişim sistemlerinin yaydığı elektromanyetik dalgaların yakalanarak verilerin elde edilmesidir. Bilgisayar monitörlerinin yaydığı elektromanyetik dalgaların yakalanarak tekrar ekran görüntüsüne dönüştürülmesi mümkündür. Bilişim sistemlerinin merkezlerine yerleştirilecek elektromanyetik dalgaları yakalayabilen radyo vericileri aracılığı ile de veriler elde edilebilir. Araya konulan yükselticiler vasıtasıyla, elektromanyetik dalgaları çok uzaklardan yakalamak ve verileri elde etmek mümkündür. Bilişim sistemleri arasında kullanılan ağlara veri gönderimi sırasında yapılan fiziksel müdahaleler sonucu, ağ üzerinde akan verileri elde edilmesi seklinde de gizlice dinleme yapılabilmektedir[61].

Bu eylem Türk Ceza Kanunu'nun 133. ve 135. maddelerinde düzenlenen kişiler arasındaki konuşmaların dinlenmesi ve kayda alınması suçu ile özel hayatın gizliliğini ihlal suçlarını oluşturur.

60 Degirmenci Olgun, s.102-103

61 Degirmenci Olgun, s.76-77

24. Sahte Elektronik Posta (Fake Mail)

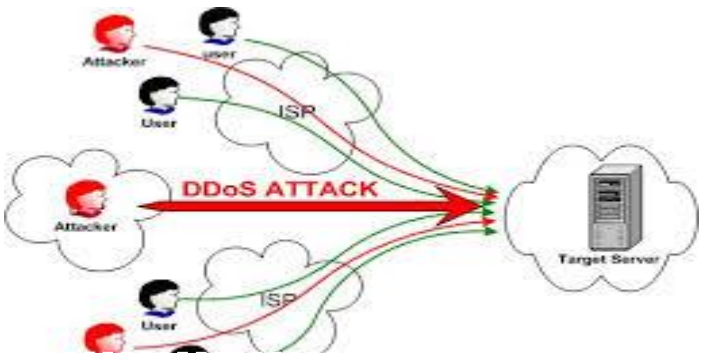


Resim 1.18. Sahte E posta Örnek Resim

Sahte elektronik posta, bir internet kullanıcısının elektronik posta şifresinin, kullanıcı adının veya ICQ numarasının sanki o kişinin elektronik posta veya ICQ hesabından gönderilmiş gibi görünen bir mail ile çalınmasıdır. Kullanıcının dikkatsizliğinden faydalanarak gerçeğine benzeyen sahte bir web sayfası yardımıyla elektronik mail adreslerinin kullanıcı adı ve şifresini ele geçirmekte kullanılan bir saldırı tipidir. Kullanıcı web sayfasına güvenerek doldurduğu bir form nedeniyle şifre ve kod bilgilerini fark etmeksizin üçüncü bir kişiye teslim etmektedir. Bundan başka e-mail servisinden geldiği sanılan böyle bir e-mailde istenen bir linke tıklanmışsa, bu sırada sahte bir şifre sorgu penceresi açılır ve kullanılan mail servisinde bir sorun olduğunu, mail şifresini tekrar girmek gerektiği söylenir. Böylece girilen şifre bilgileri fake (sahte) maili (e-posta) hazırlayan kişiye ulaşır[62]. Bu yönteme phising de denilmektedir, aşağıda bu yönteme de değineceğiz.

Bu yöntemle, Türk Ceza Kanunu'nun 244. maddesinin 1. fıkrasında düzenlenen sisteminin işleyişini engelleme veya bozma suçunu işlemek mümkündür.

25. Daniel Of Service Attack



Resmi 1.19. Daniel Of Service Attack Yöntemi Örnek

Bu yöntem bir sunucunun baş edemeyeceği kadar çok işlem talep edilmek suretiyle yetkili kişinin servis dışı kalmasına sebep olunması olarak bilinmektedir. Burada kaynağın tüketilmesi söz konusu olmaktadır. Saldırgan sayısının çokluğu ve coğrafi açıdan yaygın bir alanda faaliyet göstermesi durumunda saldırıyı kontrol etmek oldukça zor olmaktadır. Elektrik kaynağı ve ağ kabloları gibi

62 Palli Hayati, "Türk Hukukunda Ve Mukayeseli Hukukta Bilişim Suçları", Yayımlanmış Yüksek Lisans Tezi, Kayseri, Kasım 2008, s.66

araçlarda hedef alınarak fiziki zarar verilmek suretiyle servise ulaşım engellenebilmektedir[63].

Bu yöntemle, Türk Ceza Kanunu'nun 244. maddesinin 1. fıkrasında düzenlenen sisteminin işleyişini engelleme veya bozma suçunu işlemek mümkündür.

25. Phishing (Yemleme)

Resim 1.20. Yemleme Yöntemi Örnek Resim

Phishing[64], fishing (balık tutmak) ve password (şifre) kelimelerinin birleşmesinden ortaya çıkan bir terimdir. Bu yolla çok fazla suç işlenmeye başlanmıştır. Güvenilen bir kurumdan gelen e-postaya şifrenizi yazarken aslında bilgilerinizi faile gönderilmektedir.

Sahte banka site linklerinin yanı sıra Facebook, Google, Blizzard, Yahoo, WordPress, Paypal gibi kurumların da sahte sayfaları bu sistemde kullanılmaktadır.

Bu işin birkaç çeşiti vardır. En çok banka bilgilerini çalmak için sahte e-posta ekranları oluşturulmaktadır. Bunun yanında fail bir e-postayı tanıdığınız birinden gelmiş gibi göstererek e posta ile gelen linklere tıklamamak şeklinde olmaktadır, fail sosyal ağlardan topladıkları bilgilerle e-postaları daha inandırıcı hale getirebilir veya bir ödül kazandığınızı iddia ederek linke tıklamanızı teşvik edebilir. Bu tehlikelerde kurtulmak için gönderilen linklere çok dikkat edilmelidir.

Bu yöntemle Türk Ceza Kanunu'nun 245. maddesinde düzenlenen banka ve kredi kartlarının kötüye kullanma suçu işlenmesi mümkündür.

63 Palli Hayati, s.67

64 http://ekonomi.haberturk.com/teknoloji/haber/901486-magdur-sayisi-37-milyona-cikti Erişim Tarihi: 08.12.2013

ÜÇÜNCÜ BÖLÜM

TÜRK HUKUKUNDA BİLİŞİM SUÇLARI

I. BİLİŞİM SUÇLARININ TÜRK HUKUKUNA GİRİŞİ

A. Genel Olarak

Daha önce de belirttiğimiz üzere bilişim suçlarının ortaya çıkışı, bilgisayarların yaygın olarak kullanılmaya başlanmasıyla olmuştur, bilişim suçlarının işlenme miktarının çok fazla sayılara ulaşması ve bu nedenle özellikle ceza hukuku açısından düzenleme yapılması ihtiyacının oluşması ise internetin ortaya çıkması ve bunun kişilerin kullanımına açılmasıyla gerçekleşmiştir[65].

Bilişim suçlarına yönelik ilk düzenleme 765 sayılı Türk Ceza Kanunu'na 14.06.1991 tarih ve 3756 sayılı Kanun"un 20. maddesi ile 525. maddeden sonra gelmek üzere "Bilişim Alanında Suçlar" baslığı altında 11. babın eklenmesiyle olmuştur. Bunun dışında Kanunkoyucu, bilişim sektöründeki gelişmelere paralel olarak 07.06.1995 tarih ve 4110 sayılı Kanun ile 5846 sayılı FSEK'da değişikliğe gitmiş, fikri mülkiyet kapsamında olan eser kavramının içeriğine bilişim programları ve bunları oluşturan verileri dahil etmiştir. Böylece, bilişim programları da eser olarak kabul edilerek manevi ve mali hakların kasten ihlali halinde failin cezalandırılması amaçlanmıştır[66].

23.02.1995 tarihli ve 4077 sayılı Tüketicinin Korunması Hakkında Kanunun 06.03.2003 tarihli ve 4822 sayılı Kanunla değişik 3. maddesinde mal; "elektronik ortamda kullanılmak üzere hazırlanan yazılım, ses, görüntü ve benzeri gayri maddi malları" da içerecek şekilde tanımlanmış, 9/A maddesiyle de mesafeli sözleşmelerin "…görsel, telefon ve elektronik ortamda veya diğer iletişim araçları kullanılarak" gerçekleştirilebileceği, elektronik ortamda yapılan sözleşmelerin teyit işlemlerinin yeni elektronik ortamda yapılabileceği hüküm altına alınmıştır. 15/01/2004 tarihli ve 5070 sayılı Elektronik İmza Kanununun 16. maddesiyle imza oluşturma verilerinin

65 Dülger M. Volkan, "Bilisim Suçları", İstanbul, 2004, s. 59

66 Değirmenci Olgun; s.208

izinsiz kullanımı ve 17 nci maddesiyle elektronik sertifikalarda sahtekarlık suç hâline getirilmiş bulunmaktadır[67].

5237 sayılı Türk Ceza Kanununda bilişim suçları, "Bilişim Alanında Suçlar" başlıklı ayrı bir bölümde 243 ve devamı maddelerinde düzenlenmiş bulunmaktadır. Bu bölümde "bilişim sistemine girme" (m.243), "sistemi engelleme, bozma, verileri yok etme veya değiştirme" (m.244), "banka veya kredi kartlarının kötüye kullanılması" (m.245), ve "tüzel kişiler hakkında güvenlik tedbiri uygulanması" (m.246) düzenlenmiştir. Ayrıca "nitelikli hırsızlık" başlıklı 142/2-(e) maddesinde hırsızlık suçunun bilişim sistemlerinin kullanılması suretiyle işlenmesi ve nitelikli dolandırıcılık başlıklı 158/1-(f) maddesinde düzenlenen dolandırıcılık suçunun "bilişim sistemlerinin, banka veya kredi kurumlarının araç olarak kullanılması suretiyle işlenmesi" ağırlatıcı neden olarak hüküm altına alınmıştır. Bu suç tiplerine aşağıda ayrıntılı olarak değineceğiz.

Adalet Bakanlığı tarafından, dünyadaki gelişmeler ve 5237 sayılı Türk Ceza Kanunu'nda bu konuda mevcut boşluğunu doldurulması yönünde hükümler içeren "Bilişim Ağı Hizmetlerinin Düzenlenmesi ve Bilişim Suçları Hakkındaki Kanun Tasarısı" adında kanun tasarısı hazırlamış ancak tasarı şu ana kadar yasalaşmamıştır[68].

B. 765 sayılı Türk Ceza Kanunu'nda Öngörülen Suçlar

765 sayılı Türk Ceza Kanunu, 1 Hazian 2005 tarihi itibari ile yürürlükten kaldırılmış ve yerine 5237 sayılı Türk Ceza Kanunu yürürlüğe girmiştir. Ancak bilişim hukuku süreci ile ilgili yaşanan tarihi süreci göstermesi açısından 765 sayılı T.C.K.'nın hükümlerini ele alacağız.

Bilişim suçları açısından ceza kanunlarındaki lehe ve aleyhe kanunun belirlenebilmesi için ve 5237 sayılı T.C.K.'daki bilişim suçlarına ilişkin düzenlemeleri daha iyi anlayabilmek için 765 sayılı T.C.K.'daki bilişim suçlarına ilişkin mülga düzenlemeler çalışmamızda yer almıştır.

765 sayılı T.C.K.'da yer alan suç tipleri; 525a/1 maddesindeki verilerin ele geçirilmesi suçu, 525a/2'deki başkasına zarar vermek için verilerin kullanılması, nakledilmesi veya çoğaltılması suçu, 525b/1'deki verilere veya sisteme zarar verilmesi suçu, 525b/2 maddesindeki bilgileri otomatik isleme tabi tutmuş bir sistemi

67 Bilişim Ağı Hizmetlerinin Düzenlenmesi Ve Bilişim Suçları Hakkında Kanun Tasarısı Genel Gerekçesi http://www.hukuki.net/showthread.php?17625-Bilisim-agi-hizmetlerinin-duzenlenmesi Erişi Tarihi: 01.06.2013

68 Yayci Esra, s.64

kullanarak hukuka aykırı yarar sağlanması suçu ve 525c maddesindeki verilerde sahtekârlık yapılması suçlarıdır.

5237 sayılı Türk Ceza Kanunu'nda ise bilişim suçları; esas olarak "Bilişim Alanında Suçlar" ve "özel hayata ve hayatın gizli alanına karsı suçlar" bölümünde düzenlenmiştir Ancak 5237 sayılı Türk Ceza Kanunu'nun çeşitli bölümlerinde de bilişim sistemleriyle islenmesi olanaklı olan suç tiplerine de yer verilmiştir. Bilişim alanında suçlar bölümünün 243. maddesinde "hukuka aykırı olarak bilişim sistemine girme ve sistemde kalma suçu", 244. maddesinin 1. ve 2. fıkralarında "bilişim sisteminin isleyişinin engellenmesi, bozulması, verilerin yok edilmesi veya değiştirilmesi suçu", 244. maddesinin 4. fıkrasında "bilişim sistemi aracılığıyla hukuka aykırı yarar sağlama suçu", 245. maddesinde banka veya kredi kartlarının kötüye kullanılması suçu yer almaktadır. Bunun yanında, özel hayata ve hayatın gizli alanına karsı suçlar bölümünde ise bilişim suçu olarak nitelendirilebilecek; 135. maddede "kişisel verilerin kaydedilmesi suçu", 136. maddede "kişisel verileri hukuka aykırı olarak verme veya ele geçirme suçu", 138. maddede "verilerin yok edilmemesi suçu" yer almaktadır.

Ayrıca, 5237 sayılı T.C.K.'nın farklı birçok bölümünde bilişim suçlarıyla islenmesi olanaklı olan suç tipleri de bulunmaktadır. Bunlara, T.C.K.'nın 132. maddesindeki "haberleşmenin gizliliğini ihlal suçu", 124. maddesindeki "haberleşmenin engellenmesi suçu", 125. maddesindeki hakaret suçu, 142/2-e maddesindeki "bilişim sisteminin kullanılması yoluyla islenen hırsızlık suçu", m.158/1-f maddesindeki "bilişim sisteminin kullanılması yoluyla islenen dolandırıcılık suçu", 226. Maddesindeki "müstehcenlik suçu", 228. maddesindeki "kumar oynanması için yer ve imkan sağlama suçu" örnek gösterilebilir.

a) 525a Maddesindeki Suçlar

525a maddesinde iki ayrı suç düzenlenmiştir. Bunlar;

525a/1 maddesinde yer alan *"Bilgileri otomatik olarak işleme tabi tutmuş bir sistemden, programları, verileri veya diğer herhangi bir unsuru hukuka aykırı olarak ele geçirme "* suç ile 525a/2 maddesinde yer alan *"Bilgileri otomatik işleme tabi tutmuş bir sistemde yer alan bir programı, verileri veya diğer herhangi bir unsuru başkasına zarar vermek üzere kullanma, nakletme veya çoğaltma"* suçlarıdır.

765 sayılı eski T.C.K.'da 525a/1 maddesinde düzenlenen bilişim suçunun koruduğu hukuksal değerin ne olduğu konusunda doktrinde çeşitli görüşler ortaya çıkmıştır.

Bir görüşe göre, programları, verileri veya diğer herhangi bir unsuru hukuka aykırı olarak ele geçirme fiilinde bilgisayarda yer alan bilgiyi öğrenme yani sır aleyhinde işlenmiş bir suç söz konusudur[69].

Bir başka görüşe göre, suçla korunan menfaat sırrın korunması ile ilgili olmakla birlikte, korunan menfaatin sır olarak saklanması şart değildir.Çünkü burada kişinin iznine bağlı bir alan bulunmaktadır[70].

Başka bir görüşe göre, suçun mal aleyhine işlenen cürümlerin hemen devamına konulmuş olması tesadüf değildir. Hem bilişim suçlarının T.C.K.'da yeri hem de (525c maddesinde sahtecilik suçu dışında) suçun konusu dikkate alındığında konan hukuksal değer mal varlığıdır[71].

Diğer bir görüşe göre ise, korunan hukuksal değer kişisel verilerin ve özel hayatın gizliliği de dahil, hukukça korunan her türlü çıkarlardır[72].

Başka bir görüşe göre, suçla korunan hukuksal değer, yalnızca sırrın korunması, malvarlığının korunması, bilişim sisteminin güvenliği değildir. Burada korunan hukuksal değer, kişinin, başkalarının elde etmesine izin vermediği şeylerin ele geçirilmesi ile elde ettiği her türlü değerdir[73]. Biz de bu görüşe katılmaktayız. Korunan hukuksal değerin yararın bilimsel, manevi, maddi, kişisel olup olmadığının bir önemi yoktur. Bu suç işlendiğinde her türlü değer zedelenebilir. Bu nedenle bu suçlarda korunan hukuksal değerin ne olduğu konusunda herkeşçe kabul edilebilecek bir niteleme yapabilmek esasen zordur. Bunun sebebi de bilişim teknolojilerinin sürekli yenilenmesi durağan bir yapıya sahip olmamasıdır[74].

765 sayılı eski T.C.K.'da 525a/2 maddesinde düzenlenen bilişim suçunun koruduğu hukuksal yararın da ne olduğu konusunda doktrinde çeşitli görüşler ortaya çıkmıştır; ancak en yaygın görüşe göre, maddede öngörülen çeşitli hareketlere bağlı olarak hukuksal değerde de çeşitlilik söz konusudur. "kullanma" ve "nakletme"

---

69 Yazıcıoğlu Yılmaz, s.222

70 Değirmenci Olgun, s.173

71 Karagülmez Ali, s.136'dan Ersoy Yüksel "Genel Hukuki Koruma Çerçevesinde Bilişim Suçları", Ankara Üniversitesi Siyasi Bilimler Dergisi Cilt 49, Sayı 3-4, 1994, s.166

72 Akbulut Berrin, "Türk Ceza Hukukunda Bilişim Suçları", Yayımlanmamış Doktora Tezi, Selçuk Üniversitesi, Sosyal Bilimler Enstitüsü, Konya,1999, s. 94,95

73 Dülger Murat Volkan, s.117,118

74 Karagülmez Ali, s.138

fiillerinde bilgisayarın dokunulmazlığı, "çoğaltma" fiillerinde fikri hakların korunması, özel hayatın korunması, hürriyet hakkı, mülkiyet hakkı gibi haklar koruma altına alınmıştır[75].

Esasında, 525a maddesinin 1. fıkrası ile 2. fıkrasında korunan hukuksal değer çok da farklı değildir. Her iki fıkrada da bilişim sistemindeki sayılan şeylere yönelik suç işlenmektedir[76].

765 sayılı eski T.C.K.'da 525a maddesinde suçu işleyecek kişi açısından herhangi bir özellik belirtilmediği için suçun faili herkes olabilir.

Bazı yazarlarca, bu suçun işlenebilmesi için belli bir bilgi birikimi olması gerektiği, bu nedenle bu suçların "beyaz yaka suçları" olarak değerlendirilmesini düşünen yazarlar vardır[77].

Bu suçu işleyen kişilere "hacker", "elektronik korsan", "siber terörist", "bilişim korsanı[78]" gibi isimler verilmektedir.

765 sayılı eski T.C.K.'nın 525a maddesinde suçu işleyecek kişi açısından herhangi bir özellik belirtilmediği için suçun mağduru herkes olabilir.

Mağdurun mutlaka verilerin sahibi olması gerekmez. Verilerin ele geçirilmesinden zarar görülmesi, mağdur olma açısından önemlidir[79]. Örneğin, bir fotomodelinin bir ajansa verdiği özel fotoğraflarının sistemden çalınması durumunda hem ajans hem de fotomodel mağdur olabilecektir. Ayrıca verdiğimiz örnekte de görüldüğü gibi suçun aynı anda birden fazla mağduru da olabilmektedir.

525a/1 ve 525a/2'de yer alan suçların konusu, bilgileri otomatik olarak işleme tabi tutmuş bir sistemdeki programlar, veriler veya diğer unsurlar oluşturur. Suçun konusunu oluşturan bu hususları daha önce incelediğimizden tekrar ele almayacağız. Ancak diğer unsurlar konusuna değinmek gerekirse bunlar program, veri dışındaki kişisel nitelik gösteren bilgiler şeklinde anlamak gerekir[80].

525a/1 de yer alan suçtaki hareket kavramını inceleyecek olursak, ele geçirme eylemine değinmek yerinde olacaktır. "Ele geçirme" ifadesi CD, USB, disket gibi şeyler dışında uygun bir ifade olmamıştır. Çünkü fail bilişim sistemine girdiğinde bilgilere ulaşmış ve öğrenmiş bulunmaktadır, o bilgileri ayrıca ele

75 Karagülmez Ali, s.140

76 Karagülmez Ali, s.141

77 Dülger Murat Volkan, s.119'dan "İngilizce 'white-collar crime' teriminden Türkçe'ye çevrilen 'Beyaz yaka suçları'; kavram olarak oluşumunda şiddet içermeyen, ticari alanda dolandırıcılık, güveni kötüye kullanma gibi suç tipleri için kullanılan genel addır" Black's Law Dictionary s.1590

78 Dülger Murat Volkan, s.120

79 Aynı görüş için bkz. Akbulut Berrin, s. 95

80 Karagülmez Ali, s.135

geçirmesi gerekmemektedir. Bu nedenle bu suçlar "konut dokunulmazlığının elektronik ihlaline" de benzetilmektedir. Bu nedenle ele geçirme ibaresi eleştirilmektedir[81].

Geçekten de, başkasının bilişim sistemine yetkisiz ulaşan, orada izinsiz kalan kişiye ele geçirmediğinden bahisle cezalandırma yoluna gidilememesi doğru olmayacaktır. 5237 sayılı T.C.K.'nın 243. maddesinde hukuka aykırı olarak bilişim sistemine girme ve orada kalmaya devam etme suç olarak düzenlenmiştir.

525a/2 maddesinde yer alan suçtaki hareket kavramını inceleyecek olursak, burada seçimlik hareketler mevcuttur. Bu seçimlik hareketler; kullanmak, nakletmek ve çoğaltmaktır.

Kullanmak eyleminde fail, bilişim sistemine girerek veri üzerinde çalışabilmekte yani veri üzerinde etkide bulunabilmektedir[82]. Bu eylemin gerçekleştirilebilmesi için yukarıda belirtildiği üzere Truva atı benzeri yazılımlar kullanılmaktadır[83].

Nakletmek eylemi ile fail, verileri bilişim sisteminden ağ sistemi ile çekebileceği gibi verileri taşımaya yarayan araçlarla da yapabilir. Hatta bir bilişim sisteminin ana belleğinin sökülüp taşınması da verilerin aktarımı amacı ile yapılmışsa nakletme eylemi olarak değerlendirilebilir[84].

Çoğaltmak eylemi ile fail, veriler üzerinde niteliksel bir değişiklik yapmaksızın niceliksel bir değişiklik yapmakta, verilerin kopya sayısını artırmaktadır[85].

525a/1 maddesinde yer alan suçtaki netice ele geçirmedir. Buradaki ele geçirme öğrenme olarak algılanmalıdır. Bu nedenle öğrenme ile netice gerçekleşmektedir. Hareketin gerçekleşmesi ile netice de gerçekleşir. Bu suçlar harekete bitişik suçlardır[86]. Bu suçta zarar oluşması gerekmez. Bu suç zarar suçu değil, tehlike suçudur.

525a/2 maddesinde yer alan suçtaki netice, hareketin çeşitliliği nedeniyle birden fazla olabilir. Hareketin gerçekleşmesi ile netice de gerçekleşir. Bu suçlar

81 Karagülmez Ali, s.136

82 Akbulut Berrin, s.125

83 Dülger Murat Volkan, s.141

84 Akbulut Berrin, s.125; YAZICIOĞLU Yılmaz s.249; DÜLGER Murat Volkan, s.141

85 Akbulut Berrin, s.125; YAZICIOĞLU Yılmaz, s.249; DÜLGER Murat Volkan, s.141

86 Yazicioğlu Yılmaz, s.250, 251

harekete bitişik suçlardır[87]. Bu suçta zarar oluşması gerekmez. Bu suç zarar suçu değil, tehlike suçudur.

525a/1 maddesinde yer alan suç, bilerek ve isteyerek genel suç işleme kastı ile işlenir. Fail, bu suçta bilişim sisteminde bulunan verileri haksız olarak ele geçirdiğini, hukuka aykırı olarak hareket ettiğini bilmesi yeterlidir. Failin belli bir saikle hareket etmesi gereken özel kast durumu bu suç için geçerli değildir[88]. Sanığın veya başkasının bu eylemden fiilen zarar görmesi gerekli değildir[89].

525a/2 maddesinde yer alan suçun işlenebilmesi için 525a/1 den farklı olarak sayılan fiillerin başkasına zarar verme özel kastıyla gerçekleştirilmesi gerekir. Bu zarar maddi olabileceği gibi manevi de olabilir[90]. Burada sanığın zarar verme özel kastıyla hareket etmesi öngörülmüş ise de bu zararın gerçekleşmesi gerekmez. Yukarıda da belirttiğimiz üzere zarar verme ihtimalinin bulunması yeterlidir.

525a maddesindeki suçların failin bilerek ve isteyerek hareket etmesi şartını aradığından bu suçların taksirle işlenmesi mümkün değildir

525a maddesinde belirtilen suçların hukuka uygunluk sebebini hak sahibi kişinin rızası oluşturacaktır. Ancak kişiye verilen rızanın sınırları aşıldığında tekrardan hukuka aykırılık oluşacaktır. Örneğin, bilgisayarda internete girilmesine izin verdiğimiz bir kişi, sistemin içindeki bütün verileri yok etme ya da zarar verme cihetine giderse verilen iznin sınırlarını aşmış olmakta ve hukuka aykırılık unsuru oluşmaktadır.

Bir suç kanunun verdiği yetkiye dayanarak işlendiğinde de hukuka uygunluk kazanabilmektedir. 525a/1 maddesinde yer alan suç ile ilgili 4422 sayılı mülga Çıkar Amaçlı Suç Örgütleriyle Mücadele Kanunu'nun 2. ve 4. maddesinde bu tür bir hukuka uygunluk nedeni bulunmaktaydı. Bu maddelerde bir kamu görevlisinin çıkar amaçlı bir suç örgütlenmesi içinde bulunduğundan şüphelendiği kişilerin bilişim sistemine girerek veri ele geçirilmesi suç oluşturmuyordu[91].

765 sayılı T.C.K.'nın 525. maddesinde değişiklik yapan 3756 sayılı Kanun'un, TBMM'ye sevk edilen halinde, bu suça teşebbüs durumunda da suç tamamlanmış gibi ceza verilmesi düzenlenmişken, komisyon görüşmelerinde bu husus çıkarılmıştır. Ancak madde gerekçesinde *"Birinci ve ikinci fıkrada yer alan*

87 Yazicioğlu Yılmaz, s.250, 251

88 Akbulut Berrin, s.118; DEĞRMENCİ Olgun, s.179

89 Karagülmez Ali, s.140

90 Karagülmez Ali, s.141

91 Dülger Murat Volkan, s.129

suçların teşekkülü için failin bir yarar elde etmesi veya başkası için fiilen bir zararın meydana gelmiş bulunması şartı yoktur, fiile teşebbüs etmiş olması yeterlidir" denilmektedir. Bu durumda gerekçe ile madde metni arasında çelişki olduğu görülmektedir[92]. Asıl olan madde metnidir, madde metninde de teşebbüs yer almadığı için, kanunun genel hükümlerine bakmak gerekir. Genel hükümlere bakıldığında yukarıda da belirtildiği üzere bu suçlara harekete bitişik suçlardır. Bu nedenle bu suçlara tam teşebbüs mümkün gözükmemektedir. Ancak elektrik kesilmesi gibi failin elinde olmayan nedenlerle eylemin yarıda kalması durumunda eksik teşebbüs derecesinde kalabilecektir[93]. KARAGÜLMEZ'e göre ise bu suçlara eksik ve tam teşebbüs mümkündür[94].

765 sayılı T.C.K.'da yer alan verilerin ele geçirilmesi suçunda (525a/1) ve verileri başkasına zarar vermek amacı ile kullanmak, nakletmek ve çoğaltmak suçunda (525a/2) iştirak açısından bir özellik söz konusu olmayıp, genel hükümler uygulanacaktır. Genel hükümler değerlendirildiğinde bu suç tipleri için iştirak türlerinin gerçekleşmesi mümkündür[95].

765 sayılı T.C.K.'da yer alan verilerin ele geçirilmesi suçunda (525a/1) ve verileri başkasına zarar vermek amacı ile kullanmak, nakletmek ve çoğaltmak suçunda (525a/2) suçların içtimaı mümkündür.

b) 525b Maddesindeki Suçlar

525b/1'de yer alan *"Başkasına zarar vermek veya kendisine veya başkasına yarar sağlamak maksadıyla, bilgileri otomatik işleme tabi tutmuş bir sistemi veya verileri veya diğer herhangi bir unsuru kısmen veya tamamen tahrip etme veya değiştirme veya silme veya sistemin işlemesine engel olma veya yanlış biçimde işlemesini sağlama suçu"* ile

525b/2 maddesinde yer alan *"Bilgileri otomatik işleme tabi tutmuş bir sistemi kullanarak kendisi veya başkası lehine hukuka aykırı yarar sağlama*" suçlarıdır.

765 sayılı eski T.C.K.'da 525b/1-2 maddesinde düzenlenen bilişim suçunun koruduğu hukuksal değerin ne olduğu konusunda doktrinde çeşitli görüşler ortaya çıkmıştır.

92 Karagülmez Ali, s.139.140

93 Aynı görüş için bkz. Dülger Murat Volkan, s.144

94 Karagülmez Ali, s.140

95 Akbulut Berrin, s.197; Değrmenci Olgun, s.181,182

Bir görüşe göre, maliklerin rızaları dışında müdahaleye uğramalarının önlenmesi amaçlanmakta, bilişim sistemi içerisindeki unsurlar bakımında sahip oldukları mülkiyet hakkı koruma altına alınmaktadır[96].

Bir başka görüşe göre, korunan hukuksal değer, sistem, program veya verinin maliki veya kullanıcısının bunlar üzerindeki tasarruf hakkıdır. Üstelik bu fıkra, kullanıcıya yönelik fiillerde de uygulanabilir[97].

Başka bir görüşe göre, bu suç bilişim sistemin fiziki yapısını değil, verileri koruduğu için, korunan hukuksal değer de, kişinin verilerde olan bilgilere herhangi bir engel olmadan erişebilmesindeki çıkarıdır[98].

Diğer bir görüşe göre ise, korunan hukuksal değer bilişim sisteminin, özelinde de veri ve diğer unsurların dokunulmazlığıdır[99].

Esasında, 525b maddesinin 1.fıkrası ile 2.fıkrasında korunan hukuksal değer bilişim sistemindeki sayılan şeylere yönelik suç işlenmektedir.

765 sayılı eski T.C.K.'da 525b maddesinde suçu işleyecek kişi açısından herhangi bir özellik belirtilmediği için suçun faili herkes olabilir. Ancak kişinin sadece kendi sistemine veya verilerine zarar vermesi suç oluşturmayacağından, verilerin kayıtlı olduğu bilişim sisteminin veya verilerin mülkiyet, kullanım ve tasarruf haklarının kime ait olduğunu ve zararı kimin meydana getirdiğini açıkça ortaya koymak gerekmektedir[100].

765 sayılı eski T.C.K.'nın 525b/1 maddesinde, mağdurun mutlaka verilerin sahibi olması gerekmez. Verilere veya veri işleme zarar verilmesi durumunda verilerle oluşturulan yazılım, ekonomik bilgiler, bilimsel çalışmalara vb. değerlere herhangi bir engel arıza ya da gecikme olmaksızın ulaşılması ve kullanılmasında çıkarı bulunan ve veriler üzerinde tasarruf yetkisi bulunan kişi de suçun mağduru olacaktır.[101] Buna göre verilere veya veri işleme zarar veren kişinin bilişim sisteminin maliki veya kullanım hakkı sahibi olmasına göre suçun mağduru da değişecektir[102].

96 Yazicioğlu Yılmaz, s.259,260

97 Değirmenci Olgun, s.187

98 Akbulut Berrin, s.130; DÜLGER Murat Volkan, s.148

99 Karagülmez Ali, s.143

100 Akbulut Berrin, s. 131

101 Akbulut Berrin, s. 132

102 Dülger Murat Volkan, s.150

765 sayılı eski T.C.K.'da 525b/2 maddesinde, mağdurun bilişim sisteminin maliki ya da zilyedi olarak sınırlandırmak mümkün değildir. Bankaların, finansman kuruluşların bilişim sistemine hukuka aykırı şekilde girildiği, hem sistemin maliki ya da zilyedi olan şirket, hem de şirketin müşterisi olan mudi zarar görmektedir. Bu nedenle ikinci fıkra da mağdur, mal varlığında azalma olan kişi veya kişilerdir[103].

765 sayılı T.C.K.'nın 525b/1 maddesinde yer alan suçun konusu veridir. Hiçbir veri bulunmayan bilişim sistemi bu suçun konusunu oluşturmayacaktır[104]. Örneğin, mağazanın vitrinin satışa sunulmuş bir bilgisayara zarar verildiğinde, zarara uğrayan bilgisayar 525b/1'in konusunu oluşturmayacaktır. 516. maddede yer alan nası ızrar suçunu oluşturacaktır[105].

765 sayılı T.C.K.'nın 525b/1 maddesinde yer alan suçun konusu ise müelliflerce tartışmalı olmakla birlikte bize göre, failin sağladığı hukuka aykırı yarardır diyebiliriz.

Kanun metninde çeşitli hareketler yazılmıştır. Şimdi bu hareket çeşitlerine göz atalım.

Tahrip etmek eylemi kelime olarak yıkma, kırıp dökme, harap etme, bozma anlamlarına gelmektedir[106]. Yasada anlatılmak istenen ise bilişim sistemine ya da veriye tamir edilemeyecek zarar verme kastedilmektedir[107]. Değiştirmek eylemiyle verilerin bir kısmına ya da tamamına yeni veriler eklenmesi ya da verilerin çıkartılması kastedilmektedir. Silme eylemiyle verilerin bir kısmını ya da tamamının ortadan kaldırılması yok edilmesi kastedilmektedir.

Sistemin işlemesine engel olma veya yanlış biçimde işlemesini sağlama, bu hareketle bilişim sisteminden elde edilecek faydanın engellenmesi ya da yanlış çalışarak fayda yerine zarar verme amaçlanmaktadır. Kanunkoyucu burada tahrip etmek dışındaki tüm hareketleri dahil etmiştir[108].

525b/2'deki hareket eylemi, bilişim sistemiyle hukuka aykırı yarar sağlamak suçu Kanunkoyucu tarafından serbest hareketli bir suç olarak düzenlenmiştir. Eylem nasıl gerçekleşirse gerçekleşsin önemli olan neticede kanunda belirtilen hukuka aykırı yararın elde edilmesidir. Bu hareket genelde şifreli yayınlara, telefon

103 Dülger Murat Volkan, s.165

104 Değirmenci Olgun, s.189

105 Akbulut Berrin, s. 133

106 Güncel Türkçe Sözlük www.tdk.gov.tr

107 Akbulut Berrin, s. 134

108 Akbulut Berrin, s. 139

hatlarına hukuka aykırı olarak girip yarar sağlama şeklinde kendini göstermektedir. T.C.K.'nın 525 b/2 fıkrasında düzenlenen "bilişim sistemi aracılığıyla hukuka aykırı yararın elde edilmesi suçunun" banka ve kredi kartlarının kullanılmasıyla hukuka aykırı yarar elde edilmesini kapsayıp kapsamadığı konusunda farklı düşünceler var olsa da, YCGK'nun bu konuda verdiği karar[109] ile bu tartışmalar son bulmuştur. Banka ve kredi kartlarının kullanılmasıyla hukuka aykırı yarar elde edilmesi de 525 b/2 maddesi kapsamında kalmaktadır[110]. YCGK'nun bu kararı 5237 sayılı kanunun 245. maddesinin düzenlenmesine ilham olmuştur.

525b/1-2 de yer alan suçlarda netice bir yararın elde edilmesidir. Her iki fıkrada zarar suçudur. Bu suçlarda zararın meydana gelmemesi mümkün değildir. Zira söz konusu hareketler bilişim sistemine zarar verme odaklanmıştır[111].

525b/1 de yer alan suç, kanunda "başkasına zarar vermek veya kendisine yarar sağlamak maksadıyla" demekle suçun özel kast ile işleneceğini belirtmiştir. *525a/2 de yer alan* suçun işlenebilmesi için "bir sistemi kullanarak kendisi veya başkası lehine hukuka aykırı yarar sağlayan" demekle suçun özel kast ile işleneceğini belirtmiştir. 525b deki suçlar failin bilerek ve isteyerek hareket etmesi şartını aradığından bu suçların taksirle işlenmesi mümkün değildir

765 sayılı T.C.K. 525b maddesindeki suçlarda failin yarar sağladığı veya başkasının zararına bilişim sistemindeki hareketleri rızaya dayanarak gerçekleştirdiği halde suç oluşmayacaktır. Çünkü yasanın öngördüğü hukuka aykırılık bu durumda ortadan kalkacaktır[112].

765 sayılı T.C.K.'da yer alan 525b/1 maddesinde yer alan *"Başkasına zarar vermek veya kendisine veya başkasına yarar sağlamak maksadıyla, bilgileri otomatik işleme tabi tutmuş bir sistemi veya verileri veya diğer herhangi bir unsuru kısmen veya tamamen tahrip etme veya değiştirme veya silme veya sistemin işlemesine engel olma veya yanlış biçimde işlemesini sağlama suçu"* ile 525b/2'de yer alan *"Bilgileri otomatik işleme tabi tutmuş bir sistemi kullanarak kendisi veya başkası lehine hukuka aykırı yarar sağlama*" iştirak açısından bir özellik söz konusu olmayıp, genel

109 YGCK 10.04.2001, 2001/76-30 E, 2001/757 K, ""…….Yukarıdaki açıklamalar ışığında somut olay değerlendirildiğinde, sanığın haksız olarak ele geçirdiği bir başkasına ait kart ve şifreyi kullanarak bir bankanın iki farklı şubesindeki ATM makinesinden para çekip hukuka aykırı yarar sağlaması eylemi TCY'nin 493/2. madde ve fıkrasındaki suçu değil aynı yasanın 525/b.2 madde ve fıkrasında düzenlenen bilgileri otomatik isleme tabi tutmuş bir sistemi kullanarak hukuka aykırı yarar sağlamak suçunu oluşturduğundan Yargıtay C. Başsavcılığı'nın itirazının kabulüne karar verilmelidir."
(UYAP Mevzuat Programı)

110 Dülger, Murat Volkan, s.260

111 Dülger Murat Volkan, s.156

112 Değirmenci Olgun, s.194; Akbulut Berrin, s. 176

hükümler uygulanacaktır. Genel hükümler değerlendirildiğinde bu suç tipleri için iştirak türlerinin gerçekleşmesi mümkündür[113].

765 sayılı T.C.K.'da yer alan 525b/1 maddesinde yer alan *"Başkasına zarar vermek veya kendisine veya başkasına yarar sağlamak maksadıyla, bilgileri otomatik işleme tabi tutmuş bir sistemi veya verileri veya diğer herhangi bir unsuru kısmen veya tamamen tahrip etme veya değiştirme veya silme veya sistemin işlemesine engel olma veya yanlış biçimde işlemesini sağlama"* suçu ile 525b/2'de yer alan *"Bilgileri otomatik işleme tabi tutmuş bir sistemi kullanarak kendisi veya başkası lehine hukuka aykırı yarar sağlama*" suçunda, suçların içtimaı mümkündür.

c) 525c Maddesindeki Suçlar

765 sayılı T.C.K.'da "Hukuk alanında delil olarak kullanılmak maksadıyla sahte bir belgeyi oluşturmak için bilgileri otomatik olarak işleme tabi tutma bir sisteme, verileri veya diğer unsurları yerleştirme veya var olan verileri, diğer unsurları tahrif etme" eylemi suç olarak düzenlenmiştir.

525c maddesinde korunan hukuksal değer, önceki maddelerden farklı olarak, genel sahtekârlık suçları ile korunmak istenilen ile aynıdır. Burada, sahtekârlığın konusunu teşkil eden elektronik belgelerin güvenirliği korunmak istenmiştir. Bu da güvenin devletçe garanti altına alınması gayesiyle ilgilidir[114].

765 sayılı eski T.C.K.'da 525c maddesinde verilerde sahtekarlık yapılması ve üretilen sahte belgelerin kullanılması suçunu işleyecek kişi açısından herhangi bir özellik belirtilmediği için suçun faili herkes olabilir.

765 sayılı T.C.K.'nın 525c maddesinde verilerde sahtekarlık yapılması ve bu belgelerin kullanılmasında mağdur her zaman devlettir. Bu suçlarda Kamuya olan güven ve inanç zedelenmektedir[115].

Hukuk alanında delil olarak kullanılabilecek bilişim sistemindeki her türlü veridir. Her ne kadar madde metnin de diğer unsurlar denmiş ise de, bunun bu maddede veri olarak anlaşılması gerekir[116].

Kanun metninde yazılı çeşitli hareketleri inceleyelim.

Sisteme, veri yerleştirme, Veri yerleştirmek, sahte belge oluşturmaya çalışılan belgede var olmayan bilgilerin, belgeye geçirilmesi bir başka deyişle belgeye

113 Yazicioğlu Yılmaz, s. 265.

114 Değirmenci Olgun, s.200; Dülger Murat Volkan, s. 196,197; Karagülmez Ali, s.148

115 Akbulut Berrin, s. 182; Dülger Murat Volkan, s.197; Değirmenci Olgun, s.201

116 Dülger Murat Volkan, s.197, dn.380

yüklenmesidir[117]. Bilişim sistemine veri yerleştirmek elektronik iletişim ile yapılabileceği gibi, manüel (el ile) de yapılabilir[118].

Sistemin içindeki sahte belgenin kağıda dökülmemiş olması ya da maksadına ulaşamamış olması durumunda, suç ortadan kalkmaz. Gerçekten de maddenin sonuna bakıldığında kullanılması farklı cezalandırılmaktadır[119].

Sistemdeki verileri tahrif etme, verilerin tahrif edilmesi ile verilerin söz konusu belgelerin sahteleştirilmesi amacıyla herhangi bir şekilde değiştirilmesi kastedilmektedir. Bu değiştirme, veri ekleme, veri çıkarma, veri değiştirme gibi şekillerde olabilir[120]. 765 sayılı T.C.K.'nın 525c maddesi, 339 ve devamı maddeleri gereğince özel hüküm sayılamaz. Zira 525c olmasaydı 339 ve devamı maddelerinden ceza verilemeyecekti. Bilişim sistemi kullanılarak sahte belge düzenlendiğinde, evrakın resmi veya özel olmasına göre 765 sayılı T.C.K.'nın 79. maddesi gereğince, daha ağır cezayı gerektiren madde hükmüne göre ceza verilecektir.[121].

765 sayılı T.C.K.'nın 525c maddesinde düzenlenen verilerde sahtecilik ve oluşturulan sahte belgenin kullanılması suçlarının her ikisi de tehlike suçudur. Suçun oluşumu için zarar aranmaz[122]. Verilerde sahtecililik suçunda birden fazla hareket belirlenmişse de sonuçta sahte bir belgenin oluşması amaçlanmakta, neticede farklılık olmamaktadır.

525c maddesinde failin suçu, sahte belgeyi hukuk alanında delil olarak kullanmak maksadıyla bilerek değiştirmesi veya tahrif ederek bilerek kullanması söz konusu olduğundan özel kast arandığı görülmektedir. 765 sayılı T.C.K.'nın 525c maddesindeki suçlarda failin, bilerek ve isteyerek hareket etmesi şartı arandığından bu suçların taksirle işlenmesi mümkün değildir

Daha önce de belirttiğimiz üzere bu suçun mağduru devlettir. Bu nedenle mağdurun rızası hukuka uygunluk sebebi kabul edilemez. Bunun yanında bu suçla ilgili başkaca yasal hukuka uygunluk sebebi bulunmamaktadır.

765 sayılı T.C.K.'nın 525c maddesinde yer alan *"Hukuk alanında delil olarak kullanılmak maksadıyla sahte bir belgeyi oluşturmak için bilgileri otomatik olarak işleme tabi tutan bir sisteme, verileri veya diğer unsurları yerleştirme veya*

117 Karagülmez Ali, s.149; Yazicioğlu Yılmaz, s.283

118 Değirmenci Olgun, s.202

119 Karagülmez Ali, s.150

120 Dülger Murat Volkan, s.200

121 Karagülmez Ali, s.151

122 Akbulut Berrin, s. 192; Dülger Murat Volkan, s.203; Yazicioğlu Yılmaz, s.284,285

var olan verileri, diğer unsurları tahrif etme, tahrif edilmiş olanları bilerek kullanma" suçlarının iştirak açısından bir özellik söz konusu olmayıp, genel hükümler uygulanacaktır. Genel hükümler değerlendirildiğinde bu suç tipleri için iştirak türlerinin gerçekleşmesi mümkündür[123].

765 sayılı T.C.K.'nın 525c maddesinde düzenlenen bu suçta, suçların içtimaı mümkündür.

d) 525d Maddesindeki Suçlar

765 sayılı T.C.K. 525d *"525 a ve 525 b maddeleri hükümlerini ihlal eden kişiler hakkında, maddelerde yazılı cezalara ek olarak,meslek icrası sırasında veya icrası dolayısıyla suçun işlendiği bir kamu hizmetinden veya meslek veya sanat veya ticaretten altı aydan üç yıla kadar yasaklanma cezası da verilir."*

Görüldüğü üzere bu madde fer'i ceza düzenlemiştir. Ancak 525c maddesinden mahkum olanlar için bu maddenin uygulanmayacağı dikkatlerden kaçmamalıdır.

C. 5237 Sayılı T.C.K. İle 765 Sayılı T.C.K.'da Düzenlenen Bilişim Suçlarının Karşılaştırılması

Her iki kanun arasında göze çarpan ilk fark, 5237 sayılı T.C.K.'nın 243. maddesinde yer alan *"hukuka aykırı olarak bilişim sistemine girme ve sistemde kalma suçu"* ile ilgili düzenlemenin 765 sayılı T.C.K.'da hiç yer almamasıdır. Hemen şunu belirtmek gerekir ki birçok mevzuatta eski ve yeni T.C.K. karşılaştırılmasında 765 sayılı T.C.K.'nın 525a maddesi, 5237 sayılı T.C.K.'nın 243. maddesiyle eşleştirilmektedir. Bu bize göre doğru değildir. 525a maddesindeki gibi 243. madde de ele geçirme suçu bulunmamaktadır[124]. Ancak uygulamada ele geçirme olmasa da sisteme girme durumunda 765 sayılı T.C.K.'nın 525a maddesi uygulandığından bu eşleşme yapılmaktadır. Aslında, bu suç tipi 5237 Sayılı T.C.K. ile Türk Ceza Hukukuna girmiş bulunmaktadır[125]. Böylece verilerin ele geçirilmesi şartı aranmaksızın bilişim sistemine girilmesi suç olarak düzenlenmiştir[126].

Ayrıca 5237 sayılı T.C.K.'nın 135. maddesinde düzenlenen *"kişisel verilerin kaydedilmesi suçu"*, 136. maddesinde düzenlenen *"kişisel verileri hukuka aykırı olarak verme veya ele geçirme suçu"*, 245. maddesinde düzenlenen *"banka veya*

123 Akbulut Berrin, s.,213; DÜLGER Murat Volkan, s.205; YAZICIOĞLU Yılmaz, s.286

124 Karagülmez Ali, s.151

125 Dülger Murat Volkan, s.211,213

126 Akbulut Berrin, s.78; DEĞİRMENCİ Olgun, s,152,153

kredi kartlarının kötüye kullanılması suçu", 142/2-e'de düzenlenen *"bilişim sisteminin kullanılması suretiyle nitelikli hırsızlık suçu"* ve 158/1-f'de düzenlenen *"Bilişim sistemlerinin, banka veya kredi kurumlarının araç olarak kullanılması suretiyle dolandırıcılık suçu"*, 765 sayılı T.C.K.'dan farklı olarak bağımsız bilişim suçu tipleri olarak düzenlenmiştir.

765 sayılı T.C.K.'da yer alan 525a/2 maddesinde düzenlenen "bilgileri otomatik isleme tabi tutmuş bir sistemde yer alan bir program, veri veya diğer herhangi bir unsuru başkasına zarar vermek üzere kullanma, nakletme veya çoğaltma suçuna ise 5237 sayılı T.C.K.'da yer verilmemiştir[127].

765 sayılı eski T.C.K. ile 5237 sayılı yeni T.C.K.'nın bilişim suçları yönünden maddeler arası karsılaştırılması aşağıdaki gibidir.

765 s. T.C.K. m. 525a/1	5237 Sayılı T.C.K. m.135, m. 136
765 s. T.C.K. m. 525b/1	5237 Sayılı T.C.K. m.244/1–2
765 s. T.C.K. m. 525b/2	5237 Sayılı T.C.K. m.244/4, 245,158/1-f,142/2-e

5237 sayılı T.C.K.'da "bilgileri otomatik olarak isleme tabi tutan sistem" ve "diğer herhangi bir unsur" ifadeleri yerine "bilişim sistemi" kavramı kullanılmıştır. Böylece kavram karışıklığına son verilmiştir,[128]

Bunların yanında, 5237 sayılı T.C.K. ile kanunun sistematiğinde değişikliğe gidilerek bilişim suçları, korudukları hukuksal değer gözetilerek düzenlenmiştir. Ancak "banka ve kredi kartlarının kötüye kullanılması suçu" açısından bir ayrım yapılmayarak koruduğu hukuksal değer gözetilmeksizin bilişim sistemlerine karşı suçlar bölümünde düzenlenmiştir[129].

II. 5237 SAYILI TÜRK CEZA KANUNU'NDA DÜZENLENEN BİLİŞİM SUÇLARI

A. GENEL OLARAK

Bilişim suçları, öğretide ve uygulamada öncelikle, doğrudan bilişim suçu (gerçek bilişim suçları), dolayısıyla bilişim suçu (bilişim bağlantılı suçlar) biçiminde tasnife tabi tutulmuştur. Türk Ceza Kanununda da bu sistem kabul edilmiştir[130].

127 Dülger Murat Volkan, s.211

128 Yayci Esra, s.67

129 Dülger Murat Volkan, s.210

130 YCGK., 17.11.2009 T., 2009/11-193 E., 2009/268 K.

Bilişim suçları, 5237 sayılı T.C.K.'da 10.bölümde yer almaktadır. Çalışmanın bu kısmında ilk önce bu kısımdaki gerçek bilişim suçlarını ardından T.C.K.'da bilişim suçları ile bağlantılı olan T.C.K.'nın 132. maddesinde düzenlenen "haberleşmenin gizliliğini ihlal", T.C.K.'nın 133. maddesinde düzenlenen "kişiler arasındaki konuşmaların dinlenmesi ve kayda alınması", T.C.K.'nın 134. maddesinde düzenlenen "özel hayatın gizliliğini ihlal", T.C.K.'nın 135. maddesinde düzenlenen "kişisel verilerin kaydedilmesi suçu", 136. maddesinde düzenlenen "kişisel verileri hukuka aykırı olarak verme veya ele geçirme suçu", 245. maddesinde düzenlenen "banka veya kredi kartlarının kötüye kullanılması suçu", 142/2-e'de düzenlenen "bilişim sisteminin kullanılması suretiyle nitelikli hırsızlık suçu" ve 158/1-f'de düzenlenen "Bilişim sistemlerinin, banka veya kredi kurumlarının araç olarak kullanılması suretiyle dolandırıcılık suçu", gibi suçları inceleyeceğiz.

B. TÜRK CEZA KANUNU'NDA "BİLİŞİM ALANINDA SUÇLAR" BÖLÜMÜNDE DÜZENLENEN SUÇ TİPLERİ

a. Hukuka Aykırı Olarak Bilişim Sistemine Girme ve Sistemde Kalma Suçu[131]

1. Genel Olarak

5237 sayılı Türk Ceza Kanunu'nun "Bilişim sistemine girme" başlıklı 243.maddesi ile "bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak girme ve orada kalmaya devam etme" eylemi suç tipi haline getirilmiştir. Yukarıda da açıkladığımız üzere, 765 sayılı Türk Ceza Kanunu'nun 525a/1 maddesindeki verilerin ele geçirilmesi suçu konusundaki eleştiriler dikkate alınarak bu madde ile veriler ele geçirilmeksizin verilere yetkisiz erişim eylemleri suç tipi haline getirilmiştir.

Avrupa Siber Suç Sözleşmesi[132]'nin "Yasadışı erişim" baslıklı 2. maddesindeki düzenleme dikkate alındığında, Türk Ceza Kanunu'nun 243. maddesi ile bu düzenleme arasında paralellik bulunduğu görülmektedir.

Bu suç tipine, mukayeseli hukukta birçok ülke hukukunda yer verilmektedir. Örnek olarak; Fransa CK. m. 323–1, Alman CK. m. 202a, Danimarka CK. m.193 ve

131 5237 sayılı T.C.K.'nın "Bilişim sistemine girme" başlıklı 243. maddesi

"[1] Bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak giren ve orada kalmaya devam eden kimseye bir yıla kadar hapis veya adlî para cezası verilir.

[2] Yukarıdaki fıkrada tanımlanan fiillerin bedeli karşılığı yararlanılabilen sistemler hakkında işlenmesi hâlinde, verilecek ceza yarı oranına kadar indirilir.

[3] Bu fiil nedeniyle sistemin içerdiği veriler yok olur veya değişirse, altı aydan iki yıla kadar hapis cezasına hükmolunur."

132 Özen Muharrem/ Baştürk İhsan, s.354

263, Norveç CK. m. 145/2, İtalyan CK. m. 616/2, 617 guarter, 617 guinguies, 618, Lüksembourg CK. m. 309, İrlanda Criminal Damage Act'de m. 5/1, Hollanda CK. m. 98, 98a, 98b, 98c ve 273 verilebilir[133].

2. Korunan Hukuksal Değer

Korunan değere suçun hukuki konusu da denir. Her suçta nasıl bir fail varsa bir de korunan hukuksal değer vardır. Bu hukuksal değer, suç tarafından ihlal edilen hukuki varlık ve değer ya da menfaattir[134]. Varlık, insanın ihtiyaçlarını tatmine elverişli her şeyi, menfaat ise, kişi ile varlık arasında olan ve kişinin bir ihtiyacını tatmin için varlığı kullanmasına imkan veren ilişkiyi ifade eder[135].

Bilişim sistemine girme ve sistemde kalma suçunun hukuksal değerinin ne olduğu konusu ile ilgili doktrinde çeşitli görüşler bulunmaktadır.

Bir görüşe göre, bu suçla birden fazla hukuksal değer korunmak istenmiştir. Bunlar, verilerin gizliliğinin korunması, özel hayatın dokunulmazlığı, kişilerin ve kurumların ihtiyaç duyduğu güvenlik duygusunun korunması değerleridir. Bu görüşü savunan yazar tüm bu hukuksal değerlerin "bilişim sistemin güvenliği" hukuksal değeri bünyesinde korunacağını savunmaktadır[136]. Bu görüşü başka yazarlar da savunmaktadır[137].

Bir başka görüşe göre, T.C.K.'nın 243. maddesinde yer alan suçun maddi unsurunun sadece sisteme yetkisiz erişim olmadığı, bunun yanında sistemde kalmaya devam etme unsurunun da arandığı, suçun unsurunun bu şekilde düzenlenişinin suçun hukuki konusunun belirlenmesinde de etkili olduğu vurgulanmaktadır. Bu açıdan bilişim sisteminin güvenliğinin korunmasına yönelik bir düzenlemede "kalmaya devam etme" seklinde bir unsura yer verilmeyeceği; aynı şekilde 2. fıkrada yer alan düzenlemenin de hukuki konunun bilişim sisteminin güvenliği olduğu düşüncesini zayıflattığı ifade edilerek, suçta "kalmaya devam etme" nin suçun unsuru olmasını esas alarak bu suçun korunan hukuksal değerinin, bilişim sistemini kullananların belirli bir süreden sonra rahatsız edilmemesi ve devamında suçun

133 Dülger Murat Volkan, s.213

134 Soyaslan, Doğan, (Genel Hükümler) s.227

135 Toroslu Nevzat, s.65

136 Dülger Murat Volkan, s.213,214, Aynı görüş için bkz. Parlar Ali/Hatipoğlu Muzaffer, "5237 sayılı T.C.K.'da Özel Ve Genel Hükümler Bakımında Sulh Ceza Davaları", Ankara, Nisan 2010, s.214

137 Özbek Veli Özer/Kanbur M. Nihat/Doğan Koray/Bacaksiz Pınar/Tepe İlker, "Türk Ceza Hukuku; Özel Hükümler", Ekim 2010, Ankara, s.896

hedefi durumundaki sistem kullanıcılarının (sahiplerinin) çıkarlarının zedelenmemesinin de hukuki konu kapsamında olduğu belirtilmektedir[138].

Başka bir görüşe göre[139], *"Türk Ceza Kanunu'nda bilişim alanında islenen suçlar içerisinde 243. maddede düzenlenen yetkisiz erişim suçunda bir zarar tehlikesinin esas alındığı görülmektedir. Bu haliyle de yetkisiz erişim suçunun hukuki konusu, 243.maddede düzenlendiği şekliyle, malvarlığının korunması kapsamında mala zarar verme suçunun özel şekli olarak düzenlenen 244. maddenin hukuki konusu ile paralellik arz etmektedir. Bu açıdan 243. maddede düzenlenen yetkisiz erişim suçunun hukuki konusu, sisteme ve veriye yönelik zarar verici fiillerin engellenmesi anlamında bir tehlike suçu olarak, genel bir ifade ile mülkiyetin korunmasıdır. Bu haliyle de, sırrın korunması ya da konut dokunulmazlığı korunması seklinde ortaya çıkan, özel hayatın gizliliğinin korunmasına ilişkin değerin ikinci plana itildiği görülmektedir."* Ketizmen doktora tezinde karşılaştırmalı hukuktan örnekler de vererek korunan hukuki değerin mal varlığı olduğunu savunmaktadır.

Diğer bir görüşe göre, bu suçla korunan hukuksal değer karma nitelik taşımaktadır. Hem bilişim sisteminin güvenirliği, hem kişilerin özel hayatı, hem de sistemi kullananlarının çıkarları korunmaktadır[140].

Bizce, bu suçta korunan hukuksal değer, bilişim sistemin güvenliğidir. Yetkisiz erişim sağlandıktan sonra, sistem de belli süre kalmak kişinin amacını belirlemek ile alakalıdır[141]. Gerçekleştirilen eylem bilişim sisteminin güvenliğine ilişkin olan harekettir.

3. Suçun Maddi Unsurları

Suçun maddi unsuru dendiğinde anlaşılması gereken o suçun işlenmesinde gerekli olan hareketler sonucunda neticenin meydana gelmesi ve hareket ile netice arasında nedensellik bağının bulunmasıdır[142].

Aşağıda suçun maddi unsurları olan aktif süje, pasif süje, hareket, netice, suçun unsuru ve nedensellik bağına değineceğiz.

3.1. Fail

5237 sayılı T.C.K.'daki 243. maddesinde suçu işleyecek kişi açısından herhangi bir özellik belirtilmediği için suçun faili herkes olabilir.

---

138 Karagülmez Ali, s.179,180

139 Ketizmen Muammer," Türk Ceza Hukuku`nda Bilişim Suçları", Doktora Tezi, Ankara Üniversitesi, Sosyal Bilimler Enstitüsü, Ankara 2006 s.119.120

140 Taşkin Şaban Cankat, s.23

141 Özbek Veli Özer/KANBUR M. Nihat/DOĞAN Koray/BACAKSIZ Pınar/TEPE İlker, s.896, 897

142 SOYASLAN, Doğan, (Genel Hükümler) s.220, 221

Bazı yazarlarca, bu suçun işlenebilmesi için belli bir bilgi birikimi olması gerektiği, bu nedenle bu suçların "beyaz yaka suçları" olarak değerlendirilmesini düşünen yazarlar vardır[143].

Bu suçu işleyen kişilere "hacker", "elektronik korsan", "siber terörist", "bilişim korsanı" gibi isimler verilmektedir.

Tüzel kişilerin sorumluluğu ise, T.C.K.'nın 246. maddesine göre değerlendirilecektir. T.C.K.'daki *"Bu bölümde yer alan suçların işlenmesi suretiyle yararına haksız menfaat sağlanan tüzel kişiler hakkında bunlara özgü güvenlik tedbirlerine hükmolunur."* Hükmü gereğince tüzel kişilere T.C.K.'nın 60. maddesindeki güvenlik tedbirleri uygulanacaktır.

Failin suçu işleyen kişi olduğunun tam olarak tespit edilmesi durumunda ceza vermek mümkündür. Bu nedenle internet kafelerden bu tür suçların işlenmesinde fail tam olarak tesit edilememekte ve ceza vermek mümkün olmamaktadır[144].

3.2. Mağdur

Mağdur, suçu oluşturan fiilden doğrudan doğruya zarar gören kimsedir[145]. Bir başka görüşe göre ise, tecavüzün zarar verdiği değerin sahibi, zarar gören şahıstır[146]. Ancak, mağdur kavramı ile suçtan zarar gören kavramlarını birbirine karıştırmamak gerekir. Suçtan zarar gören kişi her zaman suçun islenmesi dolayısı ile mağdur edilen kişi değildir. Mağduru olmayan bir suç mümkün değildir. Mağdur ancak gerçek kişi olabilir. 5237 sayılı T.C.K.'nın 20. maddesine göre ancak gerçek kişiler suçun mağduru olabilmektedirler. Tüzel kişiler suçun mağduru olamaz, ancak suçtan zarar göreni olabilir.

Bilişim sistemine hukuka aykırı olarak girilmesinden ve orada kalınmasından dolayı bilişim sisteminin güvenliği tehlikeye giren kişi bu suçun mağdurudur. Bu kişi de herkes olabilir.

3.3. Suçun Konusu

Söz edilmek istenen suçun maddi konusudur. Zira, suçun hukuki konusunu "korunan hukuksal değer başlığı altında" incelemekteyiz. Suçun maddi konusu,

---

143 Dülger Murat Volkan, s.119'dan "İngilizce 'white-collar crime' teriminden Türkçe'ye çevrilen 'Beyaz yaka suçları'; kavram olarak oluşumunda şiddet içermeyen, ticari alanda dolandırıcılık, güveni kötüye kullanma gibi suç tipleri için kullanılan genel addır" Black's Law Dictionary s.1590

144 11.CD. 24.09.2010 T. 2010/10299 E. 2010/9933 K. "…….Sanığın Halley Internet Cafe'nin sahibi olduğu, iş yerindeki 70 adet bilgisayarın gözetimi ve denetimi için gerekli hassasiyeti göstermemesi sebebiyle kusurlu olduğu gerekçesiyle cezalandırılmasına karar verilmiş ise de, adı geçen iş yerindeki İP numarası 81.215.188.170 olan bilgisayardan müştekinin elektronik posta adresine girilmesinden sanığın sorumluluğu olmamasına rağmen, üzerine atılı suçtan beraatine dair karar verilmesi gerekirken yazılı şekilde cezalandırılmasında,……." - Uyap Mevzuat Programı

145 Toroslu Nevzat, s.67

146 Soyaslan, Doğan, (Genel Hükümler) s.224

üzerinde suçun işlendiği şahıs veya şeydir[147]. Bir başka görüşe göre ise, suçun konusu, üzerinde suçun meydana geldiği hareketin kendisine yöneldiği insan ya da maddi varlıklardır[148].

Bu halde inceleme konusu olan, bu suçun konusu hukuka aykırı olarak girilen ve orada kalınan bilişim sistemidir.

3.4. Hareket

Felsefi açıdan kişiye atfedilen her şey harekettir; ancak ceza hukuku kişinin iç dünyasındaki hareketlerle ilgilenmemektedir. Düşüncenin iç dünyadan dış dünyaya çıkması durumunda ceza hukuku açısından hareket önem taşımaktadır. Dış dünyaya çıkan bir hareket icrai veya ihmali şekilde olabilir[149].

Bu suç ile ilgili "seçimlik hareketli suç" olup olmadığı hakkında doktrinde Farklı görüşler bulunmaktadır.

Bir görüşe göre, bu suç seçimlik hareketli değildir. Bu suçun oluşumu için bilişim sistemine haksız olarak "girme" yetmez, ayrıca sistemde "kalmaya devam etme" gerekmektedir[150]. Kanunkoyucu, kötüniyet taşımayıp kısa süreliğine sisteme girenleri cezalandırmak istememiştir[151]. Bize göre de bu suç seçimlik hareketli değildir. Madde metninde giren "ve" kalmaya devam eden ibaresi kullanılmaktadır. Madde metni TBMM Genel Kurulu'na "giren veya orada kalmaya devam eden" şeklinde gelmiş ancak yapılan değişikle "giren ve orada kalmaya devam eden" şeklide yasalaşmıştır[152]. Bu husus da T.C.K. 243/1 maddesindeki suçun seçimlik hareketli olmadığını her iki hareketin gerçekleşmesi gerektiğini göstermektedir. Ancak maddedeki "ve" ibaresinin "veya" olarak değiştirilmesi gerektiğini de düşünmekteyiz. Bilişim sistemine girme bizatihi suç olmalıdır[153].

Bir diğer görüşe göre, bu suçun seçimlik hareketli bir suç olarak düzenlendiğini, hukuka aykırı olarak bilişim sistemine girilmesi veya sistemde kalınmaya devam edilmesi eylemlerinden birisinin yapılmasıyla bu suçun gerçekleşeceğini, failin hangi eylemi gerçekleştirirse gerçekleştirsin cezalandırılacağını belirtmektedir[154].

147 TOROSLU Nevzat, s.66

148 TAŞKIN Şaban Cankat, s.24

149 SOYASLAN, Doğan, (Genel Hükümler) s.221

150 KARAGÜLMEZ Ali, s.180

151 TAŞKIN Şaban Cankat, s.24

152 KARAGÜLMEZ Ali, s.182

153 Aynı görüş için bkz. KARAGÜLMEZ Ali, s.204

154 DÜLGER Murat Volkan, s.217

Yargıtay bir kararında[155] *"Sanığın, katılanın yetkilisi olduğu, Z... T... İmalat Pazarlama Sanayi ve Limited Şirketinin Türkiye ……. Bankası Denizli Şubesinde bulunan hesabına internet üzerinden izinsiz giriş yaptığı, ancak şirkete ait hesaba girdikten sonra bu hesapta oynama yaparak başka bir hesaba havale yapmadığının iddia ve kabul olunması karşısında sanığın eyleminin 5237 sayılı T.C.K.'nın 244/4, 35/2 maddeleri gereğince hüküm tesisi bozmayı gerektirmiştir."* şeklindeki kararında sistemde para havalesi yapacak kadar kalmasına değinilmiştir[156].

Son olarak, daha önce de belirttiğimiz üzere 5237 sayılı T.C.K.'nun 243. maddesinde, bilişim sistemine hukuka aykırı olarak girme ve orada kalmaya devam etme suçu düzenlenmiştir. 765 sayılı T.C.K.'nun 525/a maddesinde ise, bilişim sisteminden program, veri veya diğer herhangi bir unsuru hukuka aykırı olarak ele geçirme suçu yer almaktadır. Ancak, 243. maddede, 525/a maddesindeki ele geçirme suçu bulunmamaktadır. Yani 525/a maddesine göre bilişim sistemine girmek suç değil iken 243. maddeye göre suçtur.

3.5. Netice

Suçun oluşması için mutlaka bir netice gerekir. Ceza hukukunda netice maddi bir olgu değildir. Maddi olgunun gerçekleşmesi ihtimali, tehlikesi de bir neticedir. Bu tür neticesi olabilen suçlara tehlike suçu denir[157].

Bu suç bilişim sistemine girip bir süre kalmakla tamamlanmış olur. Failin herhangi bir bilgi veya veri ele geçirme koşulu aranmaz. Failin, mağdura zarar vermiş olması şartı da aranmaz. Bu nedenle bu suç bir tehlike suçudur. Madde gerekçesinde de "Sisteme, hukuka aykırı olarak giren kişinin belirli verileri elde etmek amacıyla hareket etmiş bulunmasının önemi yoktur. Sisteme, doğal olarak, haksız ve kasten girilmiş olması suçun oluşması için yeterlidir." denilmekle suçun tehlike suçu olduğu açıklığa kavuşturulmuştur.

4. Suçun Manevi Unsurları

Kişinin bir suçtan sorumlu tutulabilmesi için sadece fiili yapması ve fiil sonucu neticenin ortaya çıkması yetmez. Aynı zamanda kişi ile fiil arasında psikolojik bir bağ bulunması gerekir[158]. Şimdi belirttiğimiz bu psikolojik bağı inceleyeceğiz.

---

155 Y. 11. CD. 2008/18190 E. 2009/3058 k.

156 Karagülmez Ali, s.202

157 Soyaslan, Doğan, (Genel Hükümler) s.232

158 Soyaslan, Doğan, (Genel Hükümler) s.387

Ceza hukukunda sorumluluğun kaynağı kasttır. Kast, kişinin yaptığı hareketi ve neticesini bilmesi ve istemesi veya neticeyi göze almasıdır. (T.C.K. madde 21)

Bu suç ancak kasten işlenebilir. Bu kast genel kasttır, kanun suçun oluşumu için özel kast aramamıştır. Bilişim sistemlerine girme ve sistemde kalma suçu, fail tarafından bilerek ve isteyerek gerçekleştirilmelidir.

Taksir, dikkat ve özen yükümlülüğüne aykırılık dolayısıyla, bir davranışın suçun kanunî tanımında belirtilen neticesi öngörülmeyerek gerçekleştirilmesidir. (T.C.K. madde 22/2) Kanunkoyucu hangi suçların taksirle işlenebileceğini madde metinlerinde açıkça belirtir.

Bu suçun kasten işlenmesi arandığından taksirle işlenemez.

5. Hukuka Aykırılık

Suç genel teorisine bakımından, suçun hukuka aykırılık unsurunun o suçun yasal maddesinde belirtilmesi yaygın bir uygulama değildir. Suç sayılan fiillerde zaten hukuka aykırılık bulunmalıdır. Suç maddesinde fiilin hukuka aykırı olduğu açıkça düzenlenmişse buna "hukuka özel aykırılık" denir[159]. Anlatılanlardan anlaşılacağı üzere herhangi bir hukuka uygunluk nedeninin bulunması durumunda suç oluşmayacaktır.

Hukuka aykırı olarak bilişim sistemine girme ve sistemde kalma suçunda fail gerçekleştirdiği eylemin hukuka aykırı olduğunu bilmelidir. Bunun yanında 765 sayılı T.C.K.'nın 525a/1 maddesinde olduğu gibi bu suç tipinde de *mağdurun rızası veya kanunla verilen yetki* de, bu suçu hukuka uygun hale getirecektir. Ancak, rızanın suçun islendiği anda verilmesi gerekir. Tehdit edilerek veya hataya düşürülerek rızanın alınması durumlarında gerçek rızanın varlığından söz edilmez.

Failin cezalandırılması için bilişim sisteminde güvenlik önlemi alınmış olması gerekmez[160]. Şifre konulması bir anlamda sisteme başkalarının girmesini önleme iradesidir. Ancak, kişi şifresini vermiş ise artık eylem hukuka uygun hale gelir. Sisteme şifre konulmamış olsa da bu sistem sahibinin sisteme girilmesine izin verdiği anlamı taşımaz. Daha önce de belirttiğimiz üzere açık rıza gerekir. Ancak, bazı durumlarda da sisteme girme orada kalma hareketi suç olduğu düşünülse de olmayabilir. Bunun en yaygın örneği ev için alınan Digitürk aboneliğinin işyerinde kullanılmasıdır. Yargıtay bir kararında[161] "Dijitürk şifresinin müdahil şirkete ait

159 Karagülmez Ali, s.134

160 Dülger Murat Volkan, s.219

161 11.CD. 13.04.2009 T. 2006/7779 E. 2009/4153 K. - UYAP Mevzuat Programı

decoder dışında özel bir alet yardımıyla çözüldüğü saptanamadığına göre, abonelik sözleşmesiyle evinde kullanmak üzere alınan decoderin, sözleşme hükümlerine aykırı olarak başka yerde kullanılmasından ibaret eylemin hukuki nitelikte bulunduğu gözetilmeden yazılı şekilde hüküm kurulması" diyerek bu durumun sözleşmeye aykırılık olduğunu söylemiştir.

Diğer hukuka uygunluk sebebi de kanunun verdiği yetkiye dayanarak yapılan müdahaledir.

Hukukumuzda bu durumun bir örneği 5651 sayılı *"İnternet Ortamında Yapılan Yayınların Düzenlenmesi Ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun"* dur. Kanunun 8. maddesinde bazı durumlarda erişimin engellenebileceği düzenlenmiştir.

Hukukumuzda bu durumun diğer örnekleri ise, Ceza Muhakemesi Kanunu'nun (C.M.K.) 134. maddesindeki "Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma" ve aynı kanunun 135. maddesindeki "İletişimin tespiti, dinlenmesi ve kayda alınması" tedbirleridir.

6. Suçun Özel Görünüş Şekilleri

6.1. Teşebbüs

Kişi, işlemeyi kastettiği bir suçu elverişli hareketlerle doğrudan doğruya icraya başlayıp da elinde olmayan nedenlerle tamamlayamaz ise teşebbüsten dolayı sorumlu tutulur. (T.C.K. m.35)

Bu suça teşebbüs olup olmayacağı tartışmalıdır. Çünkü, bu tür suçlar harekete bitişik suçlardır. Bu nedenle bu suçlara teşebbüs mümkün gözükmemektedir Ancak, elektrik kesilmesi, sistemin kullanıcısı tarafından kapatılması gibi durumlarda teşebbüs kabul edilebileceğini düşünen yazarlar vardır[162]. Sadece sisteme girilmeye çalışılması örneğin güvenlik sisteminin çözülmeye çalışılması ya da anlık girip çıkma teşebbüs olmaz. Anlık değil de orada kalmaya başladıktan sonra sistemde kalma başarılamamışsa örneğin elektrik kesilmişse bu durumda teşebbüs düşünülebilir[163].

6.2. İştirak

Türk Ceza Kanunu'nun 243. maddesinde yer alan *"Hukuka aykırı olarak bilişim sistemine girme ve sistemde kalma"* suçlarının iştirak açısından bir özellik söz

162 Parlar Ali/Hatipoğlu Muzaffer, S.716

163 Karagülmez Ali, s.185

konusu olmayıp, genel hükümler uygulanacaktır. Genel hükümler değerlendirildiğinde bu suç tipleri için iştirak türlerinin gerçekleşmesi mümkündür[164].

6.3. İçtima

Suçların içtimaında suçlardan birinin diğer suçta unsur veya ağırlaştırıcı nedeni olması, tek eylemde yasanın birden fazla hükmünün ihlali ve bir suç işlemek kararı ile yasanın aynı hükmünün birkaç defa ihlali durumları incelenmektedir. Bu hususlar 5237 sayılı T.C.K.'nın 42. maddesinde "bileşik suç", 43. maddesinde "zincirleme suç" ve 44. maddesinde ise "fikri içtima" olarak düzenlenmiştir.

Fail, aynı suç isleme kastıyla belli bir bilişim sistemine kısa aralıklarla birden çok kez girmişse bu suçtan faile verilecek cezada T.C.K. 43/1 düzenlemesi uygulanacaktır. Faile, o fiile ait tek fakat ağırlaştırılmış bir ceza verilecektir.

Diğer yandan fail uzun aralıklarla ve her seferinde sistemdeki başka bir veriyi elde etmek için sisteme giriyor ve orada kalmaya devam ediyorsa failde aynı suç isleme kastının varlığından bahsedilebilmesi mümkün değildir. Her eylem ayrı ayrı cezalandırılmalıdır. Başka bir deyişle, cezaların içtimaı kuralı uygulanmalıdır[165].

Bu suçta bileşik suçun oluşabilmesi mümkün değildir. Çünkü bileşik suçun oluşabilmesi için biri diğerinin ağırlatıcı nedeni ya da unsuru olan iki ayrı suç bulunmalıdır. Bu suçun unsurlarında böyle bir durum yoktur

Bu suç tipi yeni T.C.K.'da düzenlenen diğer bazı bilişim suçları bakımından bir "geçit suç"udur. Başka bir deyişle, o suçların islenmesi için failin öncelikle bilişim sistemine girmesi ve sistemde bir süre kalması gerekecektir. Örneğin, aşağıda inceleyeceğimiz T.C.K. 244 maddesinde düzenlenen "sistemi engelleme, bozma, verileri yok etme veya değiştirme" suçunda; T.C.K. 245. maddesinde düzenlenen "banka veya kredi kartlarının kötüye kullanılması" suçunda; T.C.K. 132. maddesinde düzenlenen "haberleşmenin gizliliğini ihlal" suçunda; T.C.K. 133. maddesinde düzenlenen "kişiler arasındaki konusmaların dinlenmesi ve kayda alınması" suçunda; T.C.K. 134. maddesinde düzenlenen "özel hayatın gizliliğini ihlal" suçunda; T.C.K. 135. maddesinde düzenlenen "kişisel verilerin kaydedilmesi" ve T.C.K. 136. maddesinde düzenlenen "verilerin hukuka aykırı olarak verilmesi veya ele geçirilmesi" suçlarında; ayrıca T.C.K. 142. maddesinde düzenlenen "bilişim sistemi

164 Akbulut Berrin, s.,213; Dülger Murat Volkan, s.205; Yazicioğlu Yılmaz, s.286

165 Dülger Murat Volkan, s.219

aracılığıyla gerçekleştirilen hırsızlık" ve T.C.K. 158. maddesinde düzenlenen "bilişim sistemi aracılığıyla dolandırıcılık" suçlarında ve Fikir ve Sanat Eserleri Kanunu (FSEK) ile Elektronik İmza Kanunu (EİK) düzenlenen bilişim suçlarında, incelemekte olduğumuz T.C.K.^nın 243. maddesindeki suç, bir geçit suçu özelliği taşır[166].

7. Suça Etki Eden Sebepler

T.C.K.'nın 243. maddesinin 2. fırasındaki düzenleme ile, "bedeli karşılığında yararlanılabilen sistemlere" karsı bu suçun islenmesi hafifletici neden olarak belirlenmiştir.

Bedeli karşılığı yararlanılan sistemlerden neyin anlaşılması gerektiği tartışmalıdır., bedeli karşılığındaki yararlanılan sistemden otomatların kastedildiği düşünüldüğünde, otomatlardan karşılıksız yararlanmanın T.C.K.'nın 163. maddesi ile ayrıca yaptırıma bağlandığı görülmektedir[167].

Şu halde, bu kavramdan ne anlaşılması gerektiğine değinmek gerekir.

Bir görüşe göre, bedeli karşılığı yararlanılabilen sistem kavramından dört şey anlaşılır. Birincisi, internetten ücretli olarak üyelik hizmet veren web siteleri (mail, gazete, dergi aboneliği, içtihat programları gibi); ikincisi internet kafe gibi yerlerde belli bir bilişim sisteminden ücreti ödenerek yararlanılması; üçüncüsü, belli bir anlaşma karşılığında, belli bir hizmetin oraya abone olan üyelere mesaj olarak reklam amaçlı ileti yollaması; dördüncüsü, belli bir süre bedel karşılığında internet hizmetinin sağlanması (özellikle de kablosuz modem aracılığıyla bağlanan internet bağlantısındaki şifrenin üçüncü bir kişi tarafından kırılarak o hizmetten bedel ödenmeksizin yararlanılması) durumları bu nedenlerden bazılarıdır[168].

Başka bir görüşe göre, web sitelerini ve cep telefonlarına bir hizmetin reklamı için gönderilen mesajların bu kapsama girdiğini kabul etmekle birlikte, bedelini ödemeden internet kafedeki bilgisayara (internete) girilmesi ve orada kalınmasını kabul etmemektedir. Bedeli ödenmeden internet kafedeki bilgisayara girilmesi gerçekleşse bile, bu girme olarak değil, kullanma olarak değerlendirilir[169]. Bizce de bu görüş daha doğrudur. T.C.K.'nın 243. maddesinin 2. fıkrasımda kastedilen,

166 Dülger Murat Volkan, s.225,226

167 Parlar Ali/Hatipoğlu Muzaffer, S.717

168 Dülger Murat Volkan, s.227

169 Karagülmez Ali, s.188

bilişim sisteminin kullanıldığı mekan değil, bilişim sisteminin içindeki elektronik yapıda sunulan ücretli hizmetlerdir[170].

T.C.K.'nın 243. maddesinin 3. fıkrasındaki düzenleme ile birinci fıkrada belirtilmiş olan suçun islenmesi sonucunda sistemdeki verilerin yok olması durumunda verilecek olan temel ceza arttırılacaktır. Burada, verinin yok olması veya verinin değişmesi şeklinde iki seçimlik sonuç bulunmaktadır. Bunlardan herhangi birinin meydana gelmesi ağırlaştırıcı nedenin uygulanması için yeterlidir. Ancak burada önemli olan, failde sistemdeki verileri yok etme yönünde bir kasıt bulunmamasıdır[171]. Anlık girip çıkma durumunda verinin yok olması veya verinin değişmesi söz konusu olursa fail bu sonuçtan sorumlu tutulmayacaktır[172].

Maddenin gerekçesinde de, bu durumun, suçun neticesi sebebiyle ağırlaşmış hali olduğu belirtilmektedir.

8. Kovuşturma, Görevli Mahkeme, Suçun Yaptırımı ve Dava Zamanaşımı

Kovuşturma: Maddede tanımlanan suçun soruşturması ve kovuşturması resen yapılır

Görevli Mahkeme: 5235 sayılı Kanun'un 10. maddesi uyarınca maddede tanımlanan suçlara dolayısıyla açılan davalara bakma görevi sulh ceza mahkemesine aittir.

Suçun Yaptırımı: Maddenin birinci fıkrasında, hukuka aykırı olarak sisteme giren ve orada kalmaya devam eden kimseye bir yıla kadar hapis veya adli para cezası verileceği düzenlenmiştir. T.C.K.'nın 49/1 maddesine göre, süreli hapis cezası, kanunda aksi belirtilmeyen hallerde bir aydan az 20 yıldan fazla olamayacaktır. Bu nedenle, hapis cezasının alt sınırını bir ay olarak kabul etmek gerekmektedir. Yasa'daki "veya" ifadesinden, yaptırımın seçenekli olduğu anlaşılmaktadır. Buna göre, faile ya hapis cezası ya da adli para cezası verilecektir. Adli para cezasının miktarının ne olacağı ve nasıl hesaplanacağı ise T.C.K. 52.maddeye göre yapılacaktır. Maddenin ikinci fıkrasında belirtilen eylemin gerçekleştirilmesi yani eylemin bedeli karşılığında işlenmesi durumunda ceza yarı oranına kadar indirilecektir. Üçüncü fıkradaki durumda, yani eylem nedeniyle verilerin yok olmasında ise faile verilecek ceza altı aydan iki yıla kadar hapis

170 Parlar Ali/Hatipoğlu Muzaffer, S.717; Karagülmez Ali, s.188

171 Karagülmez Ali, s.190

172 Parlar Ali/Hatipoğlu Muzaffer, S.718; Karagülmez Ali, s.192

olacaktır. T.C.K.'ya göre fiili isleyen tüzel kişilikse, tüzel kişiye T.C.K. 20/2 gereğince ceza verilemeyecektir. Bu durumda, T.C.K. madde 246'ya göre T.C.K.'nın 60. maddesindeki güvenlik tedbirleri uygulanır.

Dava Zamanaşımı: T.C.K.'nın 66/1-e maddesi uyarınca bu suçların dava zamanaşımı süresi 8 yıldır

b. Bilişim Sisteminin İşleyişinin Engellenmesi, Bozulması, Verilerin Yok Edilmesi veya Değiştirilmesi Suçu[173]

1. Genel Olarak

Bu maddede düzenlenen suç tipi ile 765 sayılı T.C.K.'daki 525 / b – 1 maddesinde düzenlenen "verilere veya veri işleme zarar vermek suçu" karşılanmaya çalışılmıştır.

244. maddenin 1. fıkrasındaki düzenlemeyle, Avrupa Siber Suç Sözleşmesi'nin 5. maddesinde düzenlenen "sistemlere müdahale" karşılanmaya çalışılmıştır.

Avrupa Siber Suç Sözleşmesi'nin 5. maddesine göre[174]: *"Taraflardan her biri, bilgisayar verilerine yeni veriler ilave etmek, bilgisayar verilerini başka yerlere iletmek, tahrip etmek, silmek, bozmak, değiştirmek veya erişilmez kılmak suretiyle, bilgisayar sisteminin işleyişini ciddi ölçüde ve haksız şekilde engelleme fiilinin, kasıtlı olarak kendi ulusal mevzuatı kapsamında cezai bir suç olarak tanımlanması için gerekli olabilecek yasama işlemlerini ve diğer düzenlemeleri yapacaktır"*

244. maddenin 2. fıkrasındaki düzenlemeyle de Avrupa Siber Suç Sözleşmesi'nin 4. maddesinde düzenlenen "verilere müdahale" karşılanmaya çalışılmıştır.

Avrupa Siber Suç Sözleşmesi'nin 4/1 maddesine göre[175];

"*Taraflardan her biri, bilgisayar verilerinin haksız bir şekilde tahrip edilmesi, silinmesi, bozulması, değiştirilmesi veya erişilemez kılınması fiillerinin, kasıtlı olarak yapıldıklarında kendi ulusal mevzuatı kapsamında cezai bir suç olarak*

---

173 5237 sayılı T.C.K.'nın "Sistemi engelleme, bozma, verileri yok etme veya değiştirme" başlıklı 244/1–2 Maddesi:

"[1] Bir bilişim sisteminin işleyişini engelleyen veya bozan kişi, bir yıldan beş yıla kadar hapis cezası ile cezalandırılır.

[2] Bir bilişim sistemindeki verileri bozan, yok eden, değiştiren veya erişilmez kılan, sisteme veri yerleştiren, var olan verileri başka bir yere gönderen kişi, altı aydan üç yıla kadar hapis cezası ile cezalandırılır.

[3] Bu fiillerin bir banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinde işlenmesi halinde, verilecek ceza yarı oranında artırılır.

[4] Yukarıdaki fıkralarda tanımlanan fiillerin işlenmesi suretiyle kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlamasının başka bir suç oluşturmaması hâlinde, iki yıldan altı yıla kadar hapis ve beşbin güne kadar adlî para cezasına hükmolunur."

174 Özen Muharrem/ Baştürk İhsan, s.355

175 Özen Muharrem/ Baştürk İhsan, s.355

tanımlanması için gerekli olabilecek yasama işlemlerini ve diğer düzenlemeleri yapacaktır."

Madde gerekçesinde de bu maddeyle bilişim sistemlerine yöneltilen ızrar eylemlerinin ayrı bir suç haline getirildiği vurgulanmaktadır. Ayrıca yine maddenin gerekçesinde, yapılan düzenleme ile "aracın fizik varlığı ve işlemesini sağlayan bütün diğer unsurları, söz konusu suçun konusunu oluşturmaktadır" denilerek bilişim sisteminin somut ve soyut bütün unsurlarının bu suçun konusunu oluşturacağı ifade edilmektedir. Yine madde gerekçesinde "özel bir ızrar eylemi" denilmek suretiyle bilişim sisteminin çalışmasını engellemeye yönelik eylemler kastedilmiştir[176]. Bu maddede düzenlenen suç tipleri seçimlik hareketli suçlardır. Yani sayılan hareketlerden herhangi bir tanesinin işlenmesi suçun tamamlanması için yeterlidir.

2. Korunan Hukuksal Değer

Bu suçun korunan hukuksal değerinin ne olduğu konusunda değişik görüşler vardır.

Bir görüşe göre, bu suçla, sadece bilişim sisteminin soyut unsuru olan yazılım ve veriler koruma altına alınmamış, aynı zamanda somut unsuru olan donanım kısmı da koruma altına alınmıştır. Bu nedenle de suçla korunan hukuksal değer karma bir nitelik taşımaktadır[177].

Diğer bir görüş ise, suçla korunan hukuksal değerin öncelikle sistemin sahibi olan kimsenin mülkiyet hakkı olduğunu savunmaktadır. Bu görüşe göre, maddenin ilk fıkrasında malikin yanı sıra, sistemin zilyedi bakımından da bilişim sisteminin dokunulmazlığı, iletişim kurma, teknolojik iletişim özgürlüğü korunan hukuksal değer olarak gösterilebilir[178].

Başka bir görüş ise, bu suçla korunan hukuksal değer, madde gerekçesinde de belirtildiği üzere, sistemlere yöneltilen ızrar fiillerinin özel bir suç haline getirme düşüncesiyle bağlantılıdır. Bu görüşe göre, hem bilişim sisteminin hem de bu sistem içerisinde yer alan verilerin veya diğer unsurların zarar görmemesi amaçlanmaktadır[179].

Maddenin karşılığı olan Avrupa Konseyi Siber Suç Sözleşmesi 4 ve 5 için oluşturulan dayanak raporunda; 4. madde bakımından korunan hukuksal değer,

176 Demircan Tunç, s.100

177 Dülger Murat Volkan, s.231

178 Kurt Levent, "Açıklamalı-İçtihatlı Tüm Yönleriyle Bilişim Suçları ve Türk Ceza Kanunundaki Uygulaması", Seçkin Yayıncılık, Ankara, 2005, s.161,162

179 Karagülmez Ali, s.211

bilgisayar verilerine veya programlarına zarar verilmesini, veri ve programların bozulmasını, zarar görmesini önlemek, böylece programların doğru ve aksaksız çalışmasını sağlamak olarak belirtilmiştir. 5. maddedeki korunan hukuksal değer ise, bilgisayar sabotajının engellenmesi ve böylece bilişim sisteminin sağlıklı şekilde kullanılmasının sağlanmasıyla, sisteme yönelecek haksız davranışların önlenmesidir[180].

Bir başka görüşe göre, hem maddenin gerekçesi hem de kanunun lafzı dikkatle yorumlandığında, madde ile Avrupa Konseyi Siber Suç Sözleşmesi'nin 4 ve 5.maddelerinin gerekçe raporunda belirtildiği gibi, bilişim sisteminin zarar görmemesinin amaçlandığı görülecektir. Dolayısıyla, korunan hukuksal değer, bilişim sisteminin somut ve soyut unsurlarının bütünlüğüdür[181].

3. Suçun Maddi Unsurları

Suçun maddi unsuru dendiğinde anlaşılması gereken o suçun işlenmesinde gerekli olan hareketler sonucunda neticenin meydana gelmesi ve hareket ile netice arasında nedensellik bağının bulunmasıdır[182].

Aşağıda suçun maddi unsurları olan aktif süje, pasif süje, hareket, netice, suçun unsuru ve nedensellik bağına değineceğiz.

3.1. Fail

5237 sayılı T.C.K.'nın 244. maddesinin 1. ve 2. fıkralarında suçu işleyecek kişi açısından herhangi bir özellik belirtilmediği için suçun faili herkes olabilir.

Tüzel kişilerin sorumluluğu ise, T.C.K.'nın 246. maddesine göre değerlendirilecektir. T.C.K.'daki *"Bu bölümde yer alan suçların işlenmesi suretiyle yararına haksız menfaat sağlanan tüzel kişiler hakkında bunlara özgü güvenlik tedbirlerine hükmolunur."* hükmü gereğince tüzel kişilere T.C.K.'nın 60. maddesindeki güvenlik tedbirleri uygulanacaktır.

3.2. Mağdur

Bilişim sisteminin işleyişinin engellenmesi, bozulması, verilerin yok edilmesi ve değiştirilmesi suçunun mağduru, bilişim sistemine yapılan eylemler dolayısıyla verilere ulaşamayan, sistemi kullanamayan ve sistem üzerinde tasarruf yetkisi

180 TAŞKIN, Şaban Cankat, s.42'den Convention On Cybercrime, Explonary Report, http: //conventions.coe.İnt /Treaty/en/Reports /Html/185.htm (29.10.2007)

181 TAŞKIN, Şaban Cankat, s.42

182 SOYASLAN, Doğan, (Genel Hükümler) s.220, 221

bulunan kişi, çıkarları zedelendiği için suçun mağduru olacaktır[183]. Mağdur bilişim sisteminin sistemin maliki olabileceği gibi kullanım hakkı sahibi de olabilir.

3.3. Suçun Konusu

Bu suçun konusunu bilişim sistemleri veya sistemdeki veriler ve yazılımlar oluşturmaktadır. Kanun maddesinde yazılımlar belirtilmemiş olsa da, yazılımlar verilerden oluşan bir bütün olduğundan suçun konusunu oluşturmaktadır[184].

T.C.K.'nın 244. maddesinin gerekçesinde "*böylece sistemlere yöneltilen ızrar filleri özel bir suç haline getirilmiştir, aracın fizik varlığı ve işlemesini sağlayan bütün diğer unsurları, söz konusu suçun konusunu oluşturmaktadır."* denilmektedir. Gerekçeden donanıma verilen zararlar içinde bu maddenin uygulanacağı anlamı çıksa da madde metni verileri ve bilişim sistemini korumaktadır. Bu nedenle bu ifade yanıltıcı bulunmaktadır[185]. Madde metni yorumlandığında ve okunduğunda, gerekçeden farklı bir anlam çıkmaktadır. Gerekçenin sadece uygulamacı açısından yol gösterici olması ve bağlayıcı olmaması değerlendirildiğinde donanım unsuruna verilen zararların bu madde kapsamına girmeyeceğini söyleyebiliriz.

Yukarıda açıkladığımız hususlardan sonra bu maddenin uygulamasında, bilişim sisteminde veri yüklü olup olmaması önem taşıdığını açıkça söyleyebiliriz. Sistemde herhangi bir veri yoksa T.C.K.'nın 244. maddesinin 1. fıkrası uygulanamayacaktır. Donanıma verilen zararlar için T.C.K. 151. madde uygulanacaktır[186]. Buna karsın sisteme virüs koyarak bozan, yok eden, değiştiren veya erişilmez kılan, sisteme veri yerleştiren, var olan verileri başka bir yere gönderen kimse ise T.C.K.'nın 244. maddesine göre cezalandırılacaktır.

3.4. Hareket

Şimdi kanun metninde yazılı çeşitli hareketleri inceleyelim.

3.4.1. Bilişim Sisteminin İşleyişini Engellemek Eylemi

Suç için yasada tanımlanan ilk hareket bilişim sisteminin isleyişinin engellenmesidir. İşleyişin engellenmesi, bir tanıma göre, sistemin düzgün islemesinden ötürü elde edilecek yararın engellenmesi veya sistemin olağan işlevini yerine getiremeyecek hale getirilmesidir187. Engel olma, sistemin işleyişine yönelik olabileceği gibi katkısı veya etkisi olan herhangi bir unsurun işleyişine engel olunması şeklinde de

183 Taşkin, Şaban Cankat, s.42

184 Dülger Murat Volkan, s.233

185 Dülger Murat Volkan, s.233; TAŞKIN Şaban Cankat, s.44

186 Dülger Murat Volkan, s.233,234

187 Kurt Levent, s.164

olabilir188. Bize göre de her nasıl olursa olsun sistemin isleyişinin engellenmiş olması ya da sistemin bozulması T.C.K.'nın 244. maddesindeki suçun oluşması için yeterlidir. Sistemin sürekli veya geçici süreyle çalışamaz durumda kaldığının ise suçun oluşması bakımından bir önemi yoktur[189].

3.4.2. Bilişim Sisteminin İşleyişini Bozmak Eylemi

Bu durumda, sistem çalışamaz hale getirilmektedir. Çalışamaz hale getirme, sistemin çökertilmesi program akışının değiştirilmesi, bozulması, sistemin soyut unsurlarının sözgelimi virüsler aracılığıyla isleyemez hale getirilmesidir[190].

Yazılımın kısmen veya tamamen çalışamaz hale getirilmesi durumunda sistemin işleyişini bozma eylemi gerçekleşmiş olur[191].Sistemin işleyişinin çalışmasını sağlayan düzeneğe zarar verilmesi de sistemin isleyişini bozmak olarak tanımlanabilir[192].

3.4.3. Verileri Bozma Eylemi

Bu eylem, bilişim sistemine girmeden veya girerek veri içeren bir dosyaya zararlı bir virüs yazılımı bulaştırarak ya da fiziki bir hareket yoluyla gerçekleştirilebilir. Örneğin, bilgisayarın harddiskini kırmak ya da fiziki bir etkiyle diske zarar vermek şeklinde gerçekleşebilir[193].

T.C.K.'nın 244. maddesinin 1. fıkrasında failin kastı, hangi yolla olursa olsun sistemin isleyişini bozmak veya sisteme zarar vermektir. Oysa T.C.K.'nın 244. maddesinin 2. fıkrasında ise failin kastı sistemin isleyişini bozmak değildir. Fail T.C.K.'nın 244. maddesinin 2. fıkrasında sistemin bütününe zarar vermek yerine, yalnızca sistemdeki belli bazı verilere ya da belli uygulama yazılımlarına zarar vermek kastıyla hareket etmektedir[194].

3.4.4. Verileri Yok Etme Eylemi

Bilişim sistemindeki verilerin yok edilmesinden kasıt, verilerin tamamen ortadan kaldırılması, bir başka deyişler varlığına son verilmesidir. Bilişim sistemindeki verileri ortadan kaldırma somut olarak değil, soyut olarak ortadan kaldırmadır. Bilişim sisteminin belleğindeki verilerin geri dönmeyecek şekilde

188 KARAGÜLMEZ Ali, s.211

189 DÜLGER Murat Volkan, s.234

190 KURT Levent, s.164

191 KARAGÜLMEZ Ali, s.212

192 KARAGÜLMEZ Ali, s.212

193 PARLAR Ali, "Türk Ceza Hukukunda Bilişim Suçları", Ankara, Bilge Yayınevi, Ocak, 2011, s.26

194 TAŞKIN Şaban Cankat, s.46

silinmesi (format atılması) veya geri dönüşüm kutusundaki verilerin oradan da silinmesi durumunda verilerin yok edildiği kabul edilmelidir. Öte yandan, taşınabilir bir veri aracının (harddisk, disket, CD, USB gibi) kırılması veya yakılmasıyla verilerin yok edilmesi bu suçu oluşturacaktır.

Sistemdeki geri dönüşüm kutusuna gönderilen verilerin yok edilmiş sayılıp sayılmayacağı ise tartışmalıdır. DÜLGER'e göre[195] amaç mağdurun verilere ulaşmasını engellemek olduğu için bu yolla da verilerin bir şekilde yok edildiğini kabul etmek gerekir. TAŞKIN'a göre[196] ise, geri dönüşüm kutusundaki veriler tek bir tıkla yeniden eski yerlerine getirilebilir, bu nedenle bu işlemi yok etme kabul etmemek gerekir. Bize göre ise, bu eylem de bir yok etmedir. Çünkü bilgisayar sisteminde bazen format atılsa bile bazı yöntemlerle bilgilerin geri döndürülmesi mümkün olabilmektedir, verilerin geri getirilebilir olması, failin o verileri yok etmeye çalıştığı gerçeğini ortadan kaldırmaz.

3.4.5. Verileri Değiştirme Eylemi

Verilerin değiştirilmesi eyleminde kasıt, bilişim sistemindeki bir verinin silinerek yerine baksa bir veri konması ya da sistemdeki veriyle başka bir verinin değiştirilmesidir[197]. Başka bir deyişle, verilerin orijinal halinden başka bir hale dönüştürülmesidir Dönüştürmenin kısmen veya tamamen olması ya da menfaat sağlamak veya zarar vermek kastıyla yapılması arasında fark bulunmamaktadır[198]. Fail, bu eylem sonucunda menfaat sağlamışsa ve eylem başka bir suç oluşturmuyorsa, faile T.C.K.'nın 244. maddesinin 4. fıkrasında düzenlenen ceza verilecektir[199].

Elektronik posta ve facebook hesaplarının şifresini ele geçirerek bu adreslere giren, facebook hesabında yazışmalar yapan ve şifreyi değiştiren kişi de bu hareketi gerçekleştirmiş olur ve T.C.K.'nın 244. maddesinin 2. fıkrasına göre cezalandırılır[200].

---

195 Dülger Murat Volkan, s.236

196 Taşkin Şaban Cankat, s.47

197 Dülger Murat Volkan, s.237

198 Parlar Ali, s.26

199 Taşkin Şaban Cankat, s.26

200 8. CD. 01.11.2013 T., 2012/33557 E., 2013/25987 K. "Oluşa, katılanın aşamalardaki anlatımlarına, sanığın da çalıştığı aile şirketine ait telefona bağlı internet hesabından katılana ait elektronik posta hesabına girildiğine ilişkin Microsoft şirketinden gelen yazı yanıtları ve kolluk araştırması sonuçlarına, katılanın 22.12.2010 tarihli dilekçesi ekinde ibraz ettiği fotoğraflara ve tüm dosya kapsamına göre; katılana ait elektronik posta ve facebook hesaplarının şifresini ele geçirerek bu adreslere giren, facebook hesabında yazışmalar yapan ve şifreyi değiştirmek suretiyle katılanın anılan hesaplara erişimini engelleyen sanığın, eylemine uyan T.C.K..nun 244/2. maddesi uyarınca cezalandırılmasına karar verilmesi gerekirken yazılı gerekçeyle beraat hükmü kurulması," – Uyap Mevzuat Programı

3.4.6. Verileri Erişilmez Kılmak Eylemi

Verilerin erişilmez kılınmasından kast edilen, verileri kullanan ya da bu verilere malik olan kişinin dilediği zaman verilere ulaşmasının engellenmesidir[201].

Bu eylem, sisteme giden elektriğin kesilmesi, verilerin bulunduğu sistemin bozulması, verilerin sistemden silinmesi, sistemi kullanmaya yetkili olan kişinin bilgisi olmadan sisteme sifre koymak seklinde olabileceği gibi, verileri içeren sözgelimi taşınabilir belleğin içindeki verilerin silinmesi seklinde de olabilir[202].

Suçun oluşumu bakımından verilere ulaşmanın geçici veya sürekli olarak engellenmiş olması önem taşımamaktadır. Verilere ulaşmak ne kadar süreyle engellenmiş olursa olsun suç gerçekleşecektir[203].

3.4.7. Bilişim Sistemine Veri Yerleştirmek Eylemi

Bilişim sistemine veri yerleştirme eyleminden anlaşılması gereken, bilişim sistemini kullanmakla yetkili olan kimsenin veya malikin izni olmaksızın sisteme dışarıdan herhangi bir verinin yerleştirilmesidir[204]. Bu işlem kaydetme, ekleme veya yükleme seklinde gerçekleştirilebilir[205]. Eylemin nasıl gerçekleşeceğinin önemi olmamalıdır yani taşınabilir bellek ya da internet aracılığıyla yüklenmesi durumunda da eylemin gerçekleştiği kabul edilmelidir.

Veri yüklenen sisteme fail hukuka uygun olarak girmiş olsa dahi veri yerleştirme suçu gerçekleşmiş olabilir. Örneğin bedeli ödenerek bir sisteme giren failin eğer o sisteme veri yerleştirme yetkisi yoksa suç gerçekleşmiş sayılacak ve fail cezalandırılacaktır. Bu nedenle, sisteme girmenin faile veri yükleme hakkı verip vermediği failin cezalandırılması bakımından önem taşımaktadır[206].

3.4.8. Bilişim Sisteminde Var Olan Verileri Başka Bir Yere Göndermek Eylemi

Verilerin başka yere gönderilmesinden anlaşılması gereken verileri kopyalamaya yarayan bir araçla verilerin kopyasının çıkarılarak başka bir bilişim sistemine veri aktarılması ya da sözgelimi internet yoluyla bir sistemdeki verilerin başka bir sisteme aktarılmasıdır[207].

---

201 Dülger Murat Volkan, s.237

202 Taşkin Şaban Cankat, s.47, 48

203 Dülger Murat Volkan, s.237

204 Dülger Murat Volkan, s.237

205 Taşkin Şaban Cankat, s.48

206 Dülger Murat Volkan, s.238

207 Dülger Murat Volkan, s.238

İnternet yoluyla veri gönderme eylemi e-posta ile gönderilebileceği günümüzde e-postadan daha sık kullanılan "Messenger. Facebook, Twitter, WhatsApp, Line, Tictoc" gibi birçok sosyal medya site ve programlarıyla yapılabilir.

3.5. Netice

Bu suç bir görüşe göre, zarar suçudur. Söz konusu eylemlerin gerçekleşmesi durumunda bir zararın meydana gelmemesi mümkün değildir, eylemler bilişim sistemine zarar verici özelliğe sahiptir[208]. Diğer bir görüş, özellikle verilerin değiştirilmesi ve başka yere gönderilmesi suçu bakımından bir netice aranmayacağını yani zarar doğması şartı aranmayacağını savunmaktadır[209]. Bizce de, suçun seçimlik hareketli bir suç olması nedeniyle, suçun tehlike suçu mu, yoksa zarar suçu mu olduğu her bir eylem hakkında ayrı ayrı değerlendirilmelidir.

Bilişim sisteminin işleyişini engelleme, bilişim sistemindeki verileri bozma, yok etme, değiştirme veya erişilmez kılma eylemlerinin zarar suçu; bilişim sistemine veri yerleştirme, var olan verileri başka bir yere gönderme eyleminin ise tehlike suçu olduğunu düşünüyoruz.

4. Suçun Manevi Unsurları

Kişinin bir suçtan sorumlu tutulabilmesi için sadece fiili yapması ve fiil sonucu neticenin ortaya çıkması yetmez. Aynı zamanda kişi ile fiil arasında psikolojik bir bağ bulunması gerekir[210]. Şimdi belirttiğimiz bu psikolojik bağı inceleyeceğiz.

Bu suç ancak kasten işlenebilir. Bu kast genel kasttır, kanun suçun oluşumu için özel kast aramamıştır. Bilişim sistemlerine girme ve sistemde kalma suçu, fail tarafından bilerek ve isteyerek gerçekleştirilmelidir.

Bu suçun kasten işlenmesi arandığından taksirle işlenemez.

5. Hukuka Aykırılık

T.C.K.'nın 244. maddesinin 1 ve 2. fıkralarında düzenlenen bilişim sisteminin engellenmesi, bozulması, verilerin yok edilmesi veya değiştirilmesi suçunun hukuka uygunluk sebebini bilişim sistemi veya verilerin üzerinde tasarruf yetkisine sahip olan kişinin rızası oluşturacaktır.

208 Dülger Murat Volkan, s.239

209 Kurt Levent, s.170; TAŞKIN Şaban Cankat, s.43

210 Soyaslan, Doğan, (Genel Hükümler) s.387

Tabii bu rızanın kapsamına da bakmalıdır. Verilen rızanın sınırları aşılmamalıdır. Örneğin[211], bir kişiye bilişim sisteminin teslim edilmesi ve sistemin olağan kontrolü için verilere müdahale etme yetkisinin verilmesi, o kişiye sistemin içindeki bütün verileri yok etme ya da zarar verme yetkisini içermez.

Diğer hukuka uygunluk sebebi de kanunun verdiği yetkiye dayanarak yapılan müdahaledir. Hukukumuzda bu durumun bir örneği 5651 sayılı *"İnternet Ortamında Yapılan Yayınların Düzenlenmesi Ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun"* dur. Kanunun 8. maddesinde bazı durumlarda erişimin engelleyebileceği düzenlenmiştir.

Hukukumuzda bu durumun diğer örnekleri ise, Ceza Muhakemesi Kanunu'nun (C.M.K.) 134. maddesindeki "Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma" ve aynı kanunun 135. maddesindeki "İletişimin tespiti, dinlenmesi ve kayda alınması" tedbirleridir.

6. Suçun Özel Görünüş Şekilleri

6.1. Teşebbüs

Bilişim sisteminin isleyişinin engellenmesi, bozulması, verilerin yok edilmesi veya değiştirilmesi suçunda teşebbüs mümkündür. Örneğin bilişim sistemine yerleştirilmiş olan bir virüsün sistemin kullanıcısı tarafından, fark edilmesi ve aktif hale gelmeden etkisizleştirilmesi durumunda suçta teşebbüs olanaklı hale gelmiş sayılır[212].

Eylemler tamamlanmamış olsa dahi, o ana kadarki eylemi başkaca bir suç oluşturmaktaysa, tamamlanmış olan suçtan (Örneğin T.C.K. 243. maddedeki sisteme girmek ve sistemde kalmak) tam ceza verilebilecektir.

6.2. İştirak

T.C.K.'nın 244. maddesinin 1. ve 2. fıkralarında yer alan *"*Bir bilişim sisteminin işleyişini engelleme veya bozma, verileri bozan, yok etme, değiştirme veya erişilmez kılma, sisteme veri yerleştirme, var olan verileri başka bir yere gönderme*"* suçlarının iştirak açısından bir özellik söz konusu olmayıp, genel hükümler uygulanacaktır. Genel hükümler değerlendirildiğinde bu suç tipleri için iştirak türlerinin gerçekleşmesi mümkündür

211 Yayci Esra, s.95

212 Dülger Murat Volkan, s.241

6.3. İçtima

Bu suçun zincirleme suç seklinde işlenebilmesi mümkündür. Örneğin sistemin çalışmasının engellenmesi ya da sisteme hukuka aykırı olarak veri yerleştirilmesi için kısa zaman aralıklarıyla sisteme birçok müdahale edilen durumlarda zincirleme suç oluşacaktır[213]. Bu suçun mütemadi şekilde işlenmesi de mümkündür kişi bilişim sistemine girerek aralıksız şekilde sitemden haksız çıkra sağlayabilir, bu durumda tek suçun işlendiğini kabul etmek gerekir. Zamanaşımı zincirleme şekilde işlenen suçta son eylemden, mütemadi şekilde işlendiğinde devam eden eylemin bittiği zaman gerçekleşir.

Bu suçta bileşik suçun oluşabilmesi mümkün değildir. Çünkü bileşik suçun oluşabilmesi için biri diğerinin ağırlatıcı nedeni ya da unsuru olan iki ayrı suç bulunmalıdır. Bu suçun unsurlarında böyle bir durum yoktur

Son olarak bu başlıkta şuna da değinebiliriz. T.C.K. 243'teki suç T.C.K. 244/1-2 fıkraları için bir geçit olabilir. T.C.K. 244/1-2'deki "bilişim sisteminin engellenmesi, bozulması, verilerin yok edilmesi veya değiştirilmesi" suçunun işlenebilmesi için T.C.K. 243. maddedeki hukuka aykırı olarak bilişim sistemine girme ve sistemde kalma suçunun islenmesi gerekecektir. Bu durumda yalnızca T.C.K.'nın 244. maddesinin 1. ve 2. fıkralarından faile ceza verilecektir.

7. Suça Etki Eden Sebepler

T.C.K.'nın 244. maddesinin 3. fıkrasında "Bu fiillerin bir banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinde işlenmesi halinde, verilecek ceza yarı oranında artırılır." hükmü yer almaktadır.

Bilişim sisteminin isleyişinin engellenmesi, bozulması, verilerin yok edilmesi veya değiştirilmesi suçunu düzenleyen T.C.K.'nın 244. maddesinin 3.fıkrası suçun ağırlaştırıcı halini düzenlenmiştir.

Bu düzenleme ile bütün kamu kurum veya kuruluşlarına ait bilişim sistemleri T.C.K.'nın 243. maddesinin 3. fıkrası kapsamında değerlendirilebilecektir. Banka veya kredi kurumu niteliği olan özel kurum veya şirketler dışındaki özel kurumlar ise T.C.K.'nın 243. maddesinin 3. fıkrası kapsamında değerlendirilemeyecektir[214].

T.C.K.'nın 244. maddesinin 3. fıkrası ile maddenin 765 Sayılı T.C.K.'daki karşılığı olan 525 b.1'deki önemli bir eksiklik giderilmiştir. Zarar verilen sistemin

213 Dülger Murat Volkan, s.241

214 Karagülmez Ali, s.215

bankaya, kredi kurumuna ya da bir kurum ve kuruluşa ait bilişim sistemi olması ağırlaştırıcı neden sayılmıştır. Gerçekten de, bir kişisel bilgisayara verilen zarar ile bir bankanın bilgisayara verilen zarar arasında ciddi fark olduğunu kabul etmek gerekir. Bu nedenle bankanın sistemine verilen zarar nedeniyle failin daha ağır bir cezaya çarptırılması adaletli bir yaklaşım olmuştur[215].

8. Kovuşturma, Görevli Mahkeme, Suçun Yaptırımı ve Dava Zamanaşımı

Kovuşturma: Maddede tanımlanan suçun soruşturması ve kovuşturması resen yapılır

Görevli Mahkeme: 5235 sayılı Kanun'un 10. maddesi uyarınca maddede tanımlanan suçlara dolayısıyla açılan davalara bakma görevi asliye ceza mahkemesine aittir.

Suçun Yaptırımı: T.C.K.'nın 244. maddesinin 1. ve 2. maddeleri şu şekilde düzenlenmiştir.

"[1] Bir bilişim sisteminin işleyişini engelleyen veya bozan kişi, bir yıldan beş yıla kadar hapis cezası ile cezalandırılır.

[2] Bir bilişim sistemindeki verileri bozan, yok eden, değiştiren veya erişilmez kılan, sisteme veri yerleştiren, var olan verileri başka bir yere gönderen kişi, altı aydan üç yıla kadar hapis cezası ile cezalandırılır."

T.C.K. 244/3'teki ağırlaştırıcı nedenin gerçekleşmesi durumunda ise faile verilecek olan ceza yarı oranında arttırılacaktır.

T.C.K.'ya göre fiili işleyen tüzel kişilikse, tüzel kişiye T.C.K. 20/2 gereğince ceza verilemeyecektir. Bu durumda, T.C.K.'nın 246. maddesine göre T.C.K.'nın 60. maddesindeki güvenlik tedbirleri uygulanır.

Dava Zamanaşımı: T.C.K.'nın 66/1-e maddesi uyarınca bu suçların dava zamanaşımı süresi 8 yıldır.

c. Bilişim Sistemi Aracılığıyla Hukuka Aykırı Yarar Sağlama Suçu[216]

1. Genel Olarak

Bu suç daha önce de belirttiğimiz üzere 765 Sayılı T.C.K.'nın 525/b.2'deki suç tipine karşılık gelmektedir.

---

215 Dülger Murat Volkan, s.243

216 T.C.K. 244/4 maddesinde düzenlenen bu suç, maddenin 1 ve 2. fıkralarına göndermede bulunarak şu şekilde düzenlenmiştir."Yukarıdaki fıkralarda tanımlanan fiillerin işlenmesi suretiyle kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlamasının başka bir suç oluşturmaması hâlinde, iki yıldan altı yıla kadar hapis ve beşbin güne kadar adlî para cezasına hükmolunur"

Avrupa Siber Suç Sözleşmesi[217]'nin "Bilgisayarlarla İlişkili Sahtecilik Filleri" baslıklı 8. maddesindeki düzenleme dikkate alındığında, T.C.K.'nın 244. maddesinin 4. fıkrası ile bu düzenleme arasında paralellik bulunduğu görülmektedir. Buna göre, bilgisayarlarla ilişkili sahtecilik fiilleri, bir diğer kişinin mülkiyetini zarara sokmuş, suçu isleyen kimse kasıtlı olarak kendisi veya bir başkası için haksız maddi menfaat sağlamak amacıyla hareket etmişse, suç oluşacaktır.

Eğer bilişim sisteminin isleyişi, maddenin ilk iki fıkrasında sayılan eylemlerden biriyle gerçekleştirilmiş olmasına rağmen, başka bir suç oluşmuşsa (hırsızlık, güveni kötüye kullanma, zimmet gibi) cezasının ağırlığına bakılmaksızın faile o suçun cezası uygulanacaktır[218]. Oysa maddenin gerekçesinde, "*fiilin daha ağır cezayı gerektiren başka bir suç oluşturmaması gerekir"* denilmiştir. Gerekçedeki ifade, madde metni ile çelişki halindedir. Gerekçe cezanın belirlenmesinde belirleyici değildir, bağlayıcılığı yoktur. Bu nedenle madde metni dikkate alınacak, suçun cezasının ağırlığı ne olursa olsun eğer fiil başka bir suç oluşturuyorsa, faile o suçtan ceza verilecektir[219].

T.C.K.'nın 244. maddesinin 4. fıkrası ile T.C.K. 142/2-e maddesinde düzenlenen bilişim sistemlerinin kullanılması suretiyle hırsızlık suçu arasında, aynı şekilde T.C.K.'nın 244. maddesinin 4. fıkrası ile T.C.K. 158/1-f maddesinde düzenlenen bilişim sistemlerinin, banka veya kredi kurumlarının araç olarak kullanılması suretiyle dolandırıcılık suçlarından hangisinin uygulanacağı konusunda tartışma bulunmaktadır. Verinin hırsızlık suçunun unsuru olup olamayacağı, dolandırıcılık suçunda hilenin mutlaka gerçek kişiye karşı mı yapılması gerektiği konuları tartışılmaktadır. Bu konuda Yargıtay 6. ve 11. Ceza Dairelerinin Yargıtay Ceza Genel Kurulu'nun kararları vardır. Yargıtay'ın bu kararları ve doktrindeki görüşler doğrultusunda bu tartışmaya "bilişim sistemlerinin kullanılması suretiyle hırsızlık suçu" ve "bilişim sistemlerinin, banka veya kredi kurumlarının araç olarak kullanılması suretiyle dolandırıcılık suçu" başlıklarında ayrıntılı olarak

217 Özen Muharrem/ Baştürk İhsan, s.354

218 Parlar Ali, s.27; Dülger Murat Volkan, s.243; Taşkin Şaban Cankat, s.57

219 13. CD. 09.04.2013 T., 2012/387 E., 2013/10197 K. "……..5237 sayılı T.C.K.'nın 244/4. maddesinde, "Yukarıdaki fıkralarda tanımlanan fiillerin işlenmesi suretiyle kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlamasının başka bir suç oluşturmaması halinde…" biçimindeki ifadeden bu fıkradaki düzenlemenin tali norm niteliğinde olduğunun anlaşılması, buna göre öncelikle yasada düzenlenmiş olan bilişim sistemlerinin kullanılması suretiyle işlenebilen diğer suçların oluşup oluşmadığının değerlendirildikten sonra gerçekleştirilen eylemin bu suçlardan hiçbirisinin tanımına uygun değil ise, bu durumda eylemin 244/4. maddesi kapsamında suç oluşturacağı düşünülerek; ..... müştekinin rızasına aykırı olarak mal varlığında azalmaya neden olmaya, var olan veriyi başka bir yere göndermekten ziyade, bu verinin temsil ettiği parayı alarak mal edinmeye yönelik olması nedeniyle sanığın fiilinin 5237 sayılı T.C.K.'nın 142/2-e maddesindeki nitelikli hırsızlık suçunu oluşturduğunun gözetilmemesi,….." – Uyap Mevzuat Programı

değerlendireceğimizden burada sadece tartışmalı olduğunu belirterek bu hususu geçiyoruz.

2. Korunan Hukuksal Değer

5237 sayılı T.C.K.'nın 244. maddesinin 4. fıkrasının karşılığı olan 765 sayılı T.C.K.'nın 525b/2 maddesini anlatırken yer verdiğimiz görüşlerden suçun, bilişim sistemi içerisindeki unsurlar bakımından sahip oldukları mülkiyet hakkı koruma altına aldığı görüşü T.C.K. 244/4 maddesinde belirtilen suç tipi açısından geçerli değildir. Çünkü madde metni ve gerekçeden anlaşılacağı üzere dolandırıcılık, hırsızlık, güveni kötüye kullanma suçları bu suçun kapsamında kalmaz[220].

Bize göre, bu suçun korunan hukuksal değeri mülkiyet hakkı da olabilir. Yani korunan hukuksal değerin maddi ve manevi her türlü hakkın olabileceğini düşünmekteyiz.

3. Suçun Maddi Unsurları

Aşağıda suçun maddi unsurları olan aktif süje, pasif süje, hareket, netice, suçun unsuru ve nedensellik bağına değineceğiz.

3.1. Fail

5237 sayılı T.C.K.'nın 244. maddesinin 4. fıkrasında suçu işleyecek kişi açısından herhangi bir özellik belirtilmediği için suçun faili herkes olabilir.

Tüzel kişilerin sorumluluğu ise, T.C.K.'nın 246. maddesine göre değerlendirilecektir. Bu maddedeki *"Bu bölümde yer alan suçların işlenmesi suretiyle yararına haksız menfaat sağlanan tüzel kişiler hakkında bunlara özgü güvenlik tedbirlerine hükmolunur."* Hükmü gereğince tüzel kişilere T.C.K.'nın 60. maddesindeki güvenlik tedbirleri uygulanacaktır.

3.2. Mağdur

Bu suçun mağduru, sistemi zarar gören herkes olabilecektir. Mağdurun sistemin maliki, zilyedi ya da yararlananı (sıfatı ne olursa olsun) olması durumu değiştirmeyecektir[221].

3.3. Suçun Konusu

Bunun yanında 244. maddenin 1. ve 2. fıkrasında düzenlenen suç tiplerinin konusunun, maddenin 4. fıkrasında düzenlenen suç tipinin konusu ile aynı olduğunu

220 Dülger Murat Volkan, s.245

221 Taşkin Şaban Cankat, s.58

kabul etmek gerekir. Yani T.C.K.'nın 244. maddesinin 4. fıkrasındaki suçun konusu da bir bilişim sisteminin isleyişi veya bir bilişim sistemindeki verilerdir.

3.4. Hareket

5237 sayılı T.C.K.'nın 244. maddesinin 4. fıkrasında düzenlenen suç tipinin oluşabilmesi için, failin bilişim sisteminin isleyişini engellemek, bozmak, verileri bozmak, bilişim sistemine veri yerleştirmek, bilişim sisteminde var olan verileri başka yere göndermek, verileri erişilmez kılmak, verileri değiştirmek ve verileri yok etmek eylemlerinden birini ya da bir kaçını gerçekleştirmesi gerekmektedir. Bahsettiğimiz bu eylemler 244. maddenin 1. ve 2. fıkrasında düzenlenen suç tiplerindeki hareketler olup bunlar yukarıda ayrıntılı bir şekilde incelenmiştir. Bu nedenle, burada ayrıca bir açıklama yapmayacağız. Ancak fail, bu fiilleri işlemesi suretiyle kendisine veya başkasına haksız bir çıkar sağlıyorsa, bu durumda 4. fıkra uygulanacaktır.

3.5. Netice

5237 sayılı T.C.K.'nın 244. maddesinin 1. ve 2. fıkralarından farklı olarak 4. fıkrasında failin amacı zarar vermek değil, haksız bir çıkar sağlamaktır. Bu suçta zarar hukuka aykırı yarar elde edildikten sonra mağdurda meydana gelmektedir. Bilişim sisteminde veya verilerde zarar meydana gelmemiş olabilir Bir başka deyişle, bu suçta netice bakımında hukuka aykırı yararın oluşması aranmış, herhangi bir zararın meydana gelmiş olması aranmamıştır. Bu nedenle bu suç tehlike suçudur.

4. Suçun Manevi Unsurları

Bu suç ancak kasten işlenebilir. Ancak bu suçtaki kast özel kasttır, kanun suçun oluşumu için "haksız bir çıkar sağlamak" özel kastını aramıştır.

Bu suçun kasten işlenmesi arandığından taksirle işlenemez.

5. Hukuka Aykırılık

Bu suç tipinde hukuka aykırılığı ortadan kaldıran, rızanın varlığıdır. Bu rıza bilişim sisteminin maliki veya ilgilisi tarafından verilebilir. Rızanın kim tarafından verilebileceği her somut olayda ayrı olarak değerlendirilmelidir.

6. Suçun Özel Görünüş Şekilleri

6.1. Teşebbüs

T.C.K.'nın 244. maddesinin 1. ve 2. fıkralarında düzenlenen bilişim sisteminin isleyişinin engellenmesi, bozulması, verilerin yok edilmesi veya

değiştirilmesi suçunda "teşebbüs" başlığı altında açıkladığımız hususlar T.C.K.'nın 244. maddesinin 4. fıkrası için de geçerlidir.

6.2. İştirak

T.C.K.'nın 244. maddesinin 4. fıkrasında yer alan *"fiillerin işlenmesi suretiyle kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlama"* suçunda iştirak hükümleri açısından herhangi bir özellik söz konusu olmayıp, genel hükümler uygulanacaktır. Genel hükümler değerlendirildiğinde bu suç tipleri için iştirak türlerinin gerçekleşmesi mümkündür

6.3. İçtima

Bu suç zincirleme şekilde işlenebilir. Kişi belli zaman aralıklarla bilişim sistemine girerek aynı kişiye karşı birden fazla haksız yarar sağlayabilir. Bu suçun mütemadi şekilde işlenmesi de mümkündür kişi bilişim sistemine girerek aralıksız şekilde sistemden haksız çıkar sağlayabilir, bu durumda tek suçun işlendiğini kabul etmek gerekir. Zamanaşımı zincirleme şekilde işlenen suçta son eylemden, mütemadi şekilde işlendiğinde devam eden eylemin bittiği zaman gerçekleşir.

Bu suçta bileşik suçun oluşabilmesi mümkün değildir. Çünkü bileşik suçun oluşabilmesi için biri diğerinin ağırlatıcı nedeni ya da unsuru olan iki ayrı suç bulunmalıdır. Bu suçun unsurlarında böyle bir durum yoktur

Son olarak bu başlıkta şuna da değinebiliriz. T.C.K.'nın 243. maddesindeki suç, T.C.K.'nın 244. maddesinin 4. fıkrasındaki suç için bir geçit olabilir. T.C.K.'nın 244. maddesinin 4. fıkrasındaki "fiillerin işlenmesi suretiyle kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlama" suçunun işlenebilmesi için T.C.K.'nın 243. maddesindeki hukuka aykırı olarak bilişim sistemine girme ve sistemde kalma suçunun islenmesi gerekecektir. Bu durumda yalnızca T.C.K.'nın 244. maddesinin 4. fıkrasındaki suçtan faile ceza verilecektir.

7.Kovuşturma, Görevli Mahkeme, Suçun Yaptırımı ve Dava Zamanaşımı

Kovuşturma: Maddede tanımlanan suçun soruşturması ve kovuşturması resen yapılır

Görevli Mahkeme: 5235 sayılı Kanun'un 10. maddesi uyarınca maddede tanımlanan suçlara dolayısıyla açılan davalara bakma görevi asliye ceza mahkemesine aittir.

Suçun Yaptırımı: T.C.K.'nın 244. maddesinin 4. fıkrasına göre, bilişim sisteminin işleyişini engelleyen veya bozan, bilişim sistemindeki verileri bozan, yok

eden, değiştiren veya erişilmez kılan, sisteme veri yerleştiren, var olan verileri başka bir yere gönderen kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlamasının başka bir suç oluşturmaması hâlinde, iki yıldan altı yıla kadar hapis ve beşbin güne kadar adlî para cezasına hükmedileceği düzenlenmiştir. Yasa'daki "ve" ifadesinden, yaptırımın seçenekli olmadığı anlaşılmaktadır. Buna göre, faile hem hapis cezası hem de adli para cezası verilecektir. Adli para cezasının miktarının ne olacağı ve nasıl hesaplanacağı ise T.C.K.'nın 52.maddesine göre yapılacaktır.

T.C.K.'ya göre fiili isleyen tüzel kişilikse, tüzel kişiye T.C.K. madde 20/2 gereğince ceza verilemeyecektir. Bu durumda, T.C.K. 246. maddesine göre T.C.K.'nın 60. maddesindeki güvenlik tedbirleri uygulanır.

Dava Zamanaşımı: T.C.K.'nın 66/1-e maddesi uyarınca bu suçun dava zamanaşımı süresi 8 yıldır

d. Banka veya Kredi Kartlarının Kötüye Kullanılması Suçu[222]

1. Genel Olarak

Maddenin tarihçesi şu şekildedir. 01.06.2005 tarihinde 2 fıkra olarak düzenlenmişti. 29.06. 2005 tarih ve 5377 sayılı Kanun ile maddeye 2. ve 4. Fıkralar eklenmiş, 3. Fıkranın üst sınırı arttırılmış ve adli para cezası ilave edilmiş, 06.12.2006 tarih ve 5560 sayılı Kanun ile de 5. fıkra eklenmiştir. Böylece iki fıkra olarak düzenlenen madde bugün beş fıkraya yükselmiştir.

Daha önce de 765 sayılı eski T.C.K.'nın 525 b/2 maddesini açıklarken, T.C.K.'nın 525 b/2 fıkrasında düzenlenen "bilişim sistemi aracılığıyla hukuka aykırı yararın elde edilmesi suçunun" banka ve kredi kartlarının kullanılmasıyla hukuka aykırı yarar elde edilmesini kapsayıp kapsamadığı konusunda farklı düşünceler

222 5237 sayılı T.C.K.'nın 245 Maddesi:

"[1] (8.7.2005 T. 5377 sk değ.) [1] Başkasına ait bir banka veya kredi kartını, her ne suretle olursa olsun ele geçiren veya elinde bulunduran kimse, kart sahibinin veya kartın kendisine verilmesi gereken kişinin rızası olmaksızın bunu kullanarak veya kullandırtarak kendisine veya başkasına yarar sağlarsa, üç yıldan altı yıla kadar hapis ve beşbin güne kadar adlî para cezası ile cezalandırılır.

[2] Başkalarına ait banka hesaplarıyla ilişkilendirilerek sahte banka veya kredi kartı üreten, satan, devreden, satın alan veya kabul eden kişi üç yıldan yedi yıla kadar hapis ve onbin güne kadar adlî para cezası ile cezalandırılır.

[3] Sahte oluşturulan veya üzerinde sahtecilik yapılan bir banka veya kredi kartını kullanmak suretiyle kendisine veya başkasına yarar sağlayan kişi, fiil daha ağır cezayı gerektiren başka bir suç oluşturmadığı takdirde, dört yıldan sekiz yıla kadar hapis ve beşbin güne kadar adlî para cezası ile cezalandırılır.

[4] Birinci fıkrada yer alan suçun;

a) Haklarında ayrılık kararı verilmemiş eşlerden birinin,

b) Üstsoy veya altsoyunun veya bu derecede kayın hısımlarından birinin veya evlat edinen veya evlâtlığın,

c)Aynı konutta beraber yaşayan kardeşlerden birinin,

Zararına olarak işlenmesi hâlinde, ilgili akraba hakkında cezaya hükmolunmaz.

[5] (19.12.2006 T. 5560 sk. ek) Birinci fıkra kapsamına giren fiillerle ilgili olarak bu Kanunun malvarlığına karşı suçlara ilişkin etkin pişmanlık hükümleri uygulanır.

olduğunu, ancak YCGK'nun bu konuda verdiği karar[223] ile bu tartışmalar sona erdiğini belirtmiştik. Kanunkoyucu banka ve kredi kartlarının kullanılmasıyla hukuka aykırı yarar elde edilmesi suçunu bağımsız bir suç tipi düzenleyerek tüm tartışmalara son vermiştir. Kanun maddesinin gerekçesinde de *"Aslında hırsızlık, dolandırıcılık, güveni kötüye kullanma ve sahtecilik suçlarının ratio legis'lerinin tümünü de içeren bu fiillerin, duraksamaları ve içtihat farklılıklarını önlemek amacıyla, bağımsız suç haline getirilmesi uygun görülmüştür"* denilmiştir.

Bu suçların daha iyi anlaşılabilmesi için banka kartı ve kredi kartı kavramlarının açıklanması gerekmektedir.

01.03.2006 Tarihinde Resmi Gazete'de yayımlanarak yürürlüğe giren 5464 sayılı Banka Kartları ve Kredi Kartları Kanununun "Tanımlar" başlığında bu kavramlar şu şekilde açıklanmıştır.

Banka Kartı: Mevduat hesabı ve özel cari hesapların kullanımı dahil bankacılık hizmetlerinden yararlanmayı sağlayan kartı,

Kredi Kartı: Nakit Kullanımı gerektirmeksizin mal ve hizmet alımı veya nakit çekme olanağı sağlayan basılı kartı veya fiziki varlığı bulunmayan kart numarasını,

İfade eder.

Bankanın kurduğu otomasyon sistemine hukuka uygun olarak girmeyi sağlayan banka kartı, kart sahibi tarafından bilinen bir şifre aracılığıyla banka görevlisinin yardımına gerek olmadan hesaptan ATM[224] aracılığıyla para çekmeyi sağlarken; kredi kartları, banka ile kart hamili arasında yapılan sözleşme gereğince kişinin bankanın belirli koşullarla sağladığı kredi olanağından yararlanması sonucunu doğurmaktadır[225].

Kredi kartın özelliği ve bu kartı, banka kartından ayıran en önemli nokta, kullanıcına sağladığı kredi olanağıdır. Kullanıcı, kullandığı krediyi vadesi geldiğinde geri ödeyecektir[226]. Bir başka anlatımla, kredi kartı hamilinin hesabında para bulunmasa da alışveriş yapma imkanı bulunmaktadır.

---

223 YGCK 10.04.2001, 2001/76-30 E, 2001/757 K, "…….Yukarıdaki açıklamalar ışığında somut olay değerlendirildiğinde, sanığın haksız olarak ele geçirdiği bir başkasına ait kart ve şifreyi kullanarak bir bankanın iki farklı şubesindeki ATM makinesinden para çekip hukuka aykırı yarar sağlaması eylemi TCY'nin 493/2. madde ve fıkrasındaki suçu değil aynı yasanın 525/b.2 madde ve fıkrasında düzenlenen bilgileri otomatik isleme tabi tutmuş bir sistemi kullanarak hukuka aykırı yarar sağlamak suçunu oluşturduğundan Yargıtay C. Başsavcılığı'nın itirazının kabulüne karar verilmelidir." - UYAP Mevzuat Programı

224 ATM: Automated Teller Machine (Otomatik Ödeme Makinesi)

225 Taşdemir Kubilay, Bilişim, Banka Veya Kredi Kartlarının Kötüye Kullanılması Ve Dolandırıcılık Suçları, Ankara, Temmuz 2009 s.313

226 Kurt Levent, s.180

2. Korunan Hukuksal Değer

T.C.K.'nın 245. maddesinin gerekçesinde suçun korunan hukuksal değeri ayrıntılı olarak açıklanmıştır. Bu suçun konuluş amacı, banka veya kredi kartlarının hukuka aykırı olarak kullanılması suretiyle bankaların veya kredi sahiplerinin zarara sokulmasının ve bu yolla çıkar sağlanmasının önlenmesi ile faillerin cezalandırılmasıdır. Banka veya kredi kartlarının kötüye kullanılması suçunda korunmak istenen hukuksal değer aslında "hırsızlık, dolandırıcılık, güveni kötüye kullanma ve sahtecilik suçları" ile korunan hukuksal değerlerin tamamıdır. Hırsızlık suçu ile kişinin malvarlığı, dolandırıcılık suçu ile hem kişinin karar verme hürriyeti hem de malvarlığı dokunulmazlığı, güveni kötüye kullanma suçu ile kişilerin birbirine karsı duyduğu kişisel güven ve sahtecilik suçu ile de hukuk alanında inandırıcılığı olan belgelere olan güven korunmak istenmektedir. Bu suç tipi ile de bahsettiğimiz bu hukuksal değerlerin hepsinin korunduğu doğrudur, ancak bu hukuksal değerler içerisinde en baskın olan kişinin malvarlığıdır ve bu nedenle, bu suçun hukuksal değerinin kişinin malvarlığı olduğunu rahatlıkla söyleyebiliriz[227].

Banka ve kredi kartlarının kötüye kullanılması suçunun hukuksal değerinin kişinin malvarlığı olmasına rağmen bilişim alanında suçlar bölümünde düzenlenmesi eleştirilmektedir. Bu suçun malvarlığına karşı suçlar bölümünde yer almasının kanunu sistematiğine daha uygun düşeceği savunulmaktadır[228].

3. Suçun Maddi Unsurları

3.1. Fail

5237 sayılı T.C.K.'nın 245. maddesinde suçu işleyecek kişi açısından herhangi bir özellik belirtilmediği için suçun faili herkes olabilir.

Bu suçun işlenebilmesi için bazen belli bir bilgi birikimi gerekirken bazen ise gerekmeyebilir. Başkasının kartından izni olmaksızın para çekilmesi durumunda belli bir bilgi birikimi gerekmezken, internet yoluyla başkalarının kart bilgilerine ulaşıp, kullanılmasında belli bir bilgi birikimi gerektiğini kabul etmek gerekir.

Tüzel kişilerin sorumluluğu ise, T.C.K.'nın 246. maddesindeki "Bu bölümde yer alan suçların işlenmesi suretiyle yararına haksız menfaat sağlanan tüzel kişiler hakkında bunlara özgü güvenlik tedbirlerine hükmolunur." hükmü gereğince tüzel kişilere T.C.K.'nın 60. maddesindeki güvenlik tedbirleri uygulanacaktır.

227 Kurt Levent, s.178; Dülger Murat Volkan, s.252,

228 Dülger Murat Volkan, s.252

3.2. Mağdur

Bu suç, mağdur açısından bir özellik göstermemektedir. Herkes bu suçun mağduru olabilir. Ancak yinede önemle belirtilmesi gerekir ki bu suçun mağduru malvarlığında azalma olan gerçek kişilerdir. Bir başka deyişle suçun mağduru Suçun mağduru "**kredi veya banka kartı hamili"**dir. Ayrıca birinci fıkrada "*kartın kendisine verilmesi gereken kişi*" den söz edilmektedir. Bu kişi de esasen kart hamilidir. Yargıtay Ceza Genel Kurulu (YGCK), 04.10.2011 gün ve 2011/166-213 sayılı kararında açıkça belirtmiştir. Y. 11. CD. 19.10.2011 T., 2011/7635-20911 sayılı kararında[229] belirttiğimiz YCGK kararına atıf yaparak *"CGK'nun 4.10.2011 gün ve 2011-166-213 sayılı kararında da belirtildiği üzere, sanığın katılan Fatma Handan'a ait farklı bankalardan verilmiş iki adet kredi kartını rızası dışında ele geçirip aynı gün birden fazla yerden alışveriş yapmak suretiyle menfaat temin etmekten ibaret eyleminde, iki ayrı işlenmiş suç söz konusu olmayıp zincirleme şekilde işlenen tek suçtan hüküm kurulması gerektiği gözetilmeden her kart için ayrı ayrı hüküm kurulması[230]*" kararıyla T.C.K. 245. maddenin 1. fıkrasındaki suçun mağdurunun "**kart hamili**" olduğu şeklinde karar vermiştir. Asıl kart ve asıl karta bağlı ek kartın hamili ayrı ayrı kişiler olsa bile her iki kartın kullanımında da asıl kart sahibi mağdur olacaktır.

Öte yandan, T.C.K.'nın 245. maddesinin 1. fıkrasında, kart sahibinden veya kartın kendisine verilmesi gereken kişiden söz etmektedir. Dolayısıyla T.C.K.'nın 245. maddesinin 1. fıkrasında mağdur kavramını genişletmiş hem kartın sahibini hem de kartın kendisine verilmesi gereken kişiyi koruma altına almıştır. Bu durumda adına kart düzenlenmiş, ancak kart eline ulaşmayan kimse de mağdur olabilecektir[231]. Ancak bu durum tartışmalıdır. Bize göre de kartın, kart sahibine teslim edilmeden çalınması veya başka şekilde başkasının ele geçmesi durumunda mağduru banka olarak kabul etmek gerekir. Aynı şekilde ölü kişinin banka ve kredi kartının bankaya teslim edilmesi gerekirken kullanılması durumunda da banka mağdurdur.

Suçun işlenmesinde her ne kadar banka ve kredi kurumunun bilişim sistemi aracı olarak kullanılmakta ise de; bu sistemlerin kullanılması banka veya ilgili kurumun bu suçun mağduru olduğu anlamına gelmemektedir. Elbette ki, fail

229 Bkz. UYAP Mevzuat Programı

230 Bkz. UYAP Mevzuat Programı

231 Taşdemir Kubilay, s.319

tarafından belirtilen eylemlerin gerçekleştirilmesiyle banka veya finans kurumlarının bilişim sistemlerinin ve kartlarının güvenilirliği ve genel olarak ticari itibarları zarar görmektedir. Bu sebeple, banka veya kredi kurumları "zarar gören" sıfatındadırlar.

Failin hayali hesaplara bağlı olarak ürettiği kartlarla işlem yaparak direkt bankanın ve finans kurumunun malvarlığında bir zarara yol açması durumunda mağdur tabii ki, banka veya finans kurumu olacaktır. Bir başka deyişle T.C.K.'nın 245. maddesinin 2. fıkrasında düzenlenen suçun belirtilen seçimlik hareketlerin yapılması ile oluşacağı, kartın kullanılmaması nedeniyle kart sahibi yönünden bir zarar ihtimali bulunmadığından, suçun mağdurunun hesap sahibi olmayıp kartı çıkarma yetkisine haiz olan ilgili banka, kredi veya finans kurumu olduğu açıktır.

Yargıtay 11. Ceza Dairesinin, T.C.K.'nın 245. maddesinin 1. fıkrasında mağdurun kim olacağına ilişkin bir kararında mağdurun banka olacağına ve banka sayısınca suç oluşacağına yönelik kararı bulunmaktadır[232]. Aynı şekilde T.C.K.'nın 245. maddesinin 3. fıkrasında suçun da mağduru bankadır Yargıtay 11. CD'nin mağdurun banka olacağına ve banka sayısınca suç oluşacağına yönelik kararı da bulunmaktadır[233]

Yukarıdaki açıklamalardan sonra özetle diyebilir ki, T.C.K.nın 245. maddesinin 1. fıkrasında mağdur, malvarlığında eksilme olan banka ve kredi kartı hamili olan kişidir. T.C.K. 245. maddesinin 2 ve 3. fıkrasında ise banka veya finans kurumudur.

3.3. Suçun Konusu

T.C.K.'nın 245. maddesindeki suçun konusu, failin sağladığı yarardır. Bu yarar maddi bir yarardır. Bir başka deyişle para veya menkul değerlerlerdir.[234]

3.4. Hareket

Kanunkoyucu bu suç tipini seçimlik hareketli olarak düzenlemiştir. Bu hareketlerden hangisi gerçekleşirse gerçekleştirilsin banka ve kredi kartlarının kötüye

232 11.C.D. 29.06.2010 T., 2010/1587 E., 2010/7628 K. "5237 sayılı T.C.K.. nun 245/2. maddesinde tanımlanan suçun mağdurunun; kartın henüz kullanılmaması nedeniyle sahibi olmayıp banka veya kredi kartını çıkarma yetkisine haiz banka olacağı, banka veya kredi kartlarının manyetik şeritlerinde yer alan ilk altı rakama ilgili katalogdan bakıldığında kartı çıkaran bankanın belirlenebileceği cihetle; ele geçirilen ve sahte olduğu belirlenen kartların manyetik şeritlerinde yapılan inceleme sonucu tespit edilecek bankalar sayısınca ve aynı bankaya ait birden fazla sahte kredi kartı bulunması halinde zincirleme biçimde ayrı ayrı suçların oluşacağı"

233 Y. 11.C.D. 13.04.2011 T., 2010/16795 E., 2011/2011 K. "Fikir ve eylem birliği içerisinde hareket eden sanıkların manyetik şeridi kopyalanmış Garanti Bankası ve Fortisbank'a ait sahte oluşturulmuş banka kartlarıyla ATM makinelerinden para çekmekten ibaret eylemlerinde, bankaların zarar görmesi nedeniyle mağdur olan banka sayısınca suçun oluşacağı, somut olayda da Garanti Bankası ve Fortisbank'a ait banka kartlarını kopyalayarak birden fazla para çekmekten ibaret eylemlerin zincirleme olarak gerçekleşen iki ayrı suç oluşturduğu gözetilmeden yazılı şekilde hüküm kurularak fazla ceza tayini, "

234 Dülger Murat Volkan, s.253

kullanılması suçu oluşacaktır. Şimdi bu seçimlik hareketleri başlıklar halinde ayrıntılı olarak inceleyelim.

3.4.1. Başkasına Ait Banka veya Kredi Kartıyla Hukuka Aykırı Yarar Sağlama

T.C.K. 245/1 maddesindeki suçun oluşabilmesi için kartın ne şekilde ele geçirildiğinin önemi yoktur. Suçun tanımında "her ne suretle olursa olsun ele geçiren veya elinde bulunduran kimse" denildiğinden, banka veya kredi kartının çalınmış veya yağmalanmış olması ile bulunmuş olması, geçici olarak verilmiş olması arasında fark yoktur. Önemli olan, kart ile kendisine veya başkasına yarar sağlamasıdır. Bu yarar ATM cihazından para çekme şeklinde gerçekleşebileceği gibi alışveriş yapılarak veya başka türlü gerçekleşebilir.

Ele geçirmeden maksat, kartın sahibinin haberi olmadan, bularak ya da yetkisi olmadan, bir başka deyişle mağdurun rızasına aykırı olarak kartın elde edilmesidir. Elinde bulundurmadan maksat ise, mağdurun rızası ile veya bir yetkiye dayanarak kartın elinde bulundurulmasını ifade etmektedir[235]. Bankanın gönderdiği kartları teslim eden kurye veya posta görevlisi elinde bulunduran konumundadır.

Madde de "kart sahibinin veya kartın kendisine verilmesi gereken kişinin rızası olmaksızın" denilerek banka ve kredi kartlarıyla gerçekleşecek her türlü eylemi banka ve kredi kartlarının kötüye kullanılması suçuna sokmak istemiştir. Eskinden öğretide ve Yargıtay kararlarında banka tarafından kartın henüz kullanıcısına teslim etmeden kullanılması durumunda hangi suçun oluşacağı konusunda değişik görüşler bulunmaktaydı[236]., Yukarıda kredi kartını açıklarken fiziki varlığı bulunmayan kart numarası da olabileceğini belirtmiştik. Yargıtay da bir kararında *"sanığın başkalarına ait kredi kartı bilgilerini ele geçirip, bu bilgileri kullanarak internet üzerinden alışveriş yapmak suretiyle haksız yarar sağladığını iddia ve kabul olunmasına göre, eylemin suç tarihinden sonra 01.06.2005 tarihinde yürürlüğe giren 5237 sayılı T.C.K.'nın 245/1 maddesindeki banka ve kredi kartlarının kötüye kullanılması suçunu oluşturacağı*[237]" diğer bir kararında *"Sanığın, şikayetçinin kredi kartı bilgilerini ele geçirerek ortağı olduğu işyerinde "**mail-order**" yöntemiyle, alış veriş yapılmadığı halde yapılmış gibi işlemler yapmak suretiyle yarar sağlamaktan ibaret oluşa uygun olarak sübutu kabul edilen eyleminin, 5464 Sayılı Banka Kartları*

235 Parlar Ali, s.53

236 Ayrıntılı bilgi için bkz. Dülger Murat Volkan, s.255,256

237 Y. 11 CD. 02.05.2011 T., 2010/7432 E., 2011/2321 K – UYAP Mevzuat Programı

ve Kredi Kartları Kanunun 3/e maddesi uyarınca "Kredi kartının, nakit kullanımı gerekmeksizin mal ve hizmet alımı veya nakit çekme olanağı sağlayan basılı kartı veya fiziki varlığı bulunmayan kart numarasını" ifade etmesi karşısında; T.C.K..nun 245/1. maddesinde tanımlanan "banka ve kredi kartlarının kötüye kullanılması" suçunu oluşturduğu gözetilmeden yazılı şekilde dolandırıcılık suçundan mahkumiyetine karar verilmesi,[238] " şeklindeki kararıyla fiziki varlığı bulunmasa da kart numarası ile yapılan işlemin T.C.K.'nın 245. maddesinin 1. fıkrasındaki suçu oluşturacağına karar vermiştir.

T.C.K.'nın 245. maddesinin 5 fıkrasında, 1. fıkra kapsamına giren fiillerle ilgili olarak etkin pişmanlık hükümleri uygulanacağı hüküm altına alınmıştır. Bu konuyu suça etki eden faktörler başlığı altında inceleyeceğiz.

3.4.2. Başkalarına ait banka hesaplarıyla ilişkilendirilerek sahte banka veya kredi kartı üretme, satma, devretme, satın alma veya kabul etme

Suçun konusu, gerçek bir banka hesabı ile ilişkilendirilerek üretilen, satılan, devredilen, satın alınan, kabul edilen sahte banka veya kredi kartı veya kartlarıdır.

Başkalarına ait kredi veya banka hesaplarıyla ilişkilendirme unsuru bulunuyor ise 5237 sayılı T.C.K.'nın 245. maddesinin 1. fıkrasının uygulanması gerekmektedir. İlişkilendirilen bir hesap bulunmuyor sadece sahte oluşturulan kredi veya banka kartı aracılığıyla menfaat temin etme söz konusu ise T.C.K.'nın 245. maddesinin 3. fıkrasındaki suç oluşacaktır.

Sahte banka veya kredi kartı oluşturmak, Encoder, enbosser gibi teknik cihazlarla olabileceği gibi, sahte belgelerle bankalara yapılan müracaat ile de olabilir[239].

Hemen burada T.C.K.'nın 245. maddesinin 2. fıkrasındaki suç ile 5464 sayılı Banka Kartları ve Kredi Kartları Kanunu'nun 37/2. maddesinde yer alan suçun farkını vermek gerekir.

5464 sayılı Kanunda kredi kartı veya üye işyeri sözleşmesinde veya eki belgelerde sahtecilik yapanlar veya sözleşme imzalamak amacıyla sahte belge ibraz edenler cezalandırılmaktadır. Burada belirtilen suç tipi tehlike suçudur. Çünkü kanun koyucu bu suçun oluşumunu bir zarar sonucuna bağlamamıştır[240].

238 Y. 11 CD. 07.07.2010 T., 2008/80 E., 2010/8096 K. - UYAP Mevzuat Programı

239 Budak Mesut, Hakimler Ve Savcılar Yüksek Kurulu (HSYK) Bilişim Hukuku Semineri 18-22 Mart 2013, www.hsyk.gov.tr

240 Budak Mesut, Hakimler Ve Savcılar Yüksek Kurulu (HSYK) Bilişim Hukuku Semineri 18-22 Mart 2013, www.hsyk.gov.tr

Hangi eylemlerin 5464 sayılı Banka Kartları ve Kredi Kartları Kanunu'nun 37/2. maddesinde yer alan suç kapsamına gireceğini belirten Yargıtay kararları ile açıklamaya çalışalım.

"Sanığın şikayetçi Akbank'a müracaat ederek kredi kartı talebinde bulunması üzerine başvuru aşamasında anılan banka tarafından kredi kartı sözleşmesi imzalanmadan isteminin reddine karar verildiği anlaşılmakla eylemin 5464 sayılı "Banka Kartları ve Kredi Kartları Kanunu"nun 37/2.maddesinde düzenlenen suçu oluşturup oluşturmayacağı karar yerinde tartışılmadan olayda uygulama yeri olmayan T.C.K..nun 245/3, 35.maddeleri ile hüküm kurulması,[241] "

"5464 sayılı Banka Kartları ve Kredi Kartları Kanununun 01.03.2006 tarihinde yürürlüğe girdiği ve anılan kanunun 37/2. maddesindeki "kredi kartı veya üye işyeri sözleşmesinde veya eki belgelerde sahtecilik yapanlar veya sözleşme imzalamak amacıyla sahte belge ibraz edenler" ile ilgili düzenlemenin sözleşmeye kadar olan safhada uygulanabileceği, sahte belgelerle kredi kartı alınması halinde ise 5237 sayılı T.C.K.'nın 245/2. maddesindeki suçun oluşacağı gözetilmeden, 5464 sayılı Kanuna muhalefet suçundan hüküm kurulması aleyhe temyiz olmadığından bozma sebebi yapılmamıştır.[242] "

Görüldüğü üzere kart daha üretilmeden şahıs yakalanmışsa 5464 sayılı kanun uygulanmaktadır. Kart üretildikten sonra ise artık T.C.K. T.C.K.'nın 245. maddesinin 2. fıkrasındaki suç olacaktır.

3.4.3. Sahte Oluşturulan veya Üzerinde Sahtecilik Yapılan Banka veya Kredi Kartıyla Hukuka Aykırı Yarar Sağlama

5237 sayılı T.C.K.'nın 245. maddesinin 3. fıkrasında bahsedilen kartlar ya tamamen sahte olarak üretilen kartlar ya da gerçek olarak üretilmesine rağmen üzerinde değişiklik yapılarak sahteleştirilen kartlardır.

Sahte kart oluşturma eylemi, genellikle bu kartları üretmeye yarayan cihazlarla gerçekleştirilmektedir. Banka kartının üzerinde kart sahibinin banka hesabıyla ilgili bilgileri içeren manyetik bir şerit vardır. Bu manyetik şeride söz konusu bilgiler "encoder" adı verilen bir aygıtla yüklenmektedir[243].

Gerçek kart üzerinde sahtecilik yapma eylemi, bu seçimlik harekette akla ilk olarak gerçek kredi kart üzerindeki sahibinin isminin veya imzasının değiştirilmesi

241 Y. 11.C.D. 21.06.2010 T., 2010/4547 E., 2010/7082 K.

242 Y. 11.C.D. 27.12.2010 T., 2010/14919 E., 2010/15192 K. – UYAP Mevzuat Programı

243 Akbulut Berrin s.78

gelmektedir. Resimli kartlarda kart sahibinin resminin değiştirilip failin resminin konularak kartın kullanılması da T.C.K.'nın 245. maddesinin 3. fıkrasındaki suçu oluşturur[244].

Suçun oluşması için sahte oluşturulan kartın iğfal kabiliyetinin olup olmamasının bir önemi yoktur[245].

3.5. Netice

5237 sayılı T.C.K.'nın 245. maddesinin 1. ve 3. fıkralarında düzenlenen banka veya kredi kartlarının kötüye kullanılması suçunun gerçekleşebilmesi için failin belirtilen eylemleri yapması neticesinde kendisine veya başkasına bir yarar sağlaması gerekmektedir. Bu suç tipinde failin belirtilen eylemleri gerçekleştirmesi sonucunda kendi malvarlığında bir artış meydana gelecektir, mağdurun malvarlığında ise bir azalma olacaktır. Bu nedenle bu suçta zararın oluşmaması mümkün değildir[246].

5237 sayılı T.C.K.'nın 245. maddesinin 2. fıkrasında düzenlenen suçun oluşması için madde metninde sayılan seçimlik hareketlerin gerçekleştirilmesi yeterlidir. Ayrıca bu eylemler neticesinde bir zararın oluşması aranmaz.

Bu açıklamalardan sonra diyebiliriz ki, T.C.K.'nın 245.maddesinin 1. ve 3. fıkraları zarar suçu iken 2.fıkrası bir tehlike suçudur.

4. Suçun Manevi Unsurları

T.C.K. 245. maddesinde düzenlenen suç ancak kasten işlenebilir. Failin bilerek ve isteyerek hareket etmesi bu suçun oluşumu için yeterlidir. 5237 sayılı T.C.K.'nın 245. maddesinin 1. ve 3. fıkralarında "kendisine veya başkasına yarar sağlayan kişi" ifadesi kullanılarak özel kast aranmıştır.

T.C.K.'nın 245. maddesinin 2. fıkrasında ise üretme kastı yeterlidir, bu nedenle Kanunkoyucu 2. fıkrası genel kast aramıştır[247].

Bu suçun kasten işlenmesi arandığından taksirle işlenemez.

5. Hukuka Aykırılık

Failin yarar sağladığı hareketleri rızaya dayalı olarak gerçekleştirdiği durumlarda suç oluşmayacaktır. Kanunda da "kart sahibinin veya kartın kendisine

244 Karagülmez Ali, s.311

245 Kurt Levent, s. 193

246 Karagülmez Ali, s.315

247 Karagülmez Ali, s.310

verilmesi gereken kişinin rızası olmaksızın" ibaresi kullanılarak açı şekilde belirtilmiştir.

Bu suçun yasanın verdiği bir yetkiye dayanılarak gerçekleştirilmesiyle hukuka uygun hale gelmesi ile ilgili düzenleme bulunmamaktadır[248].

6. Suçun Özel Görünüş Şekilleri

6.1. Teşebbüs

Banka ve kredi kartlarıyla ilgili 245. maddenin 1. ve 3. fıkralarındaki suçlarda suçun tamamlanması için yararın sağlanması gerekir. Yarar sağlanamadan hareketlerin yarıda kalması durumunda teşebbüs söz konusu olur.

Sahte oluşturulan veya her ne suretle olursa olsun elde edilmiş olan kartın ATM'ye sokulup işleme başlanması sırasından makinenin bağlantısının kesilmesi suça teşebbüs olacaktır[249]. Aynı şekilde sahte kredi kartı kullanılırken durumun banka görevlisi tarafından farkedilmesi durumunda da suça teşebbüs olacaktır.

Burada şu hususu da belirtmek gerekmektedir. T.C.K.'nın 245. maddesindeki suç tipi seçimlik hareketli bir suç olduğu için eylemlerin herhangi birinin tamamlanmış olması durumunda, diğer eylemler teşebbüs aşamasında kalmış olsa da suça teşebbüsten bahsedemeyiz.

6.2. İştirak

Suça iştirak açısından banka ve kredi kartlarının kullanılması suçunda bir farklılık olmayıp genel hükümler çerçevesinde değerlendirilir.

Ayrıca bu suçta üçüncü bir kişinin vasıta kılınarak suçun işlenmesi mümkün olduğu için "dolayısıyla faillik" durumu gerçekleşebilir. Madde metninde "kullandırtarak" sözcüğünün kullanılmış olması dolayısıyla failliğin mümkün olacağını göstermektedir. Ancak bu durumun söz konusu olabilmesi için eylemi bizzat gerçekleştiren kişinin yaptığı eylemin hukuka aykırı olduğunu bilmemesi ve suç işleme kastının bulunmaması gerekir[250].

248 Dülger Murat Volkan, s.262

249 Dülger Murat Volkan, s.263

250 Dülger Murat Volkan, s.263

6.3. İçtima

Yargıtay daha önceki kararlarında mağdura ait kart sayısınca suçun olduğunu savunmaktaydı[251]. Ancak son kararları ile bu görüşü bırakan Yargıtay mağdur sayısınca suçun olduğu görüşünü savunmaya başlamıştır.

Aynı "kart hamiline" ait aynı veya değişik bankalarca düzenlenen birden fazla kartın ele geçirilerek kullanılması halinde T.C.K.'nın 245. maddesinin 1. fıkrasındaki suçla ilgili zincirleme hükümleri dikkate alınarak failin cezalandırılmasına karar vermek gerekecektir. Nitekim Yargıtay da bu yönde karar vermiştir. *"5237 sayılı T.C.K.'nun 245/1 madde ve fıkrasında düzenlenen başkasına ait banka veya kredi kartını kötüye kullanmak suçunun mağduru hesap sahibi olan gerçek yada tüzel kişiler olduğu cihetle, aynı kişiye ait fakat farklı bankalarca tahsis edilmiş banka veya kredi kartı sayısı nedeniyle bağımsız suçtan bahsedilemeyeceği, aynı kişiye ait farklı bankalarca tahsis edilmiş birden fazla banka veya kredi kartının kullanılması halinde zincirleme suç hükümlerinin uygulanabileceği ancak kart ve kullanım sayısı ile yarar miktarının T.C.K.'nun 61. maddesi uyarınca temel cezanın belirlenmesi ve zincirleme suç hükümleri nedeniyle cezada yapılacak artırım oranının belirlenmesi sırasında değerlendirilmesi gerektiği gözetilmeden mağdur banka adedince suç oluşacağından bahisle yazılı şekilde fazla ceza verilmesi,[252]"*

"Sanığın, mağdurun Manisa Devlet Hastanesi'nde unuttuğu çantanın içinde bulunan Yapı Kredi ve Denizbank'a ait kredi kartlarını alıp, sahibinin rızası olmadan bankamatikten para çekmek ve alışveriş yapmaktan ibaret eyleminin, ...5237 sayılı Yasanın 245/1 nci ve 43. maddelerindeki suçu oluşturacağı.....[253]"

5237 sayılı T.C.K.'daki suçların içtiması bakımından kural olarak, kaç tane fiil varsa o kadar suç, kaç tane suç varsa o kadar ceza vardır, diyebiliriz. Peki, banka ve kredi kartlarının kötüye kullanılması suçu ile kanundaki diğer suçlar arasında içtima hükümleri nasıl uygulanacaktır. Bu konuda YCGK'nun ve 11. Ceza Dairesinin kararları verdir. Yargıtay 11. Ceza Dairesi bir kararında YCGK'nun kararına da atıf yaparak şu şekilde karar vermiştir.

---

251 Y. 11.CD. 11.03.2008 T., 2008/679 E., 2008/1431 K., "5237 sayılı T.C.K.. nun 245/1. maddesinde öngörülen "banka veya kredi kartlarının kötüye kullanılması" suçunun, hükmün düzenleme amacı ve düzenleniş biçimi ile korunan hukuki menfaat gözetildiğinde kart sayısınca oluşacağı ve zincirleme suç hükmünün de (T.C.K.. nun 43. maddesi) aynı kartın farklı zamanlarda birden fazla kullanılması, halinde uygulanacağı cihetle, somut olayda mağdur Mehmet Coşkun Şitil'e ait 5504…… 6477 no'lu ve mağdur Şenel Sitil'e ait 4509 ……..3790 no'lu iki ayrı bankadan verilmiş iki kredi kartının alışverişlerde kullanılmakla birbirinden bağımsız iki ayrı suçun oluştuğu, mağdur Şenel'e ait kartın farklı zaman dilimlerinde beş ayrı işlemde kullanılması nedeniyle de zincirleme suçun sübut bulduğu nazara alınmadan yazılı şekilde tek zincirleme suçtan mahkumiyet kararı verilerek sanığa eksik ceza tayini"

252 Y. 11. CD., 08.03.2011 T., 2010/16996 E., 2010/1319 K.- UYAP Mevzuat Programı

253 Y. 11. CD., 14.02.2008 T., 2006/1642 E., 2008/798 K. - UYAP Mevzuat Programı

" Yargıtay Ceza Genel Kurulunun 30.03.2010 gün 17-65 sayılı kararında açıklandığı üzere; ATM'ye kurulan düzenek ile para çekmek için gelen mağdurların şifreleri de öğrenilmek suretiyle ele geçirilen ve ekonomik değeri bulunduğu hususunda kuşku bulunmayan menkul mal niteliğindeki banka kartı ile başka bir ATM cihazına gidip para çekilmesi şeklinde gerçekleştirilen eylemlerin banka veya kredi kartının kötüye kullanılması suçu yanında hırsızlık suçunu da oluşturduğu,[254]"

Yargıtay kararı da değerlendirildiğinde, kartın ele geçiriliş şekli bir suç oluşturuyorsa o suçtan da cezalandırma yapılacaktır. Örnek olarak, hırsızlık, yağma, dolandırıcılık gibi suçlar neticesinde banka ve kredi kartı ele geçirilmiş ve kullanılmak suretiyle yarar elde edilmişse, Hem bu suçlardan hem de 245/1'de düzenlenen banka ve kredi kartlarını kullanmak suçundan olmak üzere iki ayrı suçtan cezalandırma yapılacaktır. KARAGÜLMEZ'e göre ise her iki suçtan birlikte cezalandırma yapabilmek için hırsızlık yağma ve dolandırıcılık suçlarının işleniş şeklinin önemli olduğunu belirtmektedir. Şöyle ki suçlar fail tarafından doğrudan kartın ele geçirilmesi için işlenmişse T.C.K. madde 44'e göre en ağır suçtan cezalandırma yapılacağı, ancak fail, mağdurun çantasını hırsızlık, dolandırıcılık veya yağma suçlarından birini işleyerek almış ve çantanın içinden çıkan kartı kullanmış ise bu durumda gerçek içtima hükümleri gereğince her iki suçun oluşacağını savunmaktadır[255]. Ancak 'güveni kötüye kullanma' ve 'kaybolmuş veya hata sonucu ele geçmiş eşya üzerinde tasarrufta bulunma' suçu yönünden iki ayrı suç olmayacağı görüşündeyiz[256]. Çünkü bu iki suçun oluşabilmesi için kartın kullanılması şartı gerekir. Kartın kullanılarak yarar elde edilmesi ile iki suçun da unsurları oluşmuş olacaktır. Yani, burada tek bir fiile birden fazla kanun maddesinin ihlal edilmesi durumu vücut bulmaktadır. Bu durumda da T.C.K. madde 44 gereğince cezası en ağır olan suçtan cezalandırma yapılacaktır. Bu suç maddesi de T.C.K.'nın 245. maddesinin 1. fıkrasında düzenlenen banka ve kredi kartlarının kötüye kullanılması suçudur[257]. Yargıtay da bu konuda *".... sanığın, hileli davranışlarda bulunmadan ATM'den maaşını çekmek için kendisinden yardım isteyen katılanın verdiği bankamatik kartını ve şifresini öğrendikten sonra kartı bankamatiğin geri vermediğini söyleyerek katılanın ayrılmasından sonra kartı ve*

254 Y. 11. CD., 01.12.2010 T., 2010/13854 E., 2010/13778 K. - UYAP Mevzuat Programı

255 Ayrıntılı bilgi için bkz. s.267-271

256 Aynı görüş için bkz. Budak Mesut "Hakimler Ve Savcılar Yüksek Kurulu (HSYK) Bilişim Hukuku Semineri", 18-22 Mart 2013, www.hsyk.gov.tr

257 Karagülmez Ali, s.270

şifreyi kullanarak hesaptaki parayı çekmekten ibaret eyleminin kart üzerindeki zilyetliğin özgür irade ile devredilmeyip, sanığın yanında beklenerek çok kısa bir süre ve yardım etmesi için verildiğinden güveni kötüye kullanma suçu oluşmayıp T.C.K. 245/1 maddesindeki yazılı suçu oluşturduğu…….gözetilmeyerek yazılı şekilde hüküm kurulması bozmayı gerektirmiştir.[258]*"* şeklinde karar vermiştir.

T.C.K.'nın 245. maddesinin 2. fıkrasında bankalar sayısınca suç vardır. Aynı bankaya ait birden fazla sahte kredi kartı bulunması halinde zincirleme suç hükümleri uygulanacaktır[259].

Sahte banka veya kredi kartı üreten, satan, devreden, satın alan veya kabul eden kişi bu kartı kullanarak kendisine veya bir başkasına yarar sağlar ise T.C.K.'nın 245. maddesinin 2. ve 3. fıkralarındaki suçların ikisinin de oluştuğu kabul edilmelidir. Ortada tek bir fiil olmadığı için fikri içtimadan söz edilemez. Sahte kredi kartı üretme, satma, kabul etme eylemleri T.C.K.'nın 245. maddesinin 3. fıkrasında düzenlenen suçun unsurunu veya ağırlaştırıcı sebebini oluşturmamaktadır. Bu nedenle iki ayrı suçun oluşacağına tereddüt yoktur[260]. Bu konuda verilmiş olan Yargıtay kararı da bulunmaktadır[261].

Bize göre, T.C.K.'nın 245 maddesinin 3. fıkrasının müstakil bir suç olarak değil, 2. fıkradaki suçun ağırlaştırıcı sebebi olarak düzenlenmesi gerekmektedir.

T.C.K.'nın 245. maddesinin 2. ve 3. fıkralarını kendi aralarında ve 5464 sayılı Kanunun 37. maddesinin 2 fıkrası ile kısaca karşılaştırmak gerekirse. Eğer, sahte nüfus cüzdanı, maaş ilmühaberi v.s. gibi bir takım belgelerle yapılan başvuru sonucu yapılan incelemede belgelerin sahte olduğu anlaşılmış ve bankaca kart üretilmeden suç duyurusunda bulunulması halinde, 5464 sayılı Banka Kartları ve Kredi Kartları Kanunu madde. 37/2; eğer yapılan bu müracaat sonucunda verilen evrakların sahteliği bankaca anlaşılmayarak faile kredi kartı teslim edilmiş ve kart kullanılarak

---

258 Y. 11. CD. 22.02.2010, 2008/1318 E., 2010/1636 K. UYAP Mevzuat Programı

259 11.C.D. 29.06.2010 T., 2010/1587 E., 2010/7628 K. "5237 sayılı T.C.K.. nun 245/2. maddesinde tanımlanan suçun mağdurunun; kartın henüz kullanılmaması nedeniyle sahibi olmayıp banka veya kredi kartını çıkarma yetkisine haiz banka olacağı, banka veya kredi kartlarının manyetik şeritlerinde yer alan ilk altı rakama ilgili katalogdan bakıldığında kartı çıkaran bankanın belirlenebileceği cihetle; ele geçirilen ve sahte olduğu belirlenen kartların manyetik şeritlerinde yapılan inceleme sonucu tespit edilecek bankalar sayısınca ve aynı bankaya ait birden fazla sahte kredi kartı bulunması halinde zincirleme biçimde ayrı ayrı suçların oluşacağı"

260 Bud AK Mesut Hakimler Ve Savcılar Yüksek Kurulu (HSYK) Bilişim Hukuku Semineri 18-22 Mart 2013, www.hsyk.gov.tr

261 Y. 11.C.D. 17.10.2011 T., 2011/11074 E., 2011/20847 K."T.C.K..nun 245.maddesinin 2.fıkrasında düzenlenen "sahte kredi kartı üretmek" suçunun, 3.fıkrada düzenlenen "sahte üretilmiş kredi kartını kullanmak" suçunun unsuru ya da ağırlatıcı nedeni olmaması sebebiyle bağımsız suçu oluşturacağı, somut olayda; Şenel G. adına düzenlenmiş sahte nüfus cüzdanını kullanarak temin ettiği sahte belgelerle Akbank, Şekerbank ve HSBC Bankasından sahte kredi kartları alıp kullanan sanıklar hakkında ayrıca T.C.K..nun 245/2 maddesinin de uygulanmasının gerektiğinin, … gözetilmemesi isabetsizliği sanıklar aleyhine temyiz olmadığından bozma sebebi sayılmamıştır."

bir yarar sağlanmış ise, T.C.K. md.245/2 + 245/3. maddeleri[262]; eğer bu şekilde ele geçirilen kart hiç kullanılmadan failde yakalanmış ise, sadece T.C.K.'nın 245. maddesinin 2. fıkrası söz konusu olacaktır.

Burada hemen şunu eklemek gerekir ki, kredi kartı başvurusu sırasında kullanılan sahte belgelerden dolayı fail hakkında şayet T.C.K.'nın 245. maddesinin 3. fıkrası uyarınca cezaya hükmolunacak ise, aynı kanunun 212.maddesi gereğince sahtecilik suçundan da ayrıca cezaya hükmolunulacaktır.

Son olarak, Banka veya Kredi Kartının Kötüye Kullanılması Suçu yanında ayrıca 243. maddeden de ceza verilebilir mi sorusu da akla gelebilmektedir. Fail ele geçirdiği veya elinde bulundurduğu gerçek banka veya kredi kartı numarası ile bilişim sistemi üzerinden yarar elde edebilmesi için mutlaka bir bankanın bilişim sistemine girmek zorundadır. Bilişim sistemine girme bu durumda T.C.K.'nın 245 maddesinin unsurudur, geçit suçu konumundadır[263]. T.C.K.' nın 42. maddesinde düzenlenen "bileşik suç" hükümleri dikkate alındığında tek bir suçtan cezalandırma olacağını kabul etmek gerekir.

7. Suça Etki Eden Sebepler

T.C.K.'nın 245. maddesinin 4. fıkrasına göre

a) Haklarında ayrılık kararı verilmemiş eşlerden birinin,

b) Üstsoy veya altsoyunun veya bu derecede kayın hısımlarından birinin veya evlat edinen veya evlâtlığın,

c) Aynı konutta beraber yaşayan kardeşlerden birinin,

Zararına olarak işlenmesi hâlinde, ilgili akraba hakkında cezaya hükmolunmaz.

T.C.K.'nın 245. maddesinin 5. fıkrası (19.12.2006 T. 5560 sk. ek) "Birinci fıkra kapsamına giren fiillerle ilgili olarak bu Kanunun malvarlığına karşı suçlara ilişkin etkin pişmanlık hükümleri uygulanır." hükmü uyarınca

1- Fail tarafından mağdurun zararı kovuşturma başlamadan önce aynen geri verme veya tazmin suretiyle tamamen giderilmesi halinde cezanın 2/3'sine kadarı indirilebilecek,

2- Etkin pişmanlık kovuşturma başladıktan sonra fakat hüküm verilmezden önce verilmesi halinde, verilecek ceza yarısına kadar indirilir.

262 Aksi görüş için bkz. Taşkin Şaban Cankat s.74 "…… bu durumda failin T.C.K. 158/1.f'deki nitelikli dolandırıcılıktan cezalandırılması gerekeceği"

263 Dülger Murat Volkan, s.264

8. Kovuşturma, Görevli Mahkeme, Suçun Yaptırımı ve Dava Zamanaşımı

Kovuşturma: Maddede tanımlanan suçun soruşturması ve kovuşturması resen yapılır

Görevli Mahkeme: 5235 sayılı Kanun'un 10. maddesi uyarınca maddede tanımlanan suçlara dolayısıyla açılan davalara bakma görevi asliye ceza mahkemesine aittir.

Suçun Yaptırımı: T.C.K. 245/1 fıkrasındaki suçu işleyenler üç yıldan altı yıla kadar hapis ve beşbin güne kadar adlî para cezası ile; T.C.K. 245/2 maddesindeki suçu işleyenler üç yıldan yedi yıla kadar hapis ve onbin güne kadar adlî para cezası ile; T.C.K. 245/3 maddesindeki suçu işleyenler dört yıldan sekiz yıla kadar hapis ve beşbin güne kadar adlî para cezası ile cezalandırılır.. Kanun maddesindeki "ve" ifadesinden, yaptırımın seçenekli olmadığı anlaşılmaktadır. Buna göre, faile hem hapis cezası hem de adli para cezası verilecektir. Adli para cezasının miktarının ne olacağı ve nasıl hesaplanacağı ise T.C.K. 52. maddeye göre yapılacaktır.

T.C.K.'ya göre fiili isleyen tüzel kişilikse, tüzel kişiye T.C.K. 20/2 gereğince ceza verilemeyecektir. Bu durumda, T.C.K. madde 246'ya göre T.C.K.'nın 60. maddesindeki güvenlik tedbirleri uygulanır.

Dava Zamanaşımı: T.C.K.'nın 66/1-e maddesi uyarınca bu suçun dava zamanaşımı süresi 8 yıldır

9. Yargıtay Kararları

Yargıtay son dönemlerde T.C.K. 245. madde ile ilgili görüş değişikliğine gitmiştir. Yeni içtihatlarının bir kısmını konuyu anlatırken paylaştık. Bunun dışında, T.C.K.'nın 245. maddesinin 1. fıkrasında mağdurun kart sahibi T.C.K.'nın 245. maddesinin 2. ve 3. fıkralarında ise banka olduğuna yönelik yeni içtihatlarından öne çıkanlar aşağıda sunmaktayız.

11. CD. 29.02.2012 T., 2008/14963 E., 2012/2585 K.[264]

"5464 sayılı Banka Kartları ve Kredi Kartları Kanunu'nun 3/e maddesi uyarınca "kredi kartının, nakit kullanımı gerekmeksizin mal ve hizmet alımı veya nakit çekme olanağı sağlayan basılı kartı veya fiziki varlığı bulunmayan kart numarasını" ifade etmesi ve sanığın olayda mail order yöntemiyle Touristica (Atlas

264 Uyap Mevzuat Programı

Turistik) isimli işyerinde First American Bank/ ABD bankasının sonu 5904 ile biten kart bilgilerini 23.08.2005 ve 25.08.2005 tarihlerinde, JP Morgan Chase Bank/ ABD bankasının sonu 2467 ile biten kart bilgilerini 05.09.2005 tarihinde, Citibank/ ABD bankasının sonu 7167 ile biten kart bilgilerini 29.09.2005 tarihinde iki kez kullandığının anlaşılması karşısında; Bankalar Arası Kart Merkezinden, bilgileri kullanılan suça konu kartların gerçek olup olmadığı, gerçek olması halinde bu hesaplara ilişkin kredi kartlarının kaç gerçek kişiye ait olduğu sorularak, kredi kartlarının gerçek kişilere ait olması halinde eylemin 5237 sayılı T.C.K.'nun 245/1. maddesindeki suçun ikisi kendi içinde teselsül eden kart sahibi gerçek kişi sayısınca oluşacağı, gerçek kişilerin hesaplarıyla ilişkilendirilerek üretilen sahte kartların olması halinde ise anılan yasanın 245/3. maddesindeki suçun ikisi kendi içinde teselsül eden banka sayısınca oluşacağı gözetilmeden eksik araştırma ile yazılı şekilde hüküm kurulması,"

11. CD., 14.01.2013 T., 2010/12259 E., 2013/554 K.[265]

"A- Sanıklar müdafilerinin banka ve kredi kartlarının kötüye kullanılması suçundan kurulan mahkumiyet hükümlerine yönelik temyiz itirazlarının incelenmesinde;

1-Fikir ve eylem birliği içerisinde hareket eden sanıkların olay günü, Bankalararası Kart Merkezi'nin 29.09.2005 tarihli raporuna göre 4929 **** **** 0000, 4929 **** **** 0008 seri numaralı kartların, gerçekte İngiltere Barclays Bank PLC London United Kingdom isimli yabancı bankaya ait kart bilgilerinin kopyalanması suretiyle sahte oluşturulmuş iki adet kredi kartını POS cihazından geçirerek menfaat sağlamaya teşebbüs etmek eyleminde; Ayrıntıları Ceza Genel Kurulunun 29.05.2001 gün ve 6-106/111 sayılı kararında açıklandığı üzere, çıkardıkları kredi kartları kopyalanarak kullanılan yabancı ve yerli bankalar bu eylemden zarar gördüklerinden suçun mağduru oldukları cihetle; aynı bankaya ait birden fazla kart bilgilerinin kopyalanması durumunda kendi içerisinde zincirleme suçu oluşturacağı gözetilerek, 5237 sayılı T.C.K.'nun 245/3, 43/1, 35/2. maddeleri uyarınca bir hüküm kurulması gerekirken yazılı şekilde iki ayrı hüküm kurulması,…"

265 Uyap Mevzuat Programı

11. CD., 21.01.2013 T., 2010/17400 E., 2013/918 K.[266]

"….Yapılan yargılamaya, toplanıp karar yerinde gösterilen delillere, mahkemenin soruşturma neticelerine uygun şekilde oluşan inanç ve takdirine, incelenen dosya içeriğine göre sanık müdafiinin yerinde görülmeyen sair temyiz itirazlarının reddine; ancak

1-5237 sayılı T.C.K.'nun 245/1. madde ve fıkrasında düzenlenen başkasına ait banka veya kredi kartını kötüye kullanmak suçunun mağduru hesap sahibi olan gerçek ya da tüzel kişiler olduğu cihetle, aynı kişiye ait fakat farklı bankalarca tahsis edilmiş banka veya kredi kartı sayısı nedeniyle ayrı suçlardan bahsedilemeyeceği, aynı kişiye ait farklı bankalarca tahsis edilmiş birden fazla banka veya kredi kartının değişik tarihlerde kullanılması halinde zincirleme suç hükümlerinin uygulanması gerektiği gözetilmeden, mağdur Osman Varol'a ait iki farklı kredi kartının suçta kullanılması nedeniyle kart sayısınca suç oluştuğu kabul edilerek yazılı şekilde bu mağdura yönelik eylemlerinden dolayı iki ayrı suçtan hüküm kurulması,…"

C. TÜRK CEZA KANUNU'NDA ÖZEL HAYATA VE HAYATIN GİZLİ ALANINA KARŞI SUÇLAR BAŞLIĞINDA DÜZENLENEN BİLİŞİM SUÇU TİPLERİ

a. Haberleşmenin Gizliliğini İhlal Suçu[267]

1. Genel Olarak

Bu suçun oluşumunda önemli olan kişiler arasındaki haberleşmenin hukuka aykırı olarak engellenmiş olmasıdır.

Günümüzde internet üzerinden haberleşme yaygınlaşmıştır. Bu nedenle, çok tabiidir ki, bu suç bilişim sistemleri aracılığıyla da islenebilir. T.C.K.'nın 132. maddesinin 3. fıkrasındaki *"her türlü yayın organı"* ifadesinden, internet de anlaşılmalıdır. Çünkü internet üzerinden neredeyse her türlü yayın yapılabilmektedir.

Madde, 765 Sayılı T.C.K.'da düzenlenen 391. maddenin[268] karşılığıdır. Ancak 765 Sayılı T.C.K.'da, yalnızca, telefon, telgraf veya telsiz iletişimin

266 Uyap Mevzuat Programı

267 T.C.K. madde 132 "[1] Kişiler arasındaki haberleşmenin gizliliğini ihlal eden kimse, bir yıldan üç yıla kadar hapis cezası ile cezalandırılır. Bu gizlilik ihlali haberleşme içeriklerinin kaydı suretiyle gerçekleşirse, verilecek ceza bir kat artırılır

[2] Kişiler arasındaki haberleşme içeriklerini hukuka aykırı olarak ifşa eden kimse, iki yıldan beş yıla kadar hapis cezası ile cezalandırılır.

[3] Kendisiyle yapılan haberleşmelerin içeriğini diğer tarafın rızası olmaksızın hukuka aykırı olarak alenen ifşa eden kişi, bir yıldan üç yıla kadar hapis cezası ile cezalandırılır. (Ek cümle: 2/7/2012-6352/79 md.) İfşa edilen bu verilerin basın ve yayın yoluyla yayımlanması halinde de aynı cezaya hükmolunur.

[4] (Mülga: 2/7/2012-6352/79 md.)"

268 765 Sayılı T.C.K. md 391 –İletişim ve Enerji Nakil Vasıtalarına Karsı Suçlar :

engellenmesi suç olarak düzenlenmişti. İnternet iletişiminin engellenmesi suç olarak düzenlenmemişti. 5237 sayılı Türk Ceza Kanunu ile internet iletişiminin engellenmesi de suç olarak düzenlenmiş ve bu konuda çıkabilecek tartışmaları engellenmiştir.

2. Korunan Hukuksal Değer

Bu suç maddesiyle kişiler arasındaki haberleşme özgürlüğü ve haberleşmenin gizliğinin korunması amaçlanmıştır.[269] Haberleşmenin aile bireyleri arasında gerçekleşmesi halinde de aynı zamanda aile yaşamı da korunan hukuksal değerlerdendir[270].

3. Suçun Maddi Unsurları

3.1. Fail

5237 sayılı T.C.K.'nın 132. maddesinde suçu işleyecek kişi açısından herhangi bir özellik belirtilmediği için suçun faili herkes olabilir.

T.C.K.'nın 137. maddesinin 1. fıkrasına göre failin bazı özellikleri taşıması durumunda suçun cezası ağırlaşır. Başka bir deyişle, bu suçun "kamu görevlisi tarafından ve görevinin verdiği yetki kötüye kullanılmak suretiyle veya belli bir meslek ve sanatın sağladığı kolaylıktan yararlanmak suretiyle" işlenmesi hâlinde, verilecek ceza yarı oranında artırılır.

Tüzel kişilerin sorumluluğu ise, T.C.K.'nın 140. maddesine göre değerlendirilecektir. Maddedeki *"Yukarıdaki maddelerde tanımlanan suçların işlenmesi dolayısıyla tüzel kişiler hakkında bunlara özgü güvenlik tedbirlerine hükmolunur."* hükmü gereğince tüzel kişilere T.C.K.'nın 60. maddesindeki güvenlik tedbirleri uygulanacaktır.

3.2. Mağdur

T.C.K.'nın 132. maddesinde suçun mağduru tüm gerçek kişiler olabilir.

3.3. Suçun Konusu

T.C.K.'nın 132. maddesinin 1. fıkrasında suçun konusu "haberleşme"; T.C.K.'nın 132. maddesinin 2. ve 3. fıkrasında ise haberleşmenin içeriğidir[271].

"(1) Bir kimse, telgraf, telefon veya telsiz makinalarına veya alat ve edevatına veya tellerine zarar verir veya elektrik ceryanlarının dağılmasına sebep olur veya her ne suretle olursa olsun telgraf veya telefon veya telsiz muhaberat ve neşriyatını inkıtaa uğratırsa bir seneden beş seneye kadar hapis cezasıyla cezalandırılır."

269 Karagülmez Ali, s.339

270 Tezcan Durmuş/Erdem Mustafa Ruhan/Önok Rıfat Murat, "Teorik Ve Pratik Ceza Özel Hukuku". 5. Bası, Seçkin Yayınevi, Ankara, 2007, s.457

271 Tezcan Durmuş/Erdem Mustafa Ruhan/Önok Rıfat Murat, s.457

3.4. Hareket

Suçun kayda almak suretiyle işlenmesi: Kayda alma, kişiler arasındaki haberleşmenin sesli ve görüntülü kayıt imkanı olan teyp, kamera vb. kayıt cihazı gibi bir aygıtla kopyalanmasıdır. T.C.K.'nın 132. maddesinin gerekçesinde de *"…….Ancak, bu gizlilik ihlâlinin, haberleşme içeriklerinin yani konuşulanların veya yazılanların kayda alınması suretiyle yapılması, bu suçun nitelikli şekli olarak tanımlanmıştır. Örneğin telefon konuşmalarının ses kayıt cihazıyla kayda alınması hâlinde, suçun bu nitelikli hâli gerçekleşmektedir."* denilmiştir. Bu nedenlerle haberleşmenin kâğıt ve benzeri şekilde not edilmesi kayda alma sayılamaz ve T.C.K.'nın 132. maddesindeki suç kapsamına girmez[272].

Belirli veya belirlenebilir iki veya daha fazla kişinin, başkalarının bilmemeleri gerektiği yönünde haklı bir inanç ve iradeyle hareket ederek, gizliliği sağlamaya özen gösterip, elverişli araçlar (internet, telefon, telsiz, faks, mektup, telgraf, kağıt vb.) ve ortak semboller (söz, yazı, işaret vb.) aracılığıyla paylaştıkları bilgi, düşünce, duygu ve tutumlarının; özel hayata ilişkin olsun ya da olmasın, başka kişi veya kişiler tarafından, özel bir çaba gösterilerek, doğrudan veya dolaylı şekilde (zarfı açılmadan ışığa tutulan mektupta olduğu gibi), okunmak veya dinlenmek suretiyle öğrenilmesi eyleminin 5237 sayılı T.C.K.'nın 132/1-1. cümlesinde; anlaşılabilir olsun ya da olmasın, başkalarının haberleşme içeriklerinin kaydı, yani; yazı, ses, görüntü, özel işaretler gibi ortak sembollerin, başka bir nesne üzerine taşınarak (örneğin; ses veya görüntünün, manyetik bant üzerine, yazının başka bir kağıt, defter vb. nesne üzerine geçirilmesi, kopyasının alınması, elektronik iletinin taşınabilir belleğe veya CD'ye aktarılması gibi işlemlerle) sabitlenmesi eyleminin 5237 sayılı T.C.K.'nın 132/1-2. cümlesinde; başkalarının haberleşme içeriklerinin, ilgilisi veya ilgililerinin rızası dışında ifşa edilmesi, yani; yayılması, açığa vurulması, afişe edilmesi, ilan edilmesi, kamuoyuna duyurulması, özetle; içeriğini öğrenme yetkisi bulunmayan kişi veya kişilerin bilgisine sunulması eyleminin 5237 sayılı T.C.K.'nın 132/2. maddesinde tanımlanan haberleşmenin gizliliğini ihlal suçu kapsamında kalacağı değerlendirilmelidir[273]. Ayrıca bu suçların şikayete tabi suçlar olduğunu da unutmamak gerekir[274].

---

272 Karagülmez Ali, s.340

273 12. CD. 02.10.2012 T., 2012/19742 E., 2012/20412 K. "……eşi tarafından işletilen internet cafede bulunan ana bilgisayardan, görümcesi mağdurenin MSN'de evli bir erkekle cinsel içerikli ikili sohbet görüşmeleri yaptığını fark eden sanığın, elektronik iletileri içerir yazıların dökümünü alıp, katılan mağdurenin arkadaşlık ilişkisi içerisinde olduğunu düşündüğü tanık Murat Bahar'a göndermek suretiyle katılana ait haberleşme içeriklerini ifşa

Suçun kişiler arasındaki haberleşme içeriklerini ifşa etmek şeklinde işlenmesi: T.C.K.'nın 132. maddesinin 2. fıkrasında ayrı olarak düzenlenmiştir. Haberleşme içeriğinin hukuka uygun olarak mı, yoksa hukuka aykırı olarak mı öğrenildiği bu suçun oluşması bakımında önem taşımaz[275].İkinci fıkrada tanımlanan suç, haberleşme içeriklerinin ifşasıyla, yayılmasıyla, yani yetkisiz kişilerce öğrenilmesinin sağlanmasıyla oluşur. Fıkra metninde bu ifşanın hukuka aykırı olması açıkça vurgulanmıştır. Bu bakımdan örneğin kişiler arasındaki telefon konuşmalarına ilişkin kayıtların, savcılık veya mahkemeye verilmesi, duruşmada açık bir şekilde dinlenmesi veya okunması hâlinde, söz konusu suç oluşmayacaktır. Buna karşılık, henüz soruşturma aşamasında iken, kişiler arasındaki konuşma içeriklerinin, hukuka uygun bir şekilde kayda alınmış olsalar bile, örneğin televizyonlarda veya gazetelerde yayınlanması hâlinde, bu suç oluşacaktır[276].

Taraflardan birisinin haberleşme içeriğini alenen ifşa etmesi: T.C.K.'nın 132. maddesinin 3. fıkrasında düzenlenmiştir. Maddenin üçüncü fıkrasında, kişinin kendisiyle yapılan haberleşmelerin içeriğini diğer tarafın rızası olmaksızın alenen ifşa etmek suretiyle haberleşmenin gizliliğini ihlâl etmesi ayrı bir suç olarak tanımlanmıştır.Bu suçun oluşabilmesi için, ifşanın alenen yapılması gerekir. Bu bakımdan, örneğin kişi kendisine gönderilen mektubu gönderenin bilgisi ve rızası dışında bir başkasına okutması hâlinde, bu suç oluşmayacaktır. Buna karşılık, mektubun gönderenin bilgisi ve rızası dışında alenen okunması, başkaları tarafından okunmasını temin için bir yere asılması veya basın ve yayın yolu ile yayınlanması hâlinde, söz konusu suç oluşacaktır[277]. Bu husus taraflar arasındaki konuşmanın kayda alınmasında da geçerlidir.

---

ettiğinin iddia edilmesi karşısında, kanıtlanması halinde eylemin, 5237 sayılı T.C.K.'nın 132/1 ve aynı Kanunun 132/2. maddesinde tanımlanan haberleşmenin gizliliğini ihlal suçunu oluşturacağı" - 12. CD. 12.06.2012 T., 2012/13428 E., 2012/14792 K. "……eşi olan katılanın sadakatinden kuşkulanan ve aldatıldığını düşünen sanığın, katılan tarafından kullanılmakta olan aracın oto koltuğuna, onun bilgisi ve rızası dışında, ses kayıt cihazı yerleştirerek, katılanın başka kişilerle yaptığı telefon görüşmelerini kaydettiğinin iddia edilmesi karşısında, kanıtlanması halinde eylemin, 5237 sayılı T.C.K.'nın 132/1-2. cümlesinde tanımlanan haberleşmenin gizliliğini ihlal suçunu oluşturacağı…" Uyap Mevzuat Programı

274 12. CD. 01.07.2013 T., 2013/9548 E., 2013/17899 K. "……sanığın, katılanın doğrudan internet adresleri üzerinden gerçekleştirdiği ikili sohbet görüşmelerine ilişkin elektronik iletileri içerir yazılarını, birlikte kullandıkları bilgisayara yüklediği casus program aracılığıyla ele geçirip, onun bilgisi ve rızası dışında, aralarında görülmekte olan boşanma davası dosyasına 07.12.2009 tarihinde metin halinde sunduğu iddiasına konu olayda, 5237 sayılı T.C.K.'nın 132. maddesinde düzenlenen haberleşmenin gizliliğini ihlal suçunun, aynı Kanunun 139/1. maddesi uyarınca soruşturulması ve kovuşturulmasının şikayete bağlı olduğu,……" Uyap Mevzuat Programı

275 Soyaslan, Doğan, Ceza Hukuku Özel Hükümler, 5. Baskı, Ankara, Yetkin Basımevi, 2005, s.269

276 T.C.K. madde 132 gerekçesi

277 T.C.K. madde 132 gerekçesi

3.5. Netice

T.C.K.'nın 132. maddesinin 1. fıkrasında zararın meydana gelmesi aranmaz. T.C.K.'nın 132. maddesinin 2. ve 3. fıkralarında yer alan ifşa eylemi ile ise zarar oluşacaktır.

4. Suçun Manevi Unsurları

Bu suç ancak kasten işlenebilir. Bu kast genel kasttır, kanun suçun oluşumu için özel kast aramamıştır.

Bu suçun kasten işlenmesi arandığından taksirle işlenemez.

5. Hukuka Aykırılık

Haberleşme gizliliğine yönelik müdahalenin suç teşkil edebilmesi için herhangi bir hak ve yetkiye dayanmaması gerekir. Bu nedenle T.C.K.'nın 26. maddesinin 1. fıkrasındaki hakkın kullanılması suçun oluşumunu engelleyecektir. Gazetecilik mesleğini yaparken hakkın kullanılması bu suçta hukuka aykırılığı kaldırır[278].

Bunun dışında kanunun verdiği bir yetkinin kullanılması da (T.C.K. madde 24) suçta hukuka aykırılığı ortadan kaldırır. C.M.K.'nın 126. maddesinde düzenlenen elkoyma gene C.M.K.'nın 135 ve devamı maddelerinde düzenlenen iletişimin denetlenmesi hukuka aykırılığı ortadan kaldırır.

Bu suçta meşru savunma da hukuka aykırılığı ortadan kaldırabilir. Örneğin telefonla tehdit eden kişinin sesinin kaydedilmesi meşru savunma olarak kabul edilir ve ceza verilmez[279].

6. Suçun Özel Görünüş Şekilleri

6.1. Teşebbüs

Bu suç salt hareket suçu olduğu için ancak icra hareketleri bölünebiliyorsa teşebbüs mümkün olacaktır[280].

6.2. İştirak

T.C.K. 132. maddesinde yer alan *"Haberleşmenin gizliliğini ihlal"* suçlarının iştirak açısından bir özellik söz konusu olmayıp, genel hükümler uygulanacaktır. Genel hükümler değerlendirildiğinde bu suç tipleri için iştirak türlerinin gerçekleşmesi mümkündür[281].

278 Tezcan Durmuş/Erdem Mustafa Ruhan/Önok Rıfat Murat,s.461

279 Tezcan Durmuş/Erdem Mustafa Ruhan/Önok Rıfat Murat,s.466

280 Tezcan Durmuş/Erdem Mustafa Ruhan/Önok Rıfat Murat,s.462

281 Akbulut Berrin, s.,213; Dülger Murat Volkan, s.205; Yazicioğlu Yılmaz, s.286

6.3. İçtima

Haberleşmenin gizliliğini ihlal suçu her defasında aynı kişiye yani aynı mağdura karşı işleniyorsa zincirleme suç hükümleri uygulanır.

Haberleşme içeriğinin ifşa edilmesi aynı zamanda hakaret suçu oluşturuyorsa T.C.K.'nın 132. maddesinin 2. ve 3. fıkraları ile T.C.K.'nın 125. maddesinde düzenlenen hakaret suçu arasında fikri içtima kurallarının uygulanması yoluna gidilmelidir. Bunun gibi ifşa etmekle çıkar sağlayacak olursa ayrıca T.C.K.'nın 107. maddesinde düzenlenen şantaj suçu da oluşabilir[282].

7. Suça Etki Eden Sebepler

T.C.K. 137. maddesine göre, failin bazı özellikleri taşıması durumunda suçun cezası ağırlaşır. Başka bir deyişle, bu suçun "kamu görevlisi tarafından ve görevinin verdiği yetki kötüye kullanılmak suretiyle veya belli bir meslek ve sanatın sağladığı kolaylıktan yararlanmak suretiyle" işlenmesi hâlinde, verilecek ceza yarı oranında artırılır.

T.C.K.'nın 132. maddesinin 4. fıkrasında bulunan haberleşme içeriğinin basın ve yayın yolu ile yayınlanması cezanın ağırlaştırılmasını gerektiren nitelikli hal ise 02.07.2012 Tarihinde Resmi Gazete'de yayımlanan 6352 sayılı Kanunun 79. maddesi ile kaldırılmıştır

8. Kovuşturma, Görevli Mahkeme, Suçun Yaptırımı ve Dava Zamanaşımı

Kovuşturma: Maddede tanımlanan suçun soruşturması ve kovuşturması şikayete bağlıdır.

Görevli Mahkeme: 5235 sayılı Kanun'un 10. maddesi uyarınca maddede tanımlanan suçlara dolayısıyla açılan davalara bakma görevi sulh ceza mahkemesine aittir.

Suçun Yaptırımı: Maddenin birinci fıkrasına göre kişiler arasındaki haberleşmenin gizliliğini ihlal eden kimse, bir yıldan üç yıla kadar hapis cezası ile cezalandırılır. Bu gizlilik ihlali haberleşme içeriklerinin kaydı suretiyle gerçekleşirse, verilecek ceza bir kat artırılır; ikinci fıkraya göre, Kişiler arasındaki haberleşme içeriklerini hukuka aykırı olarak ifşa eden kimse, iki yıldan beş yıla kadar hapis cezası ile cezalandırılır; üçüncü fıkraya göre, kendisiyle yapılan haberleşmelerin içeriğini diğer tarafın rızası olmaksızın hukuka aykırı olarak alenen ifşa eden kişi, bir yıldan üç yıla kadar hapis cezası ile cezalandırılır.

282 Tezcan Durmuş/Erdem Mustafa Ruhan/Önok Rıfat Murat,s.462

Dava Zamanaşımı: T.C.K.'nın 66/1-e maddesi uyarınca bu suçların dava zamanaşımı süresi 8 yıldır.

b. Kişiler Arasındaki Konuşmaların Dinlenmesi Ve Kayda Alınması Suçu[283]

1. Genel Olarak

T.C.K.'nın 133. maddesi kişiler arasındaki aleni olmayan konuşmaların dinlenmesi ve kayda alınmasını suç olarak düzenlemiştir. Bu nedenle, konuşmaların değil de görüntülerin kayda alınması durumunda madde 133 değil madde 134'teki özel hayatın gizliliği söz konusu olacaktır[284].

2. Korunan Hukuksal Değer

Bu suç maddesiyle haberleşme özgürlüğünden çok, özel hayatın gizliliği korunmaktadır[285].

3. Suçun Maddi Unsurları

3.1. Fail

5237 sayılı T.C.K.'nın 133. maddesinin 1. fıkrasında öngörülen suçun faili aleni olmayan konuşmanın tarafı olmayan herhangi bir kişidir. Buna karşılık T.C.K.'nın 133. maddesinin 2. fıkrasındaki suçun oluşması için ise failin söyleşiye katılmış olması şartı aranmaktadır.

T.C.K.'nın 137. maddesinin 1. fıkrasına göre failin bazı özellikleri taşıması durumunda suçun cezası ağırlaşır. Başka bir deyişle, bu suçun "kamu görevlisi tarafından ve görevinin verdiği yetki kötüye kullanılmak suretiyle veya belli bir meslek ve sanatın sağladığı kolaylıktan yararlanmak suretiyle" işlenmesi hâlinde, verilecek ceza yarı oranında artırılır.

Tüzel kişilerin sorumluluğu ise, T.C.K.'nın 140. maddesine göre değerlendirilecektir. Maddedeki *"Yukarıdaki maddelerde tanımlanan suçların işlenmesi dolayısıyla tüzel kişiler hakkında bunlara özgü güvenlik tedbirlerine*

---

283 T.C.K. madde 133 "[1] Kişiler arasındaki aleni olmayan konuşmaları, taraflardan herhangi birinin rızası olmaksızın bir aletle dinleyen veya bunları bir ses alma cihazı ile kaydeden kişi, iki yıldan beş yıla kadar hapis cezası ile cezalandırılır.

[2] Katıldığı aleni olmayan bir söyleşiyi, diğer konuşanların rızası olmadan ses alma cihazı ile kayda alan kişi, altı aydan iki yıla kadar hapis veya adlî para cezası ile cezalandırılır.

[3] (Değişik: 2/7/2012-6352/80 md.) Kişiler arasındaki aleni olmayan konuşmaların kaydedilmesi suretiyle elde edilen verileri hukuka aykırı olarak ifşa eden kişi, iki yıldan beş yıla kadar hapis ve dörtbin güne kadar adlî para cezası ile cezalandırılır. İfşa edilen bu verilerin basın ve yayın yoluyla yayımlanması halinde de aynı cezaya hükmolunur."

284 Tezcan Durmuş/Erdem Mustafa Ruhan/Önok Rıfat Murat,s.462; Karagülmez Ali, s.342

285 Tezcan Durmuş/Erdem Mustafa Ruhan/Önok Rıfat Murat,s.463

hükmolunur." hükmü gereğince tüzel kişilere T.C.K.'nın 60. maddesindeki güvenlik tedbirleri uygulanacaktır.

3.2. Mağdur

T.C.K.'nın 133. maddesindeki suçun mağduru da tüm gerçek kişiler olabilir.

3.3. Suçun Konusu

Bu suçun maddi konusu, T.C.K.'nın 133. maddesinin 1. fıkrası açısından kişiler arası aleni olmayan konuşma, madde T.C.K.'nın 133. maddesinin 2. fıkrası açısından aleni olmayan söyleşidir.

Daha önce de belirttiğimiz üzere, konuşmaların değil de görüntülerin kayda alınması durumunda madde 133 değil madde 134'teki özel hayatın gizliliği söz konusu olacaktır[286].

3.4. Hareket

Kişiler arasındaki aleni olmayan konuşmaları aletle dinleme veya ses alma cihazı ile kaydetme eylemi: T.C.K.'nın 133. maddesinin 1. fıkrasında düzenlenmiştir. Yapılan konuşma iki veya daha fazla kişi arasında gerçekleşir. Bir arada bulunan kişiler arasında yapılan konuşmanın aleni olmayan konuşma olarak kabulü için konuşmanın yapıldığı yerin önemi yoktur. Bu bakımdan, örneğin bir parkta iki kişi arasında geçen konuşmanın başkaları tarafından ancak özel gayret gösterilerek duyulabilecek olması hâlinde, aleni olmayan konuşma söz konusudur. Keza, örneğin bir evde sınırlı sayıda kişiler arasında yapılan konuşma, aleni olmayan bir konuşmadır[287].

Katıldığı aleni olmayan bir söyleşiyi, ses alma cihazı ile kaydetme: T.C.K.'nın 133. maddesinin 2. fıkrasında düzenlenmiştir. Burada konuşma değil, söyleşi kavramı kullanılmıştır. Madde gerekçesinde "Maddenin ikinci fıkrasında, kişiler arasındaki aleni olmayan konuşmaların, söyleşiye katılan kişilerden biri tarafından diğerlerinin rızası olmadan kayda alınması, suç olarak tanımlanmıştır" denilmiştir.

T.C.K.'nın 133. maddesinin 3. fıkrasında ise 1. ve 2. fıkralarında düzenlenen eylemlerin nitelikli halleri düzenlenmiştir. Bu hususa suça etki eden sebepler başlığı altında değineceğiz.

286 Tezcan Durmuş/Erdem Mustafa Ruhan/Önok Rıfat Murat,s.462; Karagülmez Ali, s.342

287 Madde gerekçesinden

3.5. Netice

T.C.K.'nın 133. maddesinin 1. ve 2. fıkrasında zararın meydana gelmesi aranmaz. Kaydetmenin yapıldığı anda suç oluşur. Kayıt etme fiilinin aleniyete dökülüp dökülmemesinin bu suçun oluşumuna bir etkisi yoktur. T.C.K.'nın 133. maddesinin 3. fıkrasında yer alan ifşa eylemi ile ise zarar oluşacaktır.

4. Suçun Manevi Unsurları

Bu suç ancak kasten işlenebilir. Bu kast genel kasttır, kanun suçun oluşumu için özel kast aramamıştır.

Bu suçun kasten işlenmesi arandığından taksirle işlenemez.

5. Hukuka Aykırılık

T.C.K.'nın 133. maddesinin suç teşkil edebilmesi için failin herhangi bir hak ve yetkiye dayanmaması gerekir. Rıza verilmesi bu suçta hukuka aykırılığı kaldırır. Bir başka deyişle, suçun oluşabilmesi için, konuşmanın taraflarından herhangi birinin rızasının olmaması yeterlidir. Bu bakımdan konuşmanın taraflarından birinin rızasının olması, fiili suç olmaktan çıkarmayacaktır. Örneğin, üç kişinin aleni olmayan bir konuşmasının dinlemesi ve kayda alınmasında iki kişinin rızası olsa bile bir kişinin rızası olmadığı için fiil suç sayılacaktır.

Bunun dışında kanunun verdiği bir yetkinin kullanılması da (T.C.K. madde 24) suçta hukuka aykırılığı ortadan kaldırır. C.M.K.'nın 135 ve devamı maddelerinde düzenlenen iletişimin denetlenmesi hukuka aykırılığı ortadan kaldırır. Bazı durumlarda da yapılan bu eylem meşru savunma kapsamında değerlendirilebilir[288].

6. Suçun Özel Görünüş Şekilleri

6.1. Teşebbüs

Bu suç salt hareket suçu olduğu için ancak icra hareketleri bölünebiliyorsa teşebbüs mümkün olacaktır[289].

6.2. İştirak

5237 sayılı T.C.K.'nın 133. maddesinin 1. fıkrasında öngörülen suçun faili aleni olmayan konuşmanın tarafı olmayan herhangi bir kişidir. Buna karşılık T.C.K.'nın 133. maddesinin 2. fıkrasında suçun oluşması için ise failin söyleşiye

288 12. CD. 26.03.2012 T., 2011/13850 E., 2012/8229 K "…Sanığın kendisini arayıp hakaret ve tehditte bulunan katılanın konuşmalarını telefonuna kaydetmekten ibaret eyleminde, T.C.K.'nın 133/1 ve 133/2. maddesindeki suçların yasal unsurlarının gerçekleşmediği gözetilmeksizin mahkemece sanığın beraati yerine mahkumiyetine karar verilmesi,.." Uyap Mevzuat Programı

289 Tezcan Durmuş/Erdem Mustafa Ruhan/Önok Rıfat Murat,s.462

katılmış olması şartı aranmaktadır. Görüldüğü üzere özgü suç niteliği vardır ve suçun işlenişine katılan diğer kişiler azmettiren ya da yardım eden olarak cezalandırılır[290].

6.3. İçtima

Kişiler arasındaki konuşmaların dinlenmesi ve kayda alınması suçu her defasında aynı kişiye aynı mağdura karşı işleniyorsa zincirleme suç hükümleri uygulanır.

Telefonla yapılan görüşmelerin kayda alınması bakımından T.C.K.'nın 132. maddesi ile 133. maddesinden hangisinin uygulanacağı konusu akla gelebilir. T.C.K.'nın 132 maddesi haberleşme araçları bakımında özel bir düzenleme içerdiği için öncelikle bu maddenin uygulanması daha doğru olur kanaatindeyiz. T.C.K. 133 yüz yüze olan konuşmalar açısından söz konusudur[291].

7. Suça Etki Eden Sebepler

T.C.K.'nın 137. maddesine göre, failin bazı özellikleri taşıması durumunda suçun cezası ağırlaşır. Başka bir deyişle, bu suçun "kamu görevlisi tarafından ve görevinin verdiği yetki kötüye kullanılmak suretiyle veya belli bir meslek ve sanatın sağladığı kolaylıktan yararlanmak suretiyle" işlenmesi hâlinde, verilecek ceza yarı oranında artırılır.

T.C.K.'nın 133. maddesinin 3. fıkrasına göre ise kişiler arasındaki aleni olmayan konuşmaların kaydedilmesi suretiyle elde edilen verileri hukuka aykırı olarak ifşa eden kişi, iki yıldan beş yıla kadar hapis ve dörtbin güne kadar adlî para cezası ile cezalandırılır. İfşa edilen bu verilerin basın ve yayın yoluyla yayımlanması halinde de aynı cezaya hükmolunur.

8. Kovuşturma, Görevli Mahkeme, Suçun Yaptırımı ve Dava Zamanaşımı

Kovuşturma: Maddede tanımlanan suçun soruşturması ve kovuşturması şikayete bağlıdır.

Görevli Mahkeme: 5235 sayılı Kanun'un 10. maddesi uyarınca T.C.K. 133/1' göre açılan davalara bakma görevi sulh ceza mahkemesine, T.C.K. 133/2-3'e göre açılan davalara bakma görevi asliye ceza mahkemesine aittir.

Suçun Yaptırımı: Maddenin birinci fıkrasına göre Kişiler arasındaki aleni olmayan konuşmaları, taraflardan herhangi birinin rızası olmaksızın bir aletle

290 Tezcan Durmuş/Erdem Mustafa Ruhan/Önok Rıfat Murat,s.466

291 Tezcan Durmuş/Erdem Mustafa Ruhan/Önok Rıfat Murat,s.466

dinleyen veya bunları bir ses alma cihazı ile kaydeden kişi, iki yıldan beş yıla kadar hapis cezası ile cezalandırılır; ikinci fıkraya göre, Katıldığı aleni olmayan bir söyleşiyi, diğer konuşanların rızası olmadan ses alma cihazı ile kayda alan kişi, altı aydan iki yıla kadar hapis veya adlî para cezası ile cezalandırılır; üçüncü fıkraya göre, Kişiler arasındaki aleni olmayan konuşmaların kaydedilmesi suretiyle elde edilen verileri hukuka aykırı olarak ifşa eden kişi, iki yıldan beş yıla kadar hapis ve dörtbin güne kadar adlî para cezası ile cezalandırılır. İfşa edilen bu verilerin basın ve yayın yoluyla yayımlanması halinde de aynı cezaya hükmolunur..

Dava Zamanaşımı: T.C.K.'nın 66/1-e maddesi uyarınca bu suçların dava zamanaşımı süresi 8 yıldır.

c. Özel Hayatın Gizliliğini İhlal Suçu[292]

1. Genel Olarak

T.C.K.'nın 134. maddesi 765 sayılı kanunda olmayan yeni bir düzenlemedir. Şimdi bu suçu incelemeye başlayalım.

2. Korunan Hukuksal Değer

Bu suç maddesiyle özel hayatın gizliliği korunmaktadır[293]. Anayasanın 20. maddesinde düzenlenen kişinin özel hayatına ve aile hayatının gizliliğini korumayı amaçlayan ceza hukukundaki düzenlemedir.

3. Suçun Maddi Unsurları

3.1. Fail

5237 sayılı T.C.K.'nın 134. maddesinde düzenlenen suçun faili herhangi bir kişi olabilir. T.C.K. 137/1 fıkrasına göre failin bazı özellikleri taşıması durumunda suçun cezası ağırlaşır. Başka bir deyişle, bu suçun "kamu görevlisi tarafından ve görevinin verdiği yetki kötüye kullanılmak suretiyle veya belli bir meslek ve sanatın sağladığı kolaylıktan yararlanmak suretiyle" işlenmesi hâlinde, verilecek ceza yarı oranında artırılır.

Tüzel kişilerin sorumluluğu ise, T.C.K.'nın 140. maddesine değerlendirilecektir. Maddedeki *"Yukarıdaki maddelerde tanımlanan suçların işlenmesi dolayısıyla tüzel kişiler hakkında bunlara özgü güvenlik tedbirlerine*

---

292 T.C.K. madde 134 : "[1] Kişilerin özel hayatının gizliliğini ihlal eden kimse, bir yıldan üç yıla kadar hapis cezası ile cezalandırılır. Gizliliğin görüntü veya seslerin kayda alınması suretiyle ihlal edilmesi halinde, verilecek ceza bir kat artırılır. (Asliye Ceza)

[2] (Değişik: 2/7/2012-6352/81 md.) Kişilerin özel hayatına ilişkin görüntü veya sesleri hukuka aykırı olarak ifşa eden kimse iki yıldan beş yıla kadar hapis cezası ile cezalandırılır. İfşa edilen bu verilerin basın ve yayın yoluyla yayımlanması halinde de aynı cezaya hükmolunur."

293 Tezcan Durmuş/Erdem Mustafa Ruhan/Önok Rıfat Murat,s.463

hükmolunur." hükmü gereğince tüzel kişilere T.C.K.'nın 60. maddesindeki güvenlik tedbirleri uygulanacaktır.

3.2. Mağdur

T.C.K. madde 134'deki suçun mağduru da tüm gerçek kişiler olabilir.

3.3. Suçun Konusu

Bu suçun maddi konusu, kişinin somut olarak özel yaşamıdır.

3.4. Hareket

T.C.K.'nın 134. maddesinin 1. fıkrasında özel hayatın gizliliğinin ihlâli suç olarak tanımlanmaktadır. Böylece, gizli yaşam alanına girerek veya başka suretle başkaları tarafından görülmesi mümkün olmayan bir özel yaşam olayının saptanması ve kaydedilmesi cezalandırılmaktadır. Burada cezalandırılan eylem T.C.K.'nın 132. ve 133. maddelerinde belirtilen eylemlerin dışında kalan eylemlerdir.

Bu suçun daha iyi anlaşılması için özel hayat kavramının açıklanması gerekir

Soyut yaklaşıma göre özel hayat, herkes için özel hayat olarak nitelenebilecek alanlardır. Konumu ne olursa olsun kişinin evinde veya dışarıda paylaşmak istemediği zaman dilimi özel hayattır. Somut yaklaşıma göre özel hayat, özel hayat belirlenirken mağdurun konumu ile olayın özelliklerinin dikkate alınması gerekir. Mağdurun konumuna göre, orta halli birisi için suç sayılan bir sonuç, toplum tarafından tanınan, şöhret olmuş vb. durumlardan göz önünde bulunan birisi için özel hayat olarak nitelenmeyebilir[294].

T.C.K.'nın 134. maddesinin 2. fıkrasında, özel hayata ilişkin elde edilen saptama ve kayıtlardan herhangi bir suretle yarar sağlanması veya bunların başkalarına verilmesi veya diğer kimselerin bilgi edinmelerinin temini veya basın ve yayın yoluyla açıklanması suçun ağırlaşmış şeklini oluşturmaktadır. İkinci fıkra ile kişinin özel hayatına ilişkin görüntü veya seslerin hukuka aykırı olarak ifşa edilmesi, ayrı bir suç olarak tanımlanmıştır. Bu görüntü veya sesler örneğin soruşturma kapsamında hukuka uygun bir şekilde kayda alınmış olabileceği gibi, birinci fıkrada tanımlanan suçun işlenmesi suretiyle elde edilmiş olabilir. İkinci fıkrada tanımlanan suç, elde edilmiş olan bu ses veya görüntü kayıtlarının ifşasıyla, yayılmasıyla, yani yetkisiz kişilerce öğrenilmesinin sağlanmasıyla oluşur[295]. Bu ifşanın hukuka aykırı

294 Karagülmez Ali, s.347

295 12. CD. 12.06.2012 T., 2011/21801 E., 2012/14797 K. "…….dosya içeriğine göre; sanığın, bir arkadaşlık sitesine giriş yaparak, kendisinin bayan olduğunu belirtip, katılanla internet ortamında tanıştığı, katılanla samimiyet kurup, doğrudan internet adresleri üzerinden, MSN tabir edilen ve direk görüşme imkanı sağlayan program aracılığıyla sohbete başladığı, bir bilgisayar programından yararlanarak, bilgisayarında kayıtlı başka bir kadının soyunma

olması gerekir. Bu bakımdan özel hayata ilişkin kayıtların, savcılık veya mahkemeye verilmesi, duruşmada gösterilmesi ve dinlenmesi hâlinde, söz konusu suç oluşmayacaktır.

İfşanın, basın ve yayın yoluyla yapılması, söz konusu suçun nitelikli unsuru olarak kabul edilmiştir.

Ayrıca, bu suçun şikayete bağlı bir suç olduğu unutulmamalıdır[296].

3.5. Netice

T.C.K.'nın 134.cmaddesinin 1. fıkrasında zararın meydana gelmesi aranmaz. Kaydetmenin yapıldığı anda suç oluşur. Kayıt etme fiilinin aleniyete dökülüp dökülmemesinin bu suçun oluşumuna bir etkisi yoktur. T.C.K.'nın 134. maddesinin 2. fıkrasında yer alan ifşa eylemi ile ise zarar oluşacaktır.

4. Suçun Manevi Unsurları

Bu suç ancak kasten işlenebilir. Bu kast genel kasttır, kanun suçun oluşumu için özel kast aramamıştır.

Bu suçun kasten işlenmesi arandığından taksirle işlenemez.

5. Hukuka Aykırılık

T.C.K.'nın 134. maddesinin suç teşkil edebilmesi için failin herhangi bir hak ve yetkiye dayanmaması gerekir. Rıza verilmesi bu suçta hukuka aykırılığı kaldırır. Bir başka deyişle, özel yaşama ilgililerin rızasına dayanarak müdahalede bulunan kişi bu suçu işlemiş olmaz. Bunun dışında kanunun verdiği bir yetkinin kullanılması da (T.C.K. madde 24) suçta hukuka aykırılığı ortadan kaldırır. C.M.K.'nın 126. maddesinde düzenlenen el koyma, aynı kanunun 139. maddesinde

---

görüntülerini kendisiymiş gibi tavır takınıp, katılana izlettirerek, katılanın da kendisini rahat hissetmesini sağladığı ve onun da görüntüdeki kadın gibi soyunmasını istediği, katılanın web kamerasını açıp, soyunduktan sonra, cinsel bölgelerine dokunmasına ilişkin görüntülerini gizlice kaydettiği, devam eden günlerde görüştüğü kişinin erkek olduğunu fark eden katılandan soyunma şovuna devam etmesini istediği, ancak katılanın kabul etmemesi üzerine, kaydettiği görüntülerini internet ortamında yayacağını söylediği, katılanın göğüs ve kalça kısımlarının göründüğü 4 parçadan ibaret resmi, kendi oluşturduğu bir blog adresinde yayınlayıp, katılana "bak bakalım ilk adımı beğendim mi?" şeklinde ileti gönderip, katılanın bu resimleri görmesini sağladıktan sonra, resimleri sayfasından kaldırdığı olayda; temyiz incelemesine konu eylemle sınırlı olarak yapılan incelemede, katılanın fiziksel mahremiyetini içerir, özel hayatına ilişkin resimlerinin, ifşa iddiasına konu edilmesi ve görüntünün yasal olarak kişisel veri kapsamında düzenlenmemiş olması karşısında, sanığa atılı verileri hukuka aykırı olarak verme veya ele geçirme suçun unsurları itibariyle oluşmadığı; ancak eylemin 5237 sayılı T.C.K.'nın 134/2. maddesinde tanımlanan özel hayatın gizliliğini ihlal suçunu oluşturduğu ve sanığın bu suçtan mahkumiyetine karar verilmesi gerektiği gözetilmeden, yasal ve yeterli olmayan gerekçelerle yazılı şekilde, sanık hakkında beraat kararı verilmesi," - Uyap Mevzuat Programı

296 12. CD., 02.10.2012 T., 2012/19106 E., 2012/20403 K.Dosya içeriğine göre, katılan sanığın, mağdurenin özel hayat kapsamındaki görüntülerini bilgisi dahilinde, kamera sistemi çalışır taşınabilir telefonuyla kayıt edip, elde ettiği görüntüleri, mağdureden habersiz ve onun rızası olmaksızın, bluetooth sistemi aracılığıyla başka kişilerin cep telefonuna göndermek ve internette bir video paylaşım sitesine koymak suretiyle özel hayatına ilişkin görüntülerinin yayılmasına sebebiyet verdiği olayda, yapılan yargılama sonucu, 5237 sayılı T.C.K.'nın 134/2. maddesinde düzenlenen özel hayatın gizliliğini ihlal suçu sabit görülerek sanığın mahkumiyetine karar verilmiş ise de, anılan suçun aynı Kanunun 139/1. maddesi uyarınca soruşturulması ve kovuşturulması şikayete bağlı olup, mağdurenin aşamalarda sanıktan şikayetçi olmadığını belirtmiş bulunması karşısında, sanık hakkında açılan kamu davasının şikayet yokluğu nedeniyle 5237 sayılı T.C.K.'nın 139/1, 73/1 ve 5271 sayılı C.M.K.'nın 223/8. maddeleri uyarınca düşmesine karar verilmesi gerektiği gözetilmeden, yazılı şekilde hüküm kurulması, - Uyap Mevzuat Programı

düzenlenen gizli soruşturma görevlendirilmesi ve 140. maddesinde düzenlenen teknik araçlarla izleme durumları suçun hukuka aykırılık unsurunu ortadan kaldırır.

Hakkın kullanılması durumu olan gazetecilik mesleğinin icrası çerçevesindeki eylemler bakımından da hukuka uygunluk sebebi vardır[297].

6. Suçun Özel Görünüş Şekilleri

6.1. Teşebbüs

Bu suç salt hareket suçu olduğu için ancak icra hareketleri bölünebiliyorsa teşebbüs mümkün olacaktır[298].

6.2. İştirak

5237 sayılı T.C.K.'daki madde 134'te düzenlenen özel hayatın gizliliği suçu iştirak açısından bir özellik söz konusu olmayıp, genel hükümler uygulanacaktır. Genel hükümler değerlendirildiğinde bu suç tipleri için iştirak türlerinin gerçekleşmesi mümkündür

6.3. İçtima

Görüntü veya seslerin kayda alan ve ifşa eden kişi aynı fail ise faile hem T.C.K.'nın 134. maddesinin 1. fıkrasından hem de 134. maddesinin 2. fıkrasından ayrı ayrı ceza verilmesi gerektiğini düşünmekteyiz. Aksi taktirde, görüntü ve sesi yalnızca kaydeden kişinin ifşa eden kişiden daha fazla ceza alması durumu gerçekleşebilir.

Özel hayatın gizliliği suçu her defasında aynı kişiye aynı mağdura karşı işleniyorsa zincirleme suç hükümleri uygulanır.

Ses ve görüntülerin ifşa edilmesi ayrıca hakaret suçunu da oluşturuyorsa fikri içtima kuralları çerçevesinde T.C.K.'nın 134. maddesinin 2. fıkrası ile 125. maddesi arasında fikri içtima kuralları uygulanmalıdır. Ayrıca, ifşa etme tehdit ile haksız bir çıkar da sağlanacak olursa T.C.K. 148. maddesinde düzenlenen yağma ve T.C.K. 107. maddesinde düzenlenen şantaj suçundan da cezalandırma yapılabilecektir[299].

7. Suça Etki Eden Sebepler

T.C.K.'nın 137. maddesine göre, failin bazı özellikleri taşıması durumunda suçun cezası ağırlaşır. Başka bir deyişle, bu suçun "kamu görevlisi tarafından ve görevinin verdiği yetki kötüye kullanılmak suretiyle veya belli bir meslek ve sanatın

297 Tezcan Durmuş/Erdem Mustafa Ruhan/Önok Rıfat Murat,s.469

298 Tezcan Durmuş/Erdem Mustafa Ruhan/Önok Rıfat Murat,s.469

299 Tezcan Durmuş/Erdem Mustafa Ruhan/Önok Rıfat Murat,s.470

sağladığı kolaylıktan yararlanmak suretiyle" işlenmesi hâlinde, verilecek ceza yarı oranında artırılır.

T.C.K. madde T.C.K.'nın 134. maddesinin 2. fıkrasının ikinci cümlesinde suçun basın ve yayın dolayısıyla işlenmesi cezanın ağırlaştırılmasını gerektiren nitelikli bir hal olarak öngörülmüştür.

8. Kovuşturma, Görevli Mahkeme, Suçun Yaptırımı ve Dava Zamanaşımı

Kovuşturma: Maddede tanımlanan suçun soruşturması ve kovuşturması şikayete bağlıdır.

Görevli Mahkeme: 5235 sayılı Kanun'un 10. maddesi uyarınca T.C.K.'nın 134. maddesine göre açılan davalara bakma görevi asliye ceza mahkemesine aittir.

Suçun Yaptırımı: Maddenin birinci fıkrasına göre kişilerin özel hayatının gizliliğini ihlal eden kimse, bir yıldan üç yıla kadar hapis cezası ile cezalandırılır. Gizliliğin görüntü veya seslerin kayda alınması suretiyle ihlal edilmesi halinde, verilecek ceza bir kat artırılır; ikinci fıkraya göre, kişilerin özel hayatına ilişkin görüntü veya sesleri hukuka aykırı olarak ifşa eden kimse iki yıldan beş yıla kadar hapis cezası ile cezalandırılır. İfşa edilen bu verilerin basın ve yayın yoluyla yayımlanması halinde de aynı cezaya hükmolunur.

Dava Zamanaşımı: T.C.K.'nın 66/1-e maddesi uyarınca bu suçların dava zamanaşımı süresi 8 yıldır.

d. Kişisel Verilerin Kaydedilmesi Suçu

1. Genel Olarak

T.C.K.'nın 135. maddesinin gerekçesinde de belirtildiği üzere, bu düzenleme ile Türkiye'nin tarafı olduğu "Kişisel Nitelikteki Verilerin Otomatik İşleme Tabi Tutulması Karsısında Şahısların Korunmasına Dair Sözleşme"nin ilgili düzenlemeleri ülkemiz hukuku açısından geçerlilik tanınmıştır.

T.C.K. 135. madde: *(Değişik: 21/2/2014 – 6526/3 md.)Hukuka aykırı olarak kişisel verileri kaydeden kimseye bir yıldan üç yıla kadar hapis cezası verilir. [2] Kişilerin siyasî, felsefî veya dinî görüşlerine, ırkî kökenlerine; hukuka aykırı olarak ahlâkî eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin bilgileri kişisel veri olarak kaydeden kimse, yukarıdaki fıkra hükmüne göre cezalandırılır.*

Görüldüğü üzere kanun maddesi çok yakın bir tarihte değişikliğe uğramıştır. Değişiklikle ceza miktarının alt sınırı artırılmıştır[300].

2. Korunan Hukuksal Değer

Kişisel verilerin kaydedilmesi suçunda korunan hukuksal değer, genel olarak kişilerin özel hayatının dokunulmazlığıdır.

3. Suçun Maddi Unsurları

3.1. Fail

5237 sayılı T.C.K.'nın 135. maddesinde suçu işleyecek kişi açısından herhangi bir özellik belirtilmediği için suçun faili herkes olabilir.

Tüzel kişilerin sorumluluğu ise, T.C.K.'nın 140. maddesine göre değerlendirilecektir. Maddedeki *"Yukarıdaki maddelerde tanımlanan suçların işlenmesi dolayısıyla tüzel kişiler hakkında bunlara özgü güvenlik tedbirlerine hükmolunur."* hükmü gereğince tüzel kişilere T.C.K.'nın 60. maddesindeki güvenlik tedbirleri uygulanacaktır.

3.2. Mağdur

T.C.K. madde 135'teki suçun mağduru da tüm gerçek kişiler olabilir.

3.3. Suçun Konusu

Kişisel verilerin kaydedilmesi suçunun konusunu "kişisel veriler" oluşturmaktadır. Nitekim 135. maddenin gerekçesinde de "Suçun konusu, kişisel verilerdir. Gerçek kişiyle ilgili her türlü bilgi, kişisel veri olarak kabul edilmelidir." Denilmiştir.

3.4. Hareket

5237 sayılı T.C.K.'nın 135. maddesinde düzenlenen "Kişisel verilerin kaydedilmesi" suçunun oluşabilmesi için, belirli veya belirlenebilir bir kişiye ait her türlü bilginin, hukuka aykırı olarak kaydedilmesi gerektir.

Kişisel veri kavramını yukarıda incelemiştik. T.C.K.'nın 135. maddesinde kişisel veri tanımlanmamıştır. Ancak 2 nolu fıkrasında, *"Kişilerin siyasî, felsefî veya dinî görüşlerine, ırkî kökenlerine; hukuka aykırı olarak ahlâkî eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin bilgileri kişisel*

300 Değişiklikten önceki hali: "[1] Hukuka aykırı olarak kişisel verileri kaydeden kimseye altı aydan üç yıla kadar hapis cezası verilir.

[2] Kişilerin siyasî, felsefî veya dinî görüşlerine, ırkî kökenlerine; hukuka aykırı olarak ahlâkî eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin bilgileri kişisel veri olarak kaydeden kimse, yukarıdaki fıkra hükmüne göre cezalandırılır."

veri olarak kaydetme" denilerek kişisel veriden ne kastedildiği açıklanmıştır. Bir başka deyişle, suçun maddi konusunu oluşturan "kişisel veri" kavramından, kişinin, yetkisiz üçüncü kişilerin bilgisine sunmadığı, istediğinde başka kişilere açıklayarak ancak sınırlı bir çevre ile paylaştığı, herkes tarafından bilinmeyen veya kolaylıkla ulaşılması ve bilinmesi mümkün olmayan, kişinin kimliğini belirleyen veya belirlenebilir kılan, kişiyi toplumda yer alan diğer bireylerden ayıran ve onun niteliklerini ortaya koymaya elverişli, gerçek kişiye ait her türlü bilginin anlaşılması gerekir. Bu konuyu iyi analiz etmek gerekir. X kişi cüzam hastasıdır diye kaydedilmişse suç oluşur, ancak X bölgesinde 50 kişi cüzam hastasıdır denilirse elbette ki bu suç oluşmayacaktır. Aynı şekilde, Y kişisi Q partisine oy vermiştir diye kaydedilmişse suç oluşur, ancak Y ilçesinde Q partisine 2000 kişi oy vermiştir diye kaydedilmişse bu suç oluşmaz. Bazı durumlarda bazı olayları kişisel veri olarak kabul ederek bu suçun oluştuğunu düşünsek de özel hayatın gizliliği kapsamında kaldığından ötürü Yargıtay bozma kararları bulunmaktadır[301].

135. maddedeki suçun en çok işlenebileceği yer bilişim alanıdır. Ancak maddede bu konuda herhangi bir sınırlandırma yapılmamıştır. Bu suç bilişim alanında her türlü depolama cihazı kullanılarak yapılabilir.

3.5. Netice

Bu suç tehlike suçudur, zararın meydana gelmesi aranmaz. Kaydetmenin yapıldığı anda suç oluşur. Kayıt etme fiilinin aleniyete dökülüp dökülmemesinin bu suçun oluşumuna bir etkisi yoktur.

4. Suçun Manevi Unsurları

Bu suç ancak kasten işlenebilir. Bu kast genel kasttır, kanun suçun oluşumu için özel kast aramamıştır.

Bu suçun kasten işlenmesi arandığından taksirle işlenemez.

5. Hukuka Aykırılık

T.C.K. madde 135'ün suç teşkil edebilmesi için failin herhangi bir hak ve yetkiye dayanmaması gerekir. Rıza verilmesi bu suçta hukuka aykırılığı kaldırır.

---

301 12. CD. 17.06.2013 T., 2012/20606 E., 2013/16477 K. "bir özel hayat görüntüsü ya da sesinin, "kişisel veri" olduğunda kuşku bulunmamakta ise de, kişinin özel hayatına ilişkin görüntüsü ya da sesinin, bilgisi dışında, resim çekme veya kaydetme özelliğine sahip aletle belli bir elektronik, dijital, manyetik yere sabitlenmesi 5237 sayılı T.C.K.'nın 134/1. maddesinin 2. cümlesinde; rızası dışında ifşa edilmesi, yani; yayılması, açığa vurulması, afişe edilmesi, ilan edilmesi, kamuoyuna duyurulması, aleniyet kazandırılması, özetle; içeriğini öğrenme yetkisi bulunmayan kişi veya kişilerin bilgisine sunulması 5237 sayılı T.C.K.'nın 134/2. maddesinde özel hayatın gizliliğini ihlal suçu kapsamında düzenlendiğinden, kişinin özel hayatına ilişkin görüntüsü, fotoğrafı ya da sesinin, yasal anlamda, 5237 sayılı T.C.K.'nın 135. maddesi kapsamında kişisel veri olarak değerlendirilemeyeceği anlaşılmakla; Sanığın mağdurelerin etek altı ve erojen bölgelerinin fotoğraflarını çekmesi eyleminin 5237 sayılı T.C.K.'nın 134/1. maddesinin 2. cümlesinde düzenlenen özel hayatın gizliliğini ihlal suçunu oluşturacağı" – Uyap Mevzuat Programı

Bunun dışında kanunun verdiği bir yetkinin kullanılması da (T.C.K. madde 24) suçta hukuka aykırılığı ortadan kaldırır. Madde gerekçesinde de *"Belirli nitelikteki kişisel verilerin kayda alınması kanun hükmünün gereği olarak yapılmaktadır. Bu bakımdan, çeşitli kamu kurumlarında verilen kamu hizmetinin gereği olarak kişilerle ilgili bazı bilgiler ilgili kanun hükümlerine istinaden kayda alınmaktadırlar. Bu durumlarda, söz konusu suç oluşmayacaktır."* Denilmektedir.

C.M.K.'nın 134. maddesinde düzenlenen bilgisayar kütüklerine el koyma, madde 135'te düzenlenen iletişimin denetlenmesi durumları suçun hukuka aykırılık unsurunu ortadan kaldırır.

6. Suçun Özel Görünüş Şekilleri

6.1. Teşebbüs

Bu suç salt hareket suçu olduğu için ancak icra hareketleri bölünebiliyorsa teşebbüs mümkün olacaktır[302].

6.2. İştirak

5237 sayılı T.C.K.'nın 135. maddesinde düzenlenen kişisel verilerin kaydedilmesi suçu iştirak açısından bir özellik söz konusu olmayıp, genel hükümler uygulanacaktır. Genel hükümler değerlendirildiğinde bu suç tipleri için iştirak türlerinin gerçekleşmesi mümkündür

6.3. İçtima

5237 sayılı T.C.K.'nın 44. maddesi gereğince, T.C.K.'nın 135. maddesinde belirtilen suçun islenmesi için, aynı kanunun 243. maddesinde düzenlenen hukuka aykırı olarak bilişim sistemine girme ve sistemde kalma suçunun da islenmesi halinde, yalnızca 135. maddesinde öngörülen ceza, faile verilecektir.

7. Suça Etki Eden Sebepler

T.C.K. 137. maddesine göre, failin bazı özellikleri taşıması durumunda suçun cezası ağırlaşır. Başka bir deyişle, bu suçun "kamu görevlisi tarafından ve görevinin verdiği yetki kötüye kullanılmak suretiyle veya belli bir meslek ve sanatın sağladığı kolaylıktan yararlanmak suretiyle" işlenmesi hâlinde, verilecek ceza yarı oranında artırılır.

302 Tezcan Durmuş/Erdem Mustafa Ruhan/Önok Rıfat Murat,s.469

8. Kovuşturma, Görevli Mahkeme, Suçun Yaptırımı ve Dava Zamanaşımı

Kovuşturma: Maddede tanımlanan suçun soruşturması ve kovuşturması resen yapılır

Görevli Mahkeme: 5235 sayılı Kanun'un 10. maddesi uyarınca T.C.K.'nın 135. maddesine göre açılan davalara bakma görevi asliye ceza mahkemesine aittir.

Suçun Yaptırımı: Maddenin birinci fıkrasına göre, Hukuka aykırı olarak kişisel verileri kaydeden kimseye bir yıldan üç yıla kadar hapis cezası verilir; ikinci fıkraya göre, Kişilerin siyasî, felsefî veya dinî görüşlerine, ırkî kökenlerine; hukuka aykırı olarak ahlâkî eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin bilgileri kişisel veri olarak kaydeden kimse, yukarıdaki fıkra hükmüne göre cezalandırılır.

Dava Zamanaşımı: T.C.K.'nın 66/1-e maddesi uyarınca bu suçların dava zamanaşımı süresi 8 yıldır.

e. Kişisel Verileri Hukuka Aykırı Olarak Verme veya Ele Geçirme Suçu

1. Genel Olarak

5237 sayılı T.C.K.'nın "Kişisel Verileri Hukuka Aykırı Olarak Verme veya Ele Geçirme" başlıklı 136. maddesi: "*(Değişik: 21/2/2014 – 6526/4 md.)Kişisel verileri, hukuka aykırı olarak bir başkasına veren, yayan veya ele geçiren kişi, iki yıldan dört yıla kadar hapis cezası ile cezalandırılır.*"

Görüldüğü üzere yakın bir tarihte madde metninde değişikliğe gidilerek suçun cezasının alt sınırı yükseltilmiştir[303].

Bu suç özellikle internet ortamında işlenmektedir.

2. Korunan Hukuksal Değer

Bu suç maddesiyle özel hayatın gizliliği korunmaktadır. T.C.K.'nın 135. maddesi ile paralellik göstermektedir.

3. Suçun Maddi Unsurları

3.1. Fail

Tüzel kişilerin sorumluluğu ise, T.C.K.'nın 140. maddesine göre değerlendirilecektir. Maddedeki *"Yukarıdaki maddelerde tanımlanan suçların işlenmesi dolayısıyla tüzel kişiler hakkında bunlara özgü güvenlik tedbirlerine*

303 Değişiklikten önceki hali: "Kişisel verileri, hukuka aykırı olarak bir başkasına veren, yayan veya ele geçiren kişi, bir yıldan dört yıla kadar hapis cezası ile cezalandırılır."

hükmolunur." hükmü gereğince tüzel kişilere T.C.K.'nın 60. maddesindeki güvenlik tedbirleri uygulanacaktır.

3.2. Mağdur

T.C.K.'nın 136. maddesindeki suçun mağduru da tüm gerçek kişiler olabilir.

3.3. Suçun Konusu

Söz edilmek istenen suçun maddi konusudur. Zira, suçun hukuki konusunu "korunan hukuksal değer başlığı altında" incelemekteyiz. Suçun maddi konusu, üzerinde suçun işlendiği şahıs veya şeydir[304]. Bir başka görüşe göre ise, suçun konusu, üzerinde suçun meydana geldiği hareketin kendisine yöneldiği insan ya da maddi varlıklardır[305].

Bu suçun maddi konusunu kişisel veriler oluşturmaktadır.

3.4. Hareket

Bu suç tipi seçimlik hareketli bir suçtur. Belirtilen eylemlerin herhangi birinin veya bir kaçının gerçekleştirilmesiyle bu suç islenmiş olacak ve faile tek bir suçun cezası verilecektir. Bu suç tipinde verilerin nasıl kaydedildiğinin bir önemi yoktur.

Şimdi kanun metninde yazılı çeşitli hareketleri inceleyelim.

3.4.1. Kişisel Verileri Başkasına Verme Eylemi

Bu suç tipi seçimlik hareketli bir suçtur. Belirtilen eylemlerin herhangi birinin veya bir kaçının gerçekleştirilmesiyle bu suç islenmiş olacak ve faile tek bir suçun cezası verilecektir.

Bu hareketteki "başkası" kelimesi gerçek kişi olabileceği gibi tüzel kişi de olabilir[306].

3.4.2. Kişisel Verileri Yayma Eylemi

Verme ile yayma hareketleri birbirine benzemektedir. Bununla birlikte, verme, yayma düzeyine ulaşmayan bir seviyede olup, kişisel verileri yayma fiili, verme fiilinden daha ileri aşamadadır. Yani yayma fiili, birden fazla kişiye kişisel verilerin verilmesini ifade etmektedir[307]. Bu eylem, kişisel verilerin yazılı olarak mektup seklinde birden fazla kişiye gönderilmesi, internet üzerinde bir web sitesinde

304 Toroslu Nevzat, s.66

305 Taşkin Şaban Cankat, s.24

306 Karagülmez Ali, s.356

307 Karagülmez Ali, s.356

kişisel verileri başkaları için erişilebilir kılmak ya da bir forum odasında açıklama yapmak seklinde gerçekleşebilir[308].

3.4.3. Kişisel Verileri Ele Geçirme Eylemi

Bu eylem, kişisel verilerin üzerinde yazılı olduğu belgelerin bulunduğu yerden alınması ya da verilerin kayıtlı olduğu bilişim sistemine girilerek verilerin bir depolama cihazına kaydedilmesi şeklinde yapılabilecektir. Görüleceği üzere sadece öğrenmek yeterli değildir, suçun oluşumu için ele geçirme gerekmektedir[309].

3.5. Netice

Suçun oluşması için mutlaka bir netice gerekir. Ceza hukukunda netice maddi bir olgu değildir. Maddi olgunun gerçekleşmesi ihtimali, tehlikesi de bir neticedir. Bu tür neticesi olabilen suçlara tehlike suçu denir[310]. Bu suç tipinin oluşması için suçun neticesinde bir zararın meydana gelmesi aranmamaktadır. Yukarıda belirtilen eylemlerin gerçekleştirilmesi suçun oluşumu için yeterlidir.

4. Suçun Manevi Unsurları

Bu suç ancak kasten işlenebilir. Bu kast genel kasttır, kanun suçun oluşumu için özel kast aramamıştır.

Bu suçun kasten işlenmesi arandığından taksirle işlenemez.

5. Hukuka Aykırılık

T.C.K. madde 136'ün suç teşkil edebilmesi için failin herhangi bir hak ve yetkiye dayanmaması gerekir. Rıza verilmesi bu suçta hukuka aykırılığı kaldırır.

Bunun dışında kanunun verdiği bir yetkinin kullanılması da (T.C.K. madde 24) suçta hukuka aykırılığı ortadan kaldırır. C.M.K.'nın 126. maddesinde düzenlenen el koyma ve 135. maddesinde düzenlenen iletişimin denetlenmesi durumları suçun hukuka aykırılık unsurunu ortadan kaldırır.

---

308 12. CD. 15.05.2012 T., 2011/20072 E., 2012/12126 K. "Köşe yazarı olarak çalışan katılanın, sanığın genel yayın yönetmenliğini yaptığı gazetede yazdığı köşesinde kullanılan fotoğrafının, katılanın rızası olmadan arkadaşlık sitesine konulması eyleminin, T.C.K.'nın 136. maddesinde düzenlenen, kişisel verileri hukuka aykırı olarak yayma suçunu oluşturacağı, hukuki durumunun buna göre tayin ve takdiri gerektiği gözetilmeden, suç vasfında yanılgıya düşülerek, yazılı şekilde karar verilmesi,"

309 8. CD. 13.11.2013 T., 2013/17807 E., 2013/27106 K."Sanık hakkında "banka veya kredi kartının kötüye kullanılması" suçundan kurulan mahkumiyet hükmünün temyizinde; Sanığın bir bankanın ATM cihazlarına yerleştirdiği düzeneklerle işlem yapmaya gelen kişilere ait kartların manyetik şerit bilgilerini kopyalamak ve şifrelerini elde etmeye çalışmaktan ibaret eylemi, alınan bilgilerle kredi kartı düzenlenip düzenlenmeyeceği bilinmediği gibi bu düşünceden her zaman vazgeçilebileceği verilerin kart düzenlenmeden de kullanılabileceği gözetildiğinde kişisel verilerin hukuka aykırı olarak ele geçirilip kaydedilmesine yönelik olup T.C.K..nun 136. maddesinde düzenlenen suçun oluştuğu gözetilmeden yazılı şekilde hüküm kurulması," Uyap Mevzuat Programı

310 Soyaslan, Doğan, (Genel Hükümler) s.232

6. Suçun Özel Görünüş Şekilleri

6.1. Teşebbüs

Bu suç salt hareket suçu olduğu için ancak icra hareketleri bölünebiliyorsa teşebbüs mümkün olacaktır. Fail tarafından icra hareketlerine başlandıktan sonra bu hareketlerin yarıda kalması durumunda teşebbüs hali gerçekleşecektir. Mesela kişisel verileri ele geçirirken sistemdeki bir hata veya elektriğin kesilmesi nedeniyle verilerin kopyalanamaması durumunda teşebbüs olacaktır.

6.2. İştirak

5237 sayılı T.C.K.'nın 136. maddesinde düzenlenen özel hayatın gizliliği suçu iştirak açısından bir özellik söz konusu olmayıp, genel hükümler uygulanacaktır. Genel hükümler değerlendirildiğinde bu suç tipleri için iştirak türlerinin gerçekleşmesi mümkündür.

6.3. İçtima

Verileri hukuka aykırı olarak verme veya ele geçirme suçu her defasında aynı kişiye aynı mağdura karşı işleniyorsa zincirleme suç hükümleri uygulanır.

5237 sayılı T.C.K.'nın 44. maddesi gereğince, T.C.K.'nın 135. maddesinde belirtilen suçun islenmesi için, aynı kanunun 243. maddesinde düzenlenen hukuka aykırı olarak bilişim sistemine girme ve sistemde kalma suçunun da islenmesi halinde, yalnızca 135. maddesinde öngörülen ceza faile verilecektir.

7. Suça Etki Eden Sebepler

T.C.K. 137. maddesine göre, failin bazı özellikleri taşıması durumunda suçun cezası ağırlaşır. Başka bir deyişle, bu suçun "kamu görevlisi tarafından ve görevinin verdiği yetki kötüye kullanılmak suretiyle veya belli bir meslek ve sanatın sağladığı kolaylıktan yararlanmak suretiyle" işlenmesi hâlinde, verilecek ceza yarı oranında artırılır.

8. Kovuşturma, Görevli Mahkeme, Suçun Yaptırımı ve Dava Zamanaşımı

Kovuşturma: Maddede tanımlanan suçun soruşturması ve kovuşturması resen yapılır

Görevli Mahkeme: 5235 sayılı Kanun'un 10. maddesi uyarınca T.C.K.'nın 136. maddesine göre açılan davalara bakma görevi asliye ceza mahkemesine aittir.

Suçun Yaptırımı: Maddeye göre, kişisel verileri, hukuka aykırı olarak bir başkasına veren, yayan veya ele geçiren kişi, iki yıldan dört yıla kadar hapis cezası ile cezalandırılır.

Dava Zamanaşımı: T.C.K.'nın 66/1-e maddesi uyarınca bu suçların dava zamanaşımı süresi 8 yıldır.

f. Verilerin Yok Edilmemesi Suçu

1. Genel Olarak

T.C.K.'nın 138. maddesi: *"[1] (Değişik: 21/2/2014 – 6526/5 md.)Kanunların belirlediği sürelerin geçmiş olmasına karşın verileri sistem içinde yok etmekle yükümlü olanlara görevlerini yerine getirmediklerinde bir yıldan iki yıla kadar hapis cezası verilir.*

[2] (Ek: 21/2/2014-6526/5 md.) Suçun konusunun Ceza Muhakemesi Kanunu hükümlerine göre ortadan kaldırılması veya yok edilmesi gereken veri olması hâlinde verilecek ceza bir kat artırılır."

Görüldüğü üzere madde çok yakın bir zamanda değişikliğe uğramıştır. Değişikle ceza miktarı artmış ve ikinci fıkra ile ağırlaştırıcı hali de düzenlenmiştir[311].

2. Korunan Hukuksal Değer

Bu suç maddesiyle öncelikle, özel hayatın gizliliği korunmaktadır. T.C.K.'nın 135. ve 136. maddesi ile paralellik göstermektedir.

Bu suç tipiyle ayrıca kamu idaresine karsı duyulan güven korunmaktadır. Çünkü kanunda verileri yok etmekle görevlendirilen kişi bunu, kamu görevi olarak yapmaktadır[312].

3. Suçun Maddi Unsurları

3.1. Fail

5237 sayılı T.C.K.'nın 138. maddesinde suçu işleyecek kişi açısından herhangi bir özellik belirtilmediği için suçun faili herkes olabilir.

Tüzel kişilerin sorumluluğu ise, T.C.K.'nın 140. maddesine göre değerlendirilecektir. maddedeki *"Bu bölümde yer alan suçların işlenmesi suretiyle yararına haksız menfaat sağlanan tüzel kişiler hakkında bunlara özgü güvenlik tedbirlerine hükmolunur."* Hükmü gereğince tüzel kişilere T.C.K.'nın 60. maddesindeki güvenlik tedbirleri uygulanacaktır.

311 Değişiklikten önceki hali: "Kanunların belirlediği sürelerin geçmiş olmasına karşın verileri sistem içinde yok etmekle yükümlü olanlara görevlerini yerine getirmediklerinde altı aydan bir yıla kadar hapis cezası verilir"

312 Dülger Murat Volkan, s.282

3.2. Mağdur

T.C.K.'nın 138. maddesindeki suçun mağduru tüm gerçek kişiler olabilir.

3.3. Suçun Konusu

Bu suçun maddi konusunu kişisel veriler oluşturmaktadır.

3.4. Hareket

T.C.K.'nın 138. maddesinde düzenlenen verileri yok etmeme suçu da failin, verilerin sistemden yok edilmesi görevini yapmamasıyla islenebilmektedir. Bu nedenle bu suç, ihmali bir hareketle gerçekleştirilmektedir. İhmal, davranış normlarıyla kişiye belli bir icrai davranışta bulunma yükümlülüğünün tahmil edildiği hallerde, kişinin yükümlülüğü yerine getirmemesidir. İhmali suçlarda söz konusu olan fiil ise, belli bir davranışın gerçekleştirilmemesi, belli bir davranışta bulunulmamasıdır[313].

3.5. Netice

Bu suç, ihmali hareketle gerçekleşir. Kanunun belirlediği süre sonunda sistem içindeki verilerin yok edilmesi eylemi gerçekleştirilmemişse bu suç gerçekleşmiş olacaktır. Bu suçta, zarar şartı aranmaz.

4. Suçun Manevi Unsurları

Bu suç ancak kasten işlenebilir. Bu kast genel kasttır, kanun suçun oluşumu için özel kast aramamıştır.

Bu suçun kasten işlenmesi arandığından taksirle işlenemez.

5. Hukuka Aykırılık

Bu suç tipi açısından gerek mağdurun rızası gerekse kanundan kaynaklanan bir hukuka uygunluk sebebi bulunmamaktadır. Zira bu suçun mağduru kamu düzenidir. Ancak mücbir sebep nedeniyle bu suç açısından bir hukuka uygunluk sebebi oluşabilecektir[314].

6. Suçun Özel Görünüş Şekilleri

6.1. Teşebbüs

Bu suç tipi ihmal suretiyle islenebileceğinden, bu suçta teşebbüs hali söz konusu olmayacaktır.

313 Özgenç İzzet: Türk Ceza Kanunu Gazi Şerhi, Genel Hükümler, Adalet Bakanlığı Eğitim Dairesi Başkanlığı, Ankara, 2005, s.231

314 Yayci Esra, s.140

6.2. İştirak

5237 sayılı T.C.K.'nın 138. maddesinde düzenlenen verileri yok etmeme suçu iştirak açısından bir özellik söz konusu olmayıp, genel hükümler uygulanacaktır. Genel hükümler değerlendirildiğinde bu suç tipleri için iştirak türlerinin gerçekleşmesi mümkündür.

6.3. İçtima

Verileri yok etme suçu, her defasında aynı kişiye aynı mağdura karşı işleniyorsa zincirleme suç hükümleri uygulanır.

7. Suça Etki Eden Sebepler

Bu suç açısında suça etki eden herhangi bir sebep bulunmamaktadır.

8. Kovuşturma, Görevli Mahkeme, Suçun Yaptırımı ve Dava Zamanaşımı

Kovuşturma: Maddede tanımlanan suçun soruşturması ve kovuşturması resen yapılır

Görevli Mahkeme: 5235 sayılı Kanun'un 10. maddesi uyarınca T.C.K. 138'ya göre açılan davalara bakma görevi Sulh ceza mahkemesine aittir.

Suçun Yaptırımı: Maddeye göre, kanunların belirlediği sürelerin geçmiş olmasına karşın verileri sistem içinde yok etmekle yükümlü olanlara görevlerini yerine getirmediklerinde bir yıldan iki yıla kadar hapis cezası verilir. Suçun konusunun Ceza Muhakemesi Kanunu hükümlerine göre ortadan kaldırılması veya yok edilmesi gereken veri olması hâlinde verilecek ceza bir kat artırılır.

Dava Zamanaşımı: T.C.K.'nın 66/1-e maddesi uyarınca bu suçların dava zamanaşımı süresi 8 yıldır.

D. TÜRK CEZA KANUNU'NDAKİ BİLİŞİM SİSTEMLERİ ARACILIĞIYLA İŞLENEBİLECEK DİĞER SUÇ TİPLERİ

a. Bilişim Sisteminin Kullanılması Yoluyla İşlenen Hırsızlık Suçu

Medeni hukuk müessesi olarak taşınır mal, özüne zarar vermeksizin nitelikleri itibari ile kendi gücüyle veya başka bir güç sayesinde bir yerden başka bir yere taşınabilen eşyadır[315], eşya ise üzerinde hakimiyet sağlanabilen, ekonomik değer taşıyan, kişilik dışı cismani varlıklardır.[316] Ceza hukuku müessesesi olarak taşınır mal ise, insanın yaşam ve ilişkilerinde herhangi bir gereksinim için kullandıkları taşınabilir şeylerdir.[317] Buna göre, hırsızlık suçuna konu olan bir malın[318]:

315 Oğuzhan Kemal/Seliçi Özer /Oktay Özdemir Saibe, Eşya Hukuku, 11. Baskı, İstanbul, 2006 s.568

316 Oğuzhan Kemal/Seliçi Özer /Oktay Özdemir Saibe, s.6

317 Tezcan Durmuş/Erdem Mustafa Ruhan /Önok R. Murat, s.474

- *malvarlığı haklarının konusunu oluşturması,*
- *maddi veya manevi bir değere sahip olması,*
- *cismani bir yapısının bulunması gerekmektedir.*

Hırsızlık suçunun konusunu başkasının taşınır bir malının (eşya) oluşturduğunu söyleyebiliriz, taşınır mal olma hususunun tek istisnası ise enerji hırsızlığıydı, ancak bu husus da karşılıksız yararlanma suçu kapsamına alınmıştır.

Teknolojinin hızla gelişmesi karşısında hırsızlık suçumum teknolojik gelişme gösteren bilişim sistemleri vasıtasıyla da işlenebilme olasılığı düşünülerek, yasa koyucu nitelikli hallerden biri olarak T.C.K.'nın 142/2-e maddesindeki hırsızlık suçunun *'bilişim sistemlerinin kullanılması suretiyle'* işlenmesini düzenlemiştir. Bu nitelikli hal 5237 sayılı Türk Ceza Kanunumuzun getirdiği yeniliklerden biridir. Buna göre, hırsızlık suçunun işlenmesi sırasında bilişim sistemleri kullanılırsa hırsızlık suçunun basit halinden daha ağır cezaya hükmedilecektir. Bilişim sistemi aracılığıyla bir suçun işlenmesinin nitelikli hal olarak sayılması yerinde bir düzenlemedir diyebiliriz. Zira, bilişim sistemi kullanıldığında kişi kendini gerektiği gibi savunamaz, saldırılara karşı zayıftır.

T.C.K.'nın 142/2-e maddesindeki nitelikli halin bazı yönlerden T.C.K.'nın 244. maddesinin 4. fıkrasındaki 'bilişim sistemine veya verileri müdahale suretiyle haksız çıkar sağlanması' suçu ile benzerlik göstermektedir ve bazı durumlarda bu iki suçtan hangisinin oluşacağı konusunda tartışmalar bulunmaktadır.

Maddi bir varlığa sahip olmayan 'veri' hırsızlık suçuna konu olabilecek midir veya maddi varlıkların, bilişim sistemlerinin araç olarak kullanılması suretiyle çalınarak hırsızlık suçuna konu edilmesi mümkün müdür, internet üzerinden başkasının hesabından para aktarılması şeklinde gerçekleşen fiiller suçu için ayrıksı bir durum var mıdır, Bu fiiller T.C.K.'nın 142/2-e maddesine mi yoksa 244. maddenin 4 fıkrasının mı kapsamına girer, soruları akla gelebilir. Şimdi bu sorulara cevap arayarak araştırmamıza devam edelim.

İlk önce bu hususlarla ilgili doktrindeki görüşlere bakarak konumuzu açıklamaya çalışalım. Daha sonra Yargıtay'ın görüşüne ve bizim görüşümüze de yer vereceğiz. İlk önce doktrindeki görüşlere değinmeye başlayarak yukarıdaki sorularımıza cevap bulmaya çalışalım.

---

318 Soyaslan, Doğan, (Genel Hükümler), s. 290-291

Verinin, hırsızlık suçuna konu olabileceğini savunan yazarlara göre, nasıl ki elektrik enerjisi fiziki bir yapıya sahip olmadığı halde hırsızlığa konu olabiliyorsa, verinin de aynı şekilde düşünülmesi gerekir, verinin ekonomik bir değeri bulunduğunu, içinde bulunduğumuz bilgi çağının bir gereği olarak verinin hırsızlık suçuna konu olması gerekmektedir. [319] [320] [321]

Verinin, hırsızlık suçuna konu olabileceğini savunan yazarlara göre, hırsızlık ancak taşınabilir bir mal üzerinde işlenebildiğinden, kanunda veri taşınabilir bir mal olarak tanımlanmadığına göre, veriyi temel alarak bilişim sistemi kullanmak suretiyle elde edilen haksız edinimleri hırsızlık suçu ile kıyaslamak mümkün değildir. Bilgisayarlarda yer alan bilgi ne fiziki bir yapı içermekte ne de taşınabilir bir mal niteliğine sahip bulunmaktadır. Dolayısıyla, bilgisayarlarla işlenen fiilleri ceza kanundaki mal aleyhine işlenen suçlar kapsamında değerlendirilmesi mümkün olmamalıdır. Bir kimse, bilgisayar sistemine yanlış veri girerek veya mevcut verileri değiştirerek bir bankadaki mevduatı kendi hesabına aktarmak suretiyle haksız yarar sağlayacak olsa, ortada yine taşınabilir bir mal bulunmadığı için hırsızlık suçundan bahsedilemeyecektir[322].

Bize göre ise, kanunda da açıkça belirtildiği üzere hırsızlık suçu, ancak taşınabilir bir fiziki mal üzerinde işlenebilecektir. T.C.K. 141/2'de "ekonomik bir değer taşıyan her türlü enerji de, taşınır mal sayılır." denilerek taşınır malın kapsamı genişletilmiş ve bu fıkraya istinaden T.C.K. m.142/1-f'de elektrik enerjisinin bu suçun konusunu oluşturacağı özel olarak düzenlenmişti. Ancak enerji ile ilgili bu hükümler de hırsızlık suçunun konusu olmaktan çıkarak karşılıksız yararlanma suçu kapsamına alınmıştır. Buradan yola çıktığımızda *veriyi,* taşınır malın yerine yerine koymamız mümkün değildir. T.C.K.'nın 142/2-e maddesine baktığımızda hırsızlık suçunun konusunu verinin oluşturacağını özel olarak düzenlemediğini görmekteyiz.

---

319 Karagülmez Ali, s.195,196

320 Taşkin Şaban Cankat, s.116

321 Parlar Ali, s.108

322 Yazicioğlu Yılmaz, "Bilişim Suçları, Hukuki Perspektifler Dergisi", Sayı 2, 2004, s.144; ÖZBEK Veli Özer, "Banka Ve Kredi Kartlarının Kötüye Kullanılması Suçu", Dokuz Eylül Hukuk Fakültesi Dergisi, Cilt 9, 2007, s.1058; ÖZEN Muharrem/BAŞTÜRK İhsan, s.137-139; HATİPOĞLU Muzaffer/PARLAR Ali, s.145'ten, KOCA Mahmut, "5237 Sayılı Yeni Türk Ceza Kanunu'nda Malvarlığına Karşı İşlenen Suçlar (Makale)", Kazancı Dergisi, Ocak 2005, Sayı 5, s.75; ERDEM Mustafa Ruhan, "Türk Ceza Kanunu'nda Malvarlığına Karşı Suçlar, (Makale)", www.ceza-bb.adalet.gov.tr/makale/119.doc s.512; YILDIZ M. Emre, "İnternet Bankacılığı Hakkında Yargıtay'ın 17.11.2009 Tarih 2009/11-193 Esas Sayılı Kararının İncelenmesi", Ceza Hukuku Dergisi, Aralık 2010, Sayı: 14, s.147 ; ESEN Sinan, "Anlatımlı Ve İçtihatlı Malvarlığına Karşı Suçlar, Belgelerde Sahtecilik Ve Bilişim Alanından Suçlar", Ankara, Eylül 2007, s.99-100; BAŞBÜYÜK İsa, "Hırsızlık Ve Dolandırıcılık Suçlarının Bilişim Sistemlerinin Araç Olarak Kullanılması Suretiyle İşlenmesi", Ceza Hukuku Dergisi, Sayı: 14, Adalet Yayınevi, Aralık 2010,s.159-160; TAŞDEMİR Kubilay, s. 276; DÜLGER Murat Volkan, s.289-290; TEZCAN Durmuş/ERDEM Mustafa Ruhan /ÖNOK R. Murat, s.506

Bu nedenle, T.C.K.'nın 141. maddesi anlamında verinin bir yerden çekip alınması bize göre hırsızlık suçunu oluşturmayacaktır.

Veri hırsızlığının, ancak mülga T.C.K.'nın 142/1-f maddesinde düzenlenen elektrik enerjisinin çalınmasında olduğu gibi özel olarak düzenleme yapılması durumunda mümkün olacağı görüşündeyiz. Bu durumda artık diyebiliriz ki, bilgisayardan çekilen bir verinin bilişim yolu suretiyle hırsızlık olarak değerlendirilmesi pek mümkün olmamaktadır. Çünkü buradaki verinin taşınabilir bir şey özelliğinden bahsedilemez. Örneğin, sahibinin rızası olmaksızın, bir başkasının bilgisayarındaki müzik dosyalarını kendi bilgisayarına alan kimsenin fiili hırsızlık suçunu oluşturmayacaktır[323]. Çünkü az önce de dediğimiz gibi örnekte bilgisayardan çekilen verinin taşınabilme özelliği bulunmamaktadır. Tabii ki yapılan bu eylem başka bir suç kapsamına giriyorsa bu suçtan cezalandırılmasına engel bulunmamaktadır. Örneğin, A'nın, B'nin bilgisayarından onun izni olmadan bilgisayarındaki dosya, fotoğraf ve video vb. verilerini kendi taşınabilir belleğine alması durumu, taşınır bir malın izinsiz olarak alınması suçu olan hırsızlanma anlamına gelmese de kanunda düzenlenen diğer suç olan bilişim sistemine girme, özel hayatın gizliliğini ihlal suçlarını oluşturacağını rahatlıkla söyleyebiliriz. Bu durumlardan farklı bir özellik taşıyan internet bankacılığından yapılan havale ile haksız çıkar sağlamanın da bilişim yollarını kullanmak suretiyle hırsızlık suçunu oluşturmayacağını düşünmekteyiz.

Sonuç olarak biz, T.C.K.'nın 142/2-e maddesindeki bilişim sistemlerini kullanmak suretiyle hırsızlık suçunun verinin çekilmesi ile oluşmayacağına, sadece bilişim yoluyla *maddi* varlıkların çalınması olaylarının gerçekleştiği durumlarda söz konusu olacağı kanaatine varmış bulunmaktayız. Çünkü dediğimiz gibi kanunumuzda veri hırsızlığına özel olarak yer verilmemiştir.

Yukarıda bilişim sistemlerinin araç olarak kullanılması suretiyle hırsızlık suçunun işlenip işlenemeyeceği problemine verinin hırsızlık suçuna konu olup olmayacağı noktasında görüşlere değindik. Kanaatimizce, verinin hırsızlık suçuna konu olamayacağı görüşünü benimseyerek, *verinin çalınabilmesi hususunda* söz konusu fıkranın işlersiz olduğunu ifade etmeye çalıştık. Ancak, bilişim sistemlerinin araç olarak kullanıldığı akla sürekli verinin çalınması hususunun gelmesi doğru değildir, bu yolla işlenen *suçun konusu maddi bir varlığa ilişkin de* olabilir. Bir diğer

323 Başbüyük İsa, s.159

ifadeyle, bilişim sistemlerinin araç olarak kullanılması suretiyle işlenen her hırsızlık suçunun konusu 'veri' olmayabilir, bunun yerine maddi bir varlık olabilir. Nitekim veri hırsızlığı söz konusu olmadan maddi varlığı olan bir şeyin bilişim sistemleri kullanılarak hırsızlık suçunun işlenmesi mümkündür. Örneğin; bilgisayar sistemlerinden faydalanmak suretiyle otomatik yükleme yapılan bir yerde, sistemin şifresini bilen kişiler bu şifre ile sisteme girip vinci harekete geçirerek kendi araçlarına ürün yüklerse, elde edilen yarar bakımından yalnızca nitelikli hırsızlık suçunu işlemiş olacaklardır[324]. Görüldüğü üzere burada maddi bir varlık bilişim sistemlerinin kullanılması suretiyle hırsızlanmaktadır.

Maddi varlıkların bilişim sistemleri suretiyle çalınması sırasında, bilişim sisteminin işleyişinin engellenmesi, sistemde yer alan verilenin değiştirilmesi, bozulması veya bir başka yere gönderilmesi de söz konusu olabilir. Örneğin; merkezi sisteme bağlı olarak çalışan ve bu sistemle uzaktan kontrol edilen bir aracın, merkezle bağlantısının kesilmesi için bağlı bulunduğu sisteme dıştan müdahale edilerek, istenilen yere yönlendirilerek çalınması durumunda nitelikli hırsızlık suçu ile birlikte T.C.K.'nın 244. maddesinin 1. fıkrasında yer alan suç da oluşmaktadır. Nitekim fail önce T.C.K.'nın 244. maddesinin 1. fıkrası anlamında bir bilişim sisteminin işleyişini engellemekte, daha sonra T.C.K.'nın 142/2-e maddesi anlamında bilişim sistemini kullanarak (uzaktan kumanda yöntemiyle) başkasına ait olan aracı kendi hakimiyet alanına sokmaktadır[325]. Hem T.C.K.'nın 244. maddesinin 1. fıkrasında hem de T.C.K.'nın 142/2-e maddesinin birlikte var olduğu bir başka örnekte şunu verebiliriz: Bilgisayar merkezi kilit sistemine bağlı olarak korunan bir deponun kapısının, bilişim sistemi şifrelerinin kırılması suretiyle açılması ve orada bulunan beyaz eşyaların çalınması olayında durum böyledir. Yine aynı şekilde güvenlik sistemi bir bilişim ağına bağlı olan bir binaya bilişim sistemi kullanılarak güvenlik ağının kaldırılması ile bir mal çalınması olayında[326] da iki suç birlikte oluşur. Ancak burada fikri içtima hükümleri de düşünülebilir.

Vermiş olduğumuz örnekler günümüz açısından var olan teknoloji ile gerçekleşmesi çok zor şeyler değildir. Günümüz şartlarında ve gelişen teknolojik gelişmelerle bu şekilde de hırsızlık suçunun işlenmesi artık mümkündür. Görüldüğü gibi yukarıda vermiş olduğumuz iki örnekte de veri değil maddi varlığı olan cismani

324 Başbüyük İsa, s. 164

325 Başbüyük İsa, s. 164

326 Taşdemir Kubilay, s. 100

şeyler bilişim sistemini kullanmak suretiyle çalınmaktadır. Bu nedenlerle bilişim sistemlerini kullanmak suretiyle hırsızlığı düzenleyen T.C.K.'nın 142/2-e maddesinin bahsettiğimiz şekilde yorumlanması durumunda yerinde bir hüküm olduğunu söyleyebiliriz.

Şimdi ise araştırmamızın diğer bir parçası olan internet bankacılığı yoluyla hukuka aykırı olarak yapılan havale işleminin nitelikli hırsızlığın konusuna mı yoksa bilişim sistemleri aracılığıyla yarar sağlama suçunun konusuna mı girdiği hususunu ele alacağız.

İnternet bankacılığı, müşterilerin banka tarafından sunulan hizmetlere internet yoluyla ulaşmalarını ve yapmak istedikleri işlemleri gerçekleştirmelerini sağlayan bankacılık hizmeti dağıtım kanalı olarak ifade edilmektedir[327]. İnternet bankacılığı, bankacılık işlemlerinin banka şubesine gitmeden internet üzerinden yapıldığı bir sistemdir. Banka müşterisi ile banka arasında yapılan bir sözleşme ile kimlik doğrulaması için banka müşterisine kullanıcı adı ve şifre verilir, bunun yanında önceden tanımlanmış IP ve mobil telefona gelen onay kodu gibi ek güvenlik sistemleri ile internet üzerinden işlem yapılmasına izin verilir.

Anlaşıldığı üzere, internet bankacılığı da insanlara sunulan bir kolaylıktır. O yüzden Hırsızlık suçunun bilişim sistemleri aracılığıyla işlenmesi, suçun işlenişinde sağladığı kolaylık ve başkaca hukuki yararların da ihlalini içerdiği için, nitelikli hal olarak öngörülmüştür[328]. Ancak daha önce de belirttiğimiz üzere bu yolla hırsızlık suçunun işlenip işlenmeyeceğini hususunda tartışma vardır. Yukarıda verinin hırsızlık suçuna konu olabilmesi hususuna ayrıntılı olarak değinmiş, bir verinin taşınmasının hırsızlık suçuna konu olamayacağına kanaat getirmiştik. Şimdi burada daha önce bahsettiklerimizin (bilgisayardan video, fotoğraf vb. veriler) dışında ayrıksı bir durum olan haksız bir şekilde ele geçirilen internet bankacılığı şifresi ile başkasına ait hesaptan havale yaparak haksız çıkar sağlanması eylemini değerlendireceğiz. Bu konuyu verinin hırsızlık suçuna konu olabilmesi hususundan ayrı bir başlıkta değerlendirmemizin sebebi, yapılan havale sonrası paranın çekilmesi ile hırsızlık suçunun maddi konusu olan başkasına ait alınan eşyanın, taşınır bir mal olma şartının gerçekleşeceği yönünde değerlendirmelerin olmasıdır. Bunun en büyük göstergesi YCGK'nın internet bankacılığı şifrelerinin kırılması suretiyle

327 14.09.2007 Tarih ve 26643 sayılı Resmi Gazetede yayımlanan Bankalarda Bilgi Sistemleri Yönetiminde Esas Alınacak İlkelere İlişkin Tebliğin 3/1-j maddesinde

328 Başbüyük İsa, s.160

gerçekleştirilen haksız havale işlemini bilişim sistemlerini kullanmak suretiyle hırsızlık suçu kabul etmesidir.

Yargıtay'ın bir kararında, internet üzerinden başkasının hesabından para aktarılması şeklinde gerçekleşen fiil, bilişim sistemi aracılığıyla hırsızlık suçu kapsamında, bir başka kararında ise, internet bankacılığı şifrelerinin kırılması suretiyle gerçekleştirilen haksız havale işlemi, T.C.K.'nın 244. maddesinin 4. fıkrası kapsamında değerlendirilmiştir.

Yargıtay'ın İnternet bankacılığını kullanmak suretiyle başkasının hesabından para aktarılması şeklinde gerçekleşen fiili, bilişim sistemini kullanmak suretiyle hırsızlık suçu kapsamında değerlendirdiği kararda;

"Sanığın internet bankacılığı hizmetinden yararlanan yakınanın şifresini elde ederek hesap bilgilerine ulaştıktan sonra, G.Bankası G.Şubesi'nde bulunan hesabındaki 5.800.-YTL' yi oluşturduğu sahte kimliğe havale çıkarttığı, bu eyleminde sistemi engelleme, bozma, verileri yok etme veya değiştirmenin söz konusu olmadığı anlaşıldığından, (...) bilişim sisteminin kullanılması suretiyle işlenen hırsızlık suçunun, sanık tarafından yakınanın hesabından paranın başkası adına havale edilmesi anında tamamlandığı gözetilmeyerek, eylemin kalkışma aşamasında kaldığının kabul edilmesi...[329]*"* Görüldüğü üzere Yargıtay bu kararında bilişim sisteminin kullanılması suretiyle işlenen hırsızlık suçunun, sanık tarafından yakınanın hesabından paranın başkası hesabına havale edilmesi anında tamamlandığını kabul etmiştir.

Yargıtay'ın İnternet bankacılığını kullanmak suretiyle başkasının hesabından para aktarılması şeklinde gerçekleşen fiili, T.C.K.'nın 244. maddesinin 4. fıkrası kapsamında değerlendirdiği karar ise şu şekildedir;

"...Somut olayda ise; sanığın, katılanın G... Bankası 1. Levent Şubesi'nde bulunan hesabına internet bankacılığı yoluyla girip hesaptaki paradan 3.200.00 TL'yi G... Bankası Osmanbey Şubesi'ndeki 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

329 6. CD. 02.06.2008, 2008/555 E., 2008/12249 K. – UYAP Mevzuat Programı

unsurlarının da gerçekleşmediği eylemin, suç tarihinde yürürlükte bulunan 765 sayılı T.C.K.'nın 525/b (5237 sayılı T.C.K.' 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,[330]*''*

Yargıtay birçok kararında, şifrelerin kırılması veya verilerin değiştirilmesinin söz konusu olup olmadığını tartışma konusu yapmadan, internet üzerinden para aktarılması şeklinde gerçekleştirilen fiilleri T.C.K.'nın 244. maddesinin 4. fıkrası kapsamında değerlendirmekteydi[331]. Ancak Yargıtay Ceza Genel Kurulu (YCGK) 17.11.2009 tarihli yeni bir kararında, internet bankacılığı üzerinden bir hesaptan başka bir hesaba hukuka aykırı bir şekilde para aktarılmasına, nitelikli hırsızlık suçunu oluşturduğu yönünde karar verilmiştir. Şöyle ki[332],

"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 sisteminin 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 TCY'nın 142/2-e maddesinde düzenlenmiş bulunan 'bilişim sistemi kullanılmak suretiyle hırsızlık' suçunun gerçekleştiği kabul edilmelidir. Şu halde, sanığın eyleminin 5237 sayılı TCY'nın 142/2-e maddesindeki nitelikli hırsızlık suçunu oluşturduğunun kabul edilmesi karşısında; 244.maddenin 4.fıkrası uyarınca uygulama yapma olanağı da bulunmamaktadır." YCGK'nın vermiş olduğu bu karar oyçokluğu ile verilmiş bir karardır.

330 11. Ceza Dairesi 2009/1616 E.N., 2009/11328 K.N. – UYAP Mevzuat Programı

331 Başbüyük İsa, s.162

332 YCGK, 17.11.2009 tarih ve 2009/11-193 E., 2009/268 K - UYAP Mevzuat Programı

Tüm bu yukarıda değindiğimiz hususlardan sonra diyebiliriz ki bize göre, internet bankacılığı yoluyla hukuka aykırı olarak yapılan havale işlemi de bilişim sistemlerini kullanmak suretiyle hırsızlık suçu (T.C.K. m.142/2-e) değildir. Bu eylem bize göre bilişim sistemleri aracılığıyla yarar sağlama (T.C.K. m.244/4) suçunu oluşturur. Bu nedenle biz Yargıtay Ceza Genel Kurulu (YCGK)' nın oyçokluğu ile aldığı 17.11.2009 tarih ve 2009/11-193 Esas numaralı kararına katılmıyor, karara muhalif kalan üyelerin görüşlerine katılıyoruz. Yukarıda da belirttiğimiz üzere doktrindeki yazarların çoğunluğu da bizim gibi düşünmektedir[333].

İnternet yoluyla bir hesaptan başka bir hesaba para aktarılması şeklinde gerçekleşen fiillerin hırsızlık suçunu oluşturmadığı düşüncemizi aşağıdaki gerekçelerle açıklayabiliriz;

İlk olarak, hırsızlık suçunda korunan hukuki menfaat mülkiyet hakkıyla birlikte zilyetliktir. Mevduat sözleşmesinin hukuki niteliği gereği, bankayla yatırılan paranın maliki de zilyedi de banka olmakta; bu nedenle mudiinin bankaya yatırdığı para üzerinde hem mülkiyet hem de zilyetlik hakkı son bulmaktadır.[334] Bu sonuçtan yola çıktığımızda, bir kimsenin hesabındaki paranın alınması ile aynı kimsenin bankadan çekmiş olduğu paranın kişinin üzerinden herhangi bir şekilde hırsızlanmasını aynı şey olarak kabul etmememiz gerekir. Bir başka deyişle burada mudinin parası çalınmış olmaz, bankadaki verilerle oynama yapılarak bankadan haksız menfaat elde edilmiş olur.

İkinci olarak, internet bankacılığı ile yapılan banka havalesi ile üzerinde tasarrufta bulunulan şey ise maddi anlamda para değil; yalnızca maddi varlığı bulunmayan kaydi paradır,[335] yani soyut bir şeydir. Kanuni tanıma göre hırsızlık suçu, bir taşınır malın bulunduğu yerden alınması suretiyle işlenebilir. Yani cismani varlığı bulunmayan şeyler hırsızlık suçunun konusunu oluşturamaz. İnternet şubesinde yapılan banka havalesi ile havale edilen şey maddi anlamda verilerin temsil ettiği paralar taşınmamakta, gönderilmemekte ya da bulunduğu yerden alınmamakta, verilerin temsil ettiği paralar bilişim sisteminde var olmaya devam etmektedir. Kısacası, burada sadece veri transferi olmaktadır. Bilişim sistemi bilişim

333 Aynı görüş için bkz. Taşdemir Kubilay, s.291-295; Özen Muharrem/BAŞTÜRK İhsan, s.139; Başbüyük İsa, s.168 – 170; Yazicioğlu Yılmaz, s.144; Yildiz M. Emre, s. 145-149

334 Ayrıntılı bilgi için bkz. Başbüyük İsa, s.166-168

335 Ayrıntılı bilgi için bkz. Başbüyük İsa, s.166-168

sistemi kullanıldığı sürece üzerinde oynanılan her şey veridir.[336] T.C.K.'nın 244. maddesindeki bilişim suçu hırsızlık suçuna göre daha özel bir düzenleme oluşturmaktadır. Buna göre, haksız bir şekilde bir hesaptan başka bir hesaba para aktarılması şeklinde gerçekleşen fiiller bize göre hırsızlık suçunun konusunu oluşturmaz. Bu durumda hırsızlık ve dolandırıcılık suçları yerine daha özel bir norm olan T.C.K.'nın 244. maddesinde yer alan düzenleme düşünülmelidir. [337] Eğer bu şekilde transfer edilen parayı bir malvarlığı değeri olarak kabul edecek olursak T.C.K.'nın 244. maddesinin 3. ve 4. fıkralarında düzenlenen suçların hiçbir önemi kalmayacaktır.[338]

Yukarıdaki gerekçelerimizin yanında Yargıtay Ceza Genel Kurulu'nun (YCGK) 17.11.2009 tarih ve 2011-103/268 numaralı kararının gerekçesine baktığımızda şu hususları görmekteyiz. Yargıtay Ceza genel kurulu şahsın kastının hırsızlık yapmak olduğu üzerinde durmuştur. Ceza Genel Kurulu'na göre failin daha önce haksız bir şekilde elde etmiş olduğu internet bankacılığı şifresini kullanarak, katılana ait hesaptan, kendisi için açtırmış olduğu hesaba havale yapması eylemindeki kastı, katılanın hesabındaki verilerin temsil ettiği parayı mal edinmektir. Yine Yargıtay'a göre, failin bu eylemdeki kastı var olan verilerin başka bir yere gönderilmesi değildir.[339] Ancak şunu hemen belirtmek gerekir ki T.C.K.'nın 244. maddesinin 4. fıkrasında yer alan bilişim sisteminin işleyişine veya sistemdeki verilere müdahale yoluyla haksız çıkar sağlama suçunda da failin kastı sadece bilişim sisteminin işleyişine veya sistemdeki verilere müdahale etmek değil aynı zamanda haksız bir çıkar sağlamaktır. Bu madde metninde açıkça görülmektedir. Bu nedenle T.C.K.'nın 244. maddesinin 4. fıkrasında yer alan suç bakımından da failin kastı verilerin temsil ettiği paraları edinmek suretiyle yarar sağlamak olabilecektir. Kısaca, T.C.K.'nın 244. maddesinin 4. fıkrası başka bir suçun kapsamına girmeyen eylemler için uygulanan tali bir suç tipi olsa da internet bankacığı yoluyla hukuka aykırı olarak yapılan havale işleminin nitelikli hırsızlığın (T.C.K. m.142/2-e) kapsamına girmediğini düşünüyoruz. Zira transfer edilen şey soyut bir unsur olan veriden ibaret olup taşınır bir mal değildir. Bu eylemi T.C.K'nın 142/2-e maddesindeki nitelikli hırsızlık kapsamına sokarsak kanunun lafzı ile ve suç ve cezada kanunilik ilkesi ile

336 Özbek Veli Özer/Kanbur M.Nihat/Doğan Koray/Bacaksiz Pınar/Tepe İlker, s.925

337 Yildiz M. Emre, s.147

338 Özbek Veli Özer/Kanbur M.Nihat/Doğan Koray/Bacaksiz Pınar/Tepe İlker, s.925

339 Yildiz M. Emre, s.148-149

ters düşer diye düşünmekteyiz. Bu nedenle internet bankacığı yoluyla hukuka aykırı olarak yapılan havale işlemi bize göre, bilişim sistemleri aracılığıyla yarar sağlama suçuna (T.C.K. m.244/4) karşılık gelmektedir.

b. Bilişim Sistemlerinin Kullanılması Yoluyla İşlenen Dolandırıcılık Suçu

T.C.K.'nın 158. maddesinde dolandırıcılık suçunun nitelikli halleri düzenlenmektedir. maddenin 1.fıkrasının f bendinde ise, bu nitelikli hallerden sayılan bilişim sisteminin araç kullanılması yoluyla islenen dolandırıcılık suçu düzenlenmiştir.

T.C.K.'nın 158/1-f maddesi: "……Bilişim sistemlerinin, banka veya kredi kurumlarının araç olarak kullanılması suretiyle,……İşlenmesi hâlinde, iki yıldan yedi yıla kadar hapis ve beşbin güne kadar adlî para cezasına hükmolunur. Ancak, (e), (f) ve (j) bentlerinde sayılan hâllerde hapis cezasının alt sınırı üç yıldan, adlî para cezasının miktarı suçtan elde edilen menfaatin iki katından az olamaz."

Dolandırıcılık suçunu düzenleyen T.C.K.'nın 157. maddesinde açıkça görüldüğü üzere, suçun hareket unsurunu oluşturan hileli davranışın gerçek kişiye yapılmış olması gerekir. T.C.K.'nın 158/1-f maddesinde düzenlenen bilişim sistemi aracı kılınma suretiyle dolandırıcılık suçunun, T.C.K.'nın 244. maddesinin 4. fıkrası karşısında uygulama bulup bulamayacağı konusunda tartışma bulunmaktadır.

Doktrinde bazı yazarlar bilişim sistemleri aracılığıyla dolandırıcılık suçunun işlenemeyeceği kabul etmişlerdir. Bu yazarlara göre, dolandırıcılık suçunda hileli hareket bir kişiye yapılmalıdır. 158/1-f maddesinde düzenlenen suç bilişim sistemi üzerinden gerçekleştirilmektedir. Bu nedenle bilişim sistemini aracı kılma suretiyle dolandırıcılık suçunun, T.C.K.'nın 244. maddesinin 4. fıkrası karşısında uygulama alanı bulması mümkün değildir.[340]

Doktrinde bazı yazarlara göre ise, dolandırıcılık suçu bilişim sistemleri aracılığıyla işlenebilir, bu nedenle yerinde bir düzenlemedir. TCK'nın 244. maddesinin 4. fıkrası ile arasında fark bulunmaktadır, bilişim sistemleri ile de hile yapılabilir, mutlaka gerçek kişi ile yüz yüze gelmek gerekmez[341]

340 Özbek Veli Özer, s.1059

341 Ketizmen Muammer, s.180-183; Başbüyük, s.175'ten Doğan Koray, Bilişim Suçları Ve Türk Ceza Kanunu, Hukuku Ve Adalet Dergisi, Yıl:2, S:6-7, Ekim 2005, s.307; Bakici Sedat, "Ceza Hukuku Özel Hükümler" Cilt I, Adalet Yayınevi, Ankara, 2008, s.458, 459; TAŞDEMİR Kubilay, s.172 ; Taşkin Şaban Cankat, s.116-118

Yargıtay'ın bir kararında[342], *"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. Gerçek bir kişiyle karşı karşıya gelmeden, yüz yüze veya telefon, bilgisayar, bilgi geçer gibi bir başka vasıta kullanılarak görüşmeden, konuşmadan, hileli davranışlarla gerçek kişiler dolandırılmadan sadece bilişim sistemi kullanılarak doğrudan doğruya çıkar sağlanması halinde "bilişim sistemine girerek haksız çıkar sağlama suçu" gerçekleşecektir. Somut olayda oluşa uygun kabule göre; Kayseri PTT Müdürlüğü Otomasyon Bölümünde bilgisayar teknisyeni olarak görev yapan sanık M… Ö… Ö… ile Kayseri'de bulunan özel bir dershanede öğretmen olan diğer sanık A… K…'nın fikir ve eylem birliği içersinde hareket ederek, 2002 yılının Mayıs ve Eylül ayları arasında Sivas, İstanbul-Fatih, Beyazıt, Bağcılar, Zeytinburnu, Küçükçekmece, Sefaköy, Merter, Bayrampaşa, Aksaray, Mecidiyeköy, Avcılar ve Kağıthane, Ankara- Ulus, Kızılay, Ahmetler, Emek ve Keçiören PTT merkezlerinden kabul işlemi yapılan bir kısım para havaleleri tutarlarına, PTT on-line sistemi veri tabanına girilmek suretiyle rakam ilave edilerek ödeme merkezlerince, gerçekte havale edilenden 10 veya 100 kat fazla tutarda ödeme yapılmasını sağlayarak haksız menfaat temin eden sanıkların eylemlerinin tamamen bilişim ortamında gerçekleştirilmiş olması, gerçek kişiye karşı yöneltilen her hangi hileli bir davranışın bulunmaması nedeniyle 765 sayılı T.C.K..nun 525/b-2 maddesindeki (5237 sayılı T.C.K..nun 244/4 md) bilişim suçunu oluşturacağı gözetilmeden yazılı şekilde hüküm kurulması,"* diyerek hileli hareketin gerçek kişiye yöneltilmemesi durumunda T.C.K.'nın 244. maddesinin 4. fıkrasındaki suçun oluşacağını açıkça belirtmiştir. Yargıtay'ın bu yönde benzer başka kararları da bulunmaktadır[343].

342 Y 11. CD 12.10.2009 T. 2008/11060 E, 2009/11936 K. - UYAP Mevzuat Programı, Benzer diğer bir karar için bkz. 11. CD. 07.10.2009 T., 2009/1616 E., 2009/11328K.

343 11. CD. 27.01.2009 T., 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 dolandırıcılık suçunun unsurlarının bulunmadığı, fiilin 5237 sayılı T.C.K..nun 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," 11. CD. 22.01.2008 T., 2007/8423 E., 2008/117 K." Somut olayda; sanığın, katılan Mücahit S'in kimlik bilgilerine göre düzenlenip kendi fotoğrafı yapıştırılmış ele geçirilemeyen sahte nüfus cüzdanını kullanarak katılan A A.Ş.nin Yenigün Şubesi'nde hesap açtırarak diğer katılan Murat Ç'ın bankada bulunan para hesabındaki var olan verileri (bilgileri) sahte kimlikle açtırdığı hesaba internet yoluyla havale edip hesap cüzdanı ibraz ederek banka şubesinden çektiğinin iddia ve kabul olunması karşısında; eyleminin, paranın sanığın açtırdığı hesaba intikaline kadar katılan Murat Ç'a yöneltilmiş hile bulunmaması ve tamamen bilişim sistemi içinde gerçekleştirilmesi

Bize göre ise T.C.K.'nın 158/1-f maddesi yerinde bir düzenlemedir. T.C.K.'nın 244. maddesinin 4. fıkrası ile benzerlik gösterse de birbirinden çok farklıdır. Her iki maddede de haksız yarar elde edilmesi söz konusu olsa da T.C.K.'nın 158. maddede hileli davranış söz konusudur. Bilişim sistemi aracılığıyla gerçek kişiye karşı hileli davranışta bulunabilmesi mümkündür. Bu nedenle bilişim sistemi aracı kılınarak yarar sağlanmışsa T.C.K.'nın158/1-f maddesine söz konusu olurken bilişim sistemine karşı yapılan fiillerle yarar elde edilmesi durumunda T.C.K.'nın 244. maddesinin 4. fıkrası söz konusu olacaktır. Ayrıca T.C.K.'nın 244. Maddesindeki suçu oluşması için aynı maddenin 1 ve 2. fıkralarında yazılı eylemlerin gerçekleştirilmesi gerekir, T.C.K.'nın 158/1-f maddesi için ise böyle bir şey söz konusu değildir.

Örnekle açıklamaya çalışırsak, bir çalışanın fabrikanın veri tabanına müdahale etmek suretiyle, kendisine fazla mesai yapmış gibi göstererek fazla ücret alması durumunda T.C.K.'nın 244. maddesinin 4. fıkrasının uygulanması söz konusudur[344]. Çünkü burada iradesi fesada uğratılmış gerçek bir kişi bulunmamaktadır. T.C.K. 158/1-f maddesine örnek olarak ise günümüzde sıklıkla karşılaştığımız Facebook üzerinde yapılan dolandırıcılığı örnek gösterebiliriz. X, A kişisinin Facebook hesap şifresini öğrenerek A'nın hesabındaki arkadaşlarından kendisini A olarak tanıtıp, para talep eder ve A'nın arkadaşı da X'e para gönderirse X, T.C.K. madde 158/1-f'deki bilişim sistemlerini araç olarak kullanmak suretiyle dolandırıcılık suçunu işlemiş olur. Burada fail hileli hareketlerle gerçek kişiyi kandırmış bilişim sistemini ise sadece aracı kullanmıştır.

Günümüzde çok sık rastlanan bilişim sistemi aracılığıyla yapılan dolandırıcılığa bir başka örnek de şu şekildedir. Asıl amacı insanları dolandırmak olan fail internet sitesi açarak ürün satışı yapar, ürünlerin fiyatlarını da piyasa fiyatından daha aşağılarda tutarak cazip hale getirir. Mağdur, ürünün ücretini yatırmasına rağmen ürün gelmez ya da boş bir kutu veya içinde oyuncak bir saat olan bir kutu gönderilir.

T.C.K.'nın 158/1-f maddesi, banka veya kredi kurumlarının araç olarak kullanılması suretiyle dolandırıcılığı da bilişim sistemi aracılığıyla dolandırıcılık suçuyla beraber düzenlemiştir. Bu hususa "Banka ve Kredi Kartlarının Kötüye

---

nedeniyle 5237 sayılı T.C.K.. nun 244/4 maddesine uyan suçu oluşturduğu gözetilmeden, vasıflandırılmada yanılgıya düşülerek unsurları oluşmayan banka aracı kılınmak suretiyle nitelikli dolandırıcılık suçundan mahkûmiyet hükmü kurulması,"

344 Başbüyük İsa., s. 177,178

Kullanılması Suçu" başlığı altında değinilmiştir. Burada tekrar belirtmek isteriz ki T.C.K.'nın 245. maddesi ile T.C.K.'nın157. ve 158. maddesi arasında tüm fıkralar için gerçek içtima kuralları uygulanır. Bileşik suç söz konusu değildir. Ancak, aksini düşünen bazı yazarlar T.C.K.'nın 245. maddesinin 3. fıkrasındaki 'teki düzenlemeyi ayrı tutmaktadır, maddede "fiil daha ağır cezayı gerektiren başka bir suç oluşturmadığı takdirde" denildiği için T.C.K. madde 245/3'teki suç ile T.C.K. madde 158/1-f'de düzenlenen nitelikli dolandırıcılıkla beraber söz konusu olduğunda daha ağır ceza içeren olan T.C.K. 245/3'ten ceza verileceğini savunmaktadırlar[345].

c. Haberleşmenin Engellenmesi Suçu[346]

Bu suç ile kişiler arasındaki haberleşmenin hukuka aykırı olarak engellenmesi hususu düzenlenmiştir. Suçun oluşumunda önemli olan kişiler arasındaki haberleşmenin hukuka aykırı olarak engellenmiş olmasıdır.

Günümüzde internet üzerinden haberleşme aşırı yaygınlaşmıştır. Bu nedenle bu suç suçun bilişim sistemleri aracılığıyla da islenebilir. Maddenin üçüncü fıkrasındaki *"her türlü yayın organı"* ifadesinden denilerek de bilişim sistemi kapsama sokulmuştur. Çünkü internetten artı her türlü yayın yapmak mümkündür.

5237 sayılı T.C.K.'nın 124. maddesi, 765 Sayılı T.C.K.'nın 391. maddesinin[347] karşılığıdır. Ancak 765 sayılı T.C.K.'da, yalnızca, telefon, telgraf veya telsiz iletişimin engellenmesi suç olarak düzenlenmiştir. Buna göre, internet iletişiminin engellenmesi suç oluşturmayacaktır. Yeni kanun bu konuda çıkabilecek tartışmaları engellemiştir.

Maddedeki suçun oluşumu bakımından hukuka özel aykırılık aranacaktır[348].

345 Başbüyük İsa, s. 187

346 T.C.K. madde 124 "[1] Kişiler arasındaki haberleşmenin hukuka aykırı olarak engellenmesi hâlinde, altı aydan iki yıla kadar hapis veya adlî para cezasına hükmolunur.

[2] Kamu kurumları arasındaki haberleşmeyi hukuka aykırı olarak engelleyen kişi, bir yıldan beş yıla kadar hapis cezası ile cezalandırılır.

[3] Her türlü basın ve yayın organının yayınının hukuka aykırı bir şekilde engellenmesi hâlinde, ikinci fıkra hükmüne göre cezaya hükmolunur."

347 765 Sayılı T.C.K. md 391 –İletişim ve Enerji Nakil Vasıtalarına Karsı Suçlar : "(1) Bir kimse, telgraf, telefon veya telsiz makinalarına veya alat ve edevatına veya tellerine zarar verir veya elektrik ceryanlarının dağılmasına sebep olur veya her ne suretle olursa olsun telgraf veya telefon veya telsiz muhaberat ve nesriyatını inkıtaa uğratırsa bir seneden bes seneye kadar hapis cezasıyla cezalandırılır."

348 Taşkin Şaban Cankat, s.115

d. Hakaret Suçu[349]

5237 sayılı T.C.K. ile 765 Sayılı T.C.K. dönemindeki hakaret ve sövme ayrımı kaldırılmıştır.

Hakaret suçunun bilişim sistemi aracılığıyla işlenmesi mümkündür. Özellikle maddenin ikinci fıkrası dikkate alındığında bilişim sitemi ile yakın ilişkili olduğu görülecektir.

Maddenin ikinci fıkrasına göre, Örneğin, mağdura yönelik hakaretamiz bir ileti (e-posta, sms, mms vb.) gönderilmesi durumunda suç islenmiş olacaktır.

Ayrıca, bilişim sisteminde işlenen bazı hakaret suçları, maddenin 4. fıkrasında düzenlenen alenen hakaret kapsamına girebilir. Örneğin, herkesin internete girerek görebileceği haber sitesinin altına hakaret içerikli yazılar yazılması veya şahsın herkese açık olan facebook profil sayfasına hakaret içerikli sözler yazılması durumunda hakaret suçu alenen işlenmiş olacaktır. Yargıtay'ın 04.03.2014 Tarih 2013/1791 Esas 2014/4946 Karar sayılı hükmünde "Oluşa, katılanın aşamalardaki anlatımlarına, sanığın babası adına kayıtlı telefona bağlı internet hesabından katılana ait elektronik posta hesabına girildiğine ilişkin Microsoft şirketinden gelen yazı yanıtlarına, Türk Telekom Müdürlüğünün yazılarına, katılanın şikayeti sırasında ibraz ettiği ekran çıktılarına ve tüm dosya kapsamına göre; katılana ait elektronik posta ve facebook hesaplarının şifresini ele geçirerek bu adreslere giren, facebook hesabındaki özel fotoğraflarını alarak ve şifreyi değiştirmek suretiyle katılanın anılan hesaplara erişimini engelleyen, daha sonra oluşturduğu Ayşe Hekim isimli hesaba katılanın fotoğraflarını koyarak "Bandırma o...su Gizem A...'ı tanıyanlar buraya" "Bandırma'nın o..nu iyi tanıyın" şeklinde yazılar yazan sanığın, eylemine uyan T.C.K..nun 244/2 ve 125/2. madde yollamasıyla 125/1. maddesi

---

349 T.C.K. madde 125: "[1] (8.7.2005 T. 5377 sk değ.) Bir kimseye onur, şeref ve saygınlığını rencide edebilecek nitelikte somut bir fiil veya olgu isnat eden veya sövmek suretiyle bir kimsenin onur, şeref ve saygınlığına saldıran kişi, üç aydan iki yıla kadar hapis veya adlî para cezası ile cezalandırılır. Mağdurun gıyabında hakaretin cezalandırılabilmesi için fiilin en az üç kişiyle ihtilât ederek işlenmesi gerekir.(Sulh Ceza)

[2] Fiilin, mağduru muhatap alan sesli, yazılı veya görüntülü bir iletiyle işlenmesi hâlinde, yukarıdaki fıkrada belirtilen cezaya hükmolunur.

[3] Hakaret suçunun;

a) Kamu görevlisine karşı görevinden dolayı,

b) Dinî, siyasî, sosyal, felsefi inanç, düşünce ve kanaatlerini açıklamasından, değiştirmesinden, yaymaya çalışmasından, mensup olduğu dinin emir ve yasaklarına uygun davranmasından dolayı,

c)Kişinin mensup bulunduğu dine göre kutsal sayılan değerlerden bahisle, İşlenmesi hâlinde, cezanın alt sınırı bir yıldan az olamaz.

4] (8.7.2005 T. 5377 sk değ.) Hakaretin alenen işlenmesi halinde ceza altıda biri oranında artırılır.

[5] (8.7.2005 T. 5377 sk değ.) Kurul hâlinde çalışan kamu görevlilerine görevlerinden dolayı hakaret edilmesi hâlinde suç, kurulu oluşturan üyelere karşı işlenmiş sayılır. Ancak, bu durumda zincirleme suça ilişkin madde hükümleri uygulanır."

uyarınca cezalandırılmasına karar verilmesi gerekirken, yazılı gerekçeyle beraat hükümleri kurulması,[350]" denilmiştir.

e. Müstehcenlik Suçu

5237 sayılı T.C.K.'nın topluma karsı suçlar baslıklı üçüncü kısmının genel ahlaka karsı suçlar baslıklı yedinci bölümünde yer alan 226. maddesinde "müstehcenlik suçu" düzenlenmiştir. Bu suç tipi de bilişim sistemleri aracılığıyla islenebilen suçlardandır. Başka bir ifade ile bu maddede tanımlanan birçok suçu oluşturan hareketlerin, bilişim sistemleri vasıtasıyla gerçekleştirilmesi mümkündür.

Özellikle maddenin ikinci fıkrasında, müstehcen görüntü, yazı veya sözlerin basın ve yayın yolu ile yayınlanması veya yayınlanmasına aracılık edilmesi ve beşinci fıkrasında, maddenin üçüncü ve dördüncü fıkralarındaki suçların konusunu oluşturan ve müstehcenlik bakımından mutlak yasak kapsamına giren ürünlerin içeriğinin basın ve yayın yoluyla yayınlanması veya yayınlanmasına aracılık edilmesi ya da çocukların görmesinin, dinlemesinin veya okumasının sağlanması hallerinde, müstehcenlik suçu bilişim sistemleri kullanılmak suretiyle gerçekleşmiş olacaktır. Örneğin, fail cinsel organının fotoğrafını arkadaşlarına elektronik posta vasıtasıyla gönderirse, failin bu eylemi T.C.K.'nın 226. maddesi kapsamında kalacaktır. Aynı şekilde, şiddet kullanılarak, hayvanlarla, ölmüş insan bedeni üzerinde, doğal olmayan yoldan veya çocukların kullanıldığı görüntüleri harddisk, USB vb, cihazlara depolayan, bunları internet ortamında yayınlayan veya yayn kişinin eylemi de T.C.K.'nın 226. maddesi kapsamında kalacaktır. Yargıtay'ın bir kararında[351] *"Tespit edilen pornografik video görüntülerinden birinde çocuk kullanıldığı, diğerlerinde doğal olmayan yoldan yapılan cinsel davranışlara yer verildiği, müstehcen görüntülerin miktarına, niteliğine ve kayıt biçimine göre uzun süre içerisinde ve kasten yapıldığı anlaşılan "çocuk pornografisi ve doğal olmayan yoldan yapılan cinsel davranışlara ilişkin video kaydını dijital ortamda depolama ve bulundurma" fiilinin kişisel amaçlı dahi olsa 5237 sayılı T.C.K.'nın 226/3. maddesinde tanımlanan müstehcenlik suçunu oluşturacağı gözetilmeden, sanığın bu suçtan beraatine karar verilmesi isabetsiz"* denilmiştir.

Müstehcenlik suçunu sadece bilişim sistemiyle işlenebileceğini, maddenin de bilişim sistemi aracılığıyla kullanılmasını cezai yaptırıma bağladığına değinmiş

350 UYAP Mevzuat Programı

351 Y. 12. CD. 17.06.2013 T., 2012/20606 E., 2013/16477 K. - UYAP Mevzuat Programı

olduk. Burada bu hususlarla yetineceğiz. Maddede belirtilen eylemleri incelemeyeceğiz. Çünkü müstehcenlik suçu başlı başına bir tezin konusunu oluşturacak kadar geniş kapsamlı bir konudur.

f. Kumar Oynanması için Yer ve İmkân Sağlama Suçu

5237 sayılı T.C.K.'nın 228. maddesinde düzenlenmiştir. Bu suç tipi de bilişim sistemleri aracılığıyla islenebilecektir. İnternette sanal gazino siteleri bulunmaktadır. Buradan kumar oynatılması durumunda, unsurları oluştuğu takdirde 5237 sayılı T.C.K.'nın 228. maddesi uyarınca ceza verilmesi mümkün olacaktır. Futbol veya diğer spor müsabakaları ile ilgili yasal olmayan oyunların internet üzerinden oynatılması durumunda ise fail, 7258 sayılı Futbol Ve Diğer Spor Müsabakalarında Bahis Ve Şans Oyunları Düzenlenmesi Hakkında Kanun'a göre cezalandırılacaktır.

SONUÇ

Türk Ceza Kanunu'nda düzenlenen bilişim suçlarını çalışmamız incelerken bazı konuların tartışmalı olduğunu söyledik. Tartışmalı olan konularla ilgili önerilerimizi aşağıda sunuyoruz.

Bilişim sistemine girme ve kalmaya devam etme suçu ile ilgili olarak, T.C.K.'nın 243. maddesinin 1. fıkrasının metninde, giren "ve" kalmaya devam eden ibaresi kullanılmaktadır. Kanunkoyucu, kötü niyet taşımayıp kısa süreliğine sisteme girenleri cezalandırmak istememiştir Ancak maddedeki "ve" ibaresinin "veya" olarak değiştirilmesi gerektiğini düşünmekteyiz. Böylece, bilişim sistemine girme bizatihi suç olmalıdır. Bir başkasının modem şifresini kırarak internetten rıza dışı yararlanma da bu maddeye göre cezalandırılmalı, bu hususun bu madde kapsamına girip girmediği tartışmaları sonlandırılmalıdır.

Banka ve kredi kartlarının kötüye kullanılması suçu ile ilgili, banka ve kredi kartlarının kötüye kullanılması suçunun hukuksal değerinin çoğunluk görüşüne göre kişinin malvarlığı olduğu kabul edildiğinden bilişim alanında suçlar bölümünde düzenlenmesi eleştirilmektedir. Bu nedenle, bu suçun malvarlığına karşı suçlar bölümünde yer almasının kanunu sistematiğine daha uygun düşeceğini ve ayrıca, T.C.K.'nın 245 maddesinin 3. fıkrasının müstakil bir suç olarak değil, 2. fıkradaki suçun ağırlaştırıcı sebebi olarak düzenlenmesi gerektiğini düşünmekteyiz. Kartlara "çip" diye tabir edilen aparatın takılarak "şifre girme" uygulamasına geçilmesi bu suçun işlenme oranını düşürmüş, olumlu bir uygulama olmuştur.

T.C.K.'nın 142/2-e maddesinde düzenlenen bilişim sistemi aracı kılınma suretiyle hırsızlık suçunun, T.C.K.'nın 244. maddesinin 4. fıkrası karşısında uygulama bulup bulamayacağı konusunda tartışma bulunduğuna değinmiştik. Bilişim sistemlerinin kullanılması suretiyle hırsızlık suçunda çalışmamızda da belirttiğimiz üzere, internet bankacılığı aracılığıyla hukuka aykırı bir şekilde bir hesaptan başka bir hesaba havale yapılmasına ilişkin fiillerin de bilişim yolu suretiyle nitelikli hırsızlık suçunu oluşturmadığını, bilişim sistemleri aracılığıyla yarar sağlama suçu oluşturduğunu düşünmekteyiz. Bu düşüncemiz, Yargıtay Ceza Genel Kurulu (YCGK)' nın oyçokluğu ile aldığı 17.11.2009 tarih ve 2009/11-193 Esas numaralı

kararına ters düşmektedir ancak bu kararın oy çokluğu ile alınan bir karar olduğu bizim gibi düşünen üyelerin var olduğu gözden kaçırılmamalıdır. Muhalif kalan üyelerin gerekçeleri bize daha uygun düşmektedir. Çünkü bu eylemi bilişim yolu suretiyle hırsızlık suçu olarak kabul edersek suçta ve cezada kanunilik ilkesini görmemiş oluruz diye düşünmekteyiz. Ancak burada hemen şunu belirtmeliyiz ki, İnternet bankacılığı aracılığıyla hukuka aykırı bir şekilde bir hesaptan başka bir hesaba havale yapılması ve paranın çekilmesi eylemi ile ilgili daha önceden enerjinin taşınır sayılması hususu gibi özel düzenleme yapılması gerektiğini düşünmekteyiz. Böyle bir düzenleme olursa tartışmalar son bulacak ve kafa karışıklıkları ortadan kalkacaktır.

T.C.K.'nın 158/1-f maddesinde düzenlenen bilişim sistemi aracı kılınma suretiyle dolandırıcılık suçunun, T.C.K. T.C.K.'nın 244. maddesinin 4. fıkrası karşısında uygulama bulup bulamayacağı konusunda tartışma bulunduğuna değindik. Bize göre T.C.K.'nın 158/1-f maddesi yerinde bir düzenlemedir. T.C.K. madde T.C.K.'nın 244. maddesinin 4. fıkrası ile benzerlik gösterse de birbirinden çok farklıdır. Her iki maddede de haksız yarar elde edilmesi söz konusu olsa da T.C.K.'nın 158. maddesinde hileli davranış söz konusudur. Bilişim sistemi aracılığıyla gerçek kişiye karşı hileli davranışta bulunabilmesi mümkündür. Bu nedenle bilişim sistemi aracı kılınarak yarar sağlanmışsa T.C.K.'nın 158/1-f maddesi söz konusu olurken bilişim sistemine karşı yapılan fiillerle yarar elde edilmesi durumunda T.C.K.'nın 244. maddesinin 4. fıkrası söz konusu olacaktır. Ayrıca T.C.K.'nın 244. maddesindeki suçu oluşması için aynı maddenin 1 ve 2. fıkralarında yazılı eylemlerin gerçekleştirilmesi gerekir, T.C.K.'nın 158/1-f maddesi için ise böyle bir şey söz konusu değildir.

Bilişim sistemleri ve özellikle sistemin sonucu olarak karşımıza çıkan internet kullanımı hızla tüm dünyaya yayılmıştır. İnsanlar gündelik yaşamlarında yaptıkları her şeyi artık internetten yapabilmektedir, tabii bunu yaparken de kendilerine ait özel hayatlarına ilişkin bir çok konuyu sistemle paylaşmaktadırlar. İnsanlar bilişim karşısında daha bir savunmasızdır. Bu nedenle çıkarılması düşünülen Kişisel Verilerin Korunması Hakkındaki Kanun da bir an önce çıkarılmalıdır.

Kişilerin özel hayatları ile ilgili düzenlemeler ulusal bazda kalmamalı, uluslar arası bir çalışma ile düzenlenmelidir. İnternet ile artık sınırlar kalkmıştır. Konulan kurallara tüm ülkeler riayet etmelidir. Özel hayatın gizli tutulması tüm insanlığı

ilgilendirir. Bir başka deyişle etkin mücadelenin ulusal düzenlemelerden ziyade uluslararası işbirliği ve sözleşmelerle mümkün olabileceğini düşünmekteyiz.

KAYNAKLAR

Akbulut, Berrin *Türk Ceza Hukukunda Bilişim Suçları*, Yayımlanmamış Doktora Tezi, Selçuk Üniversitesi, Sosyal Bilimler Enstitüsü, Konya,1999

Albayrak, Mustafa (Eylül 2010) *Notlu-Atıflı-Uygulamalı Türk Ceza Kanunu (Öz Kitap)*, Adalet Yayınevi, Ankara

Aslan Hüryaşa Bilgisayar Yazılımı, Ünite 3 http://w2.anadolu.edu.tr/aos/kitap/IOLTP/2276/unite03.pdf Erişim Tarihi 01.02.2013

Avşar, B. Zakir/Öngöre, Gürsel *Bilişim Hukuku*, İstanbul, 2010 http://www.tbb.org.tr/Dosyalar/Yayinlar/Dokumanlar/BILISIM_HUKUKU.pdf Erişim Tarihi 01.02.2013

Başalp, Nilgün (2004) *Kişisel Verilerin Korunması Ve Saklanması*, Yetkin Yayınevi, Ankara

Başbüyük, İsa (Aralık 2010) *Hırsızlık Ve Dolandırıcılık Suçlarının Bilişim Sistemlerinin Araç Olarak Kullanılması Suretiyle İşlenmesi,* Ceza Hukuku Dergisi, Sayı: 14, Seçkin Yayıncılık

Bakıcı, Sedat (2008) *Ceza Hukuku Özel Hükümler Cilt I*, Adalet Yayınevi, Ankara,

Bakıcı, Sedat/Yalvaç, Gürsel (2008) *Ceza Hukuku Özel Hükümler Cilt II*, Adalet Yayınevi, Ankara

Boğa, Uğur (2011) *Bilişim Suçlarıyla Mücadele Yöntemleri, Uzmanlık Tezi, Radyo Ve Televizyon Üst Kurulu,* Ankara, http://www.rtuk.org.tr/upload/UT/48.pdf Erişim Tarihi 01.10.2013

BUDAK Mesut (18-22 Mart 2013) Hakimler Ve Savcılar Yüksek Kurulu (HSYK) Bilişim Hukuku Semineri, www.hsyk.gov.tr

Demircan, Tunç (2007) *Bilişim Alanında Suçlar*, Yüksek Lisans Tezi, Selçuk Üniversitesi Sosyal Bilimler Enstitüsü, Konya,

Dilek, Halil İbrahim (2007) *Bilişim Suçları Ve Türk Hukuk Sistemindeki Yeri*, Yüksek Lisans Tezi, Dicle Üniversitesi, Sosyal Bilimler Enstitüsü, Diyarbakır,

Dülger, Murat Volkan (2004) *Bilişim Suçları*, Ankara

Ercan, İsmail (Ağustos 2008) *Ceza Hukuku; Genel Hükümler - Özel Hükümler*, 4. Bası, İkinci Sayfa Yayınları, İstanbul

Erdem, Mustafa Ruhan *Türk Ceza Kanunu'nda Malvarlığına Karşı Suçlar, (Makale)*, www.ceza-bb.adalet.gov.tr/makale/119.doc Erişim Tarihi:11.10.2012

Esen, Sinan (Eylül 2007) *Anlatımlı Ve İçtihatlı Malvarlığına Karşı Suçlar, Belgelerde Sahtecilik Ve Bilişim Alanından Suçlar*, Adalet Yayınevi, Ankara

Ergüç, Seher (2008) *Türk Bankacılık Sisteminde İnternet Bankacılığı İle Yapılan Dolandırıcılıklar Ve Bilişim Suçları Hukuku*, Yüksek Lisans Tezi, Kadir Has Üniversitesi, Sosyal Bilimler Enstitüsü, İstanbul

Gümüş, Çetin (2008) *Bilişim Suçlarıyla Mücadelede Polisin Eğitimi,* Doktora Tezi, Fırat Üniversitesi, Fen Bilimleri Enstitüsü, Elazığ

Gündel, Ahmet (Eylül 2005) *Hırsızlık Ve Dolandırıcılık Suçları*, Seçkin Yayıncılık, Ankara

Gündüz, Muhammet Zekeriya (Ocak 2013) *Bilişim Suçlarına Yönelik IP Tabanlı Delil Tespiti,* Yüksek Lisans Tezi, Fırat Üniversitesi, Fen Bilimleri Ensititüsü

Güngör, Necmi Murat (2007) *Yeni Türk Ceza Kanunu Kapsamında Bilişim Suçları Ve Emniyet Genel Müdürlüğü Uygulamaları*, Yüksek Lisans Tezi, İstanbul Üniversitesi Sosyal Bilimleri Enstitüsü, İstanbul

Hakimler ve Savcılar için Siber Suçlar Eğitimine Giriş, Oturum 1.3.2 & 1.3.3, Elektronik Delil, www.hsyk.gov.tr

Kaban, Mater/Aşaner, Halim/Güven, Özcan/Yalvaç Gürsel (Eylül 2001) Yargıtay Ceza Genel Kurul Kararları; Eylül 1996 – Temmuz 2001, Adalet Yayınevi, Ankara

Karagülmez, Ali (2011) *Bilişim Suçları Ve Soruşturma-Kovuşturma Evreleri,* 3. Baskı, Seçkin Yayınları, Ankara

Ketizmen, Muammer (2006) *Türk Ceza Hukuku`nda Bilişim Suçları,* Doktora Tezi, Ankara Üniversitesi, Sosyal Bilimler Enstitüsü, Ankara

Kızıltan, Mehmet Burak (2007) *5237 Sayılı Türk Ceza Kanununda Bilişim Sistemine Girme, Sistemi Engelleme Ve Bozma Suçları*, Yayımlanmış Yüksek Lisans Tezi, İstanbul Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul

Kurt, Levent (2005) *Açıklamalı-İçtihatlı Tüm Yönleriyle Bilişim Suçları ve Türk Ceza Kanunundaki Uygulaması*, Seçkin Yayıncılık, Ankara

Meran Necati (Eylül 2005) *Yeni Türk Ceza Kanununda Sahtecilik-Malvarlığı Bilişim Suçları İle Ekonomi Ve Ticaret Alanındaki Suçlar,* 1. Baskı, Seçkin Yayıcılık, Ankara

Nacar, Fatma Burcu (2010) *Avrupa Birliği Ülkeleri Ve Türkiye"de Bilişim Suçlarının Ceza Hukukundaki Uygulamaları,* Atılım Üniversitesi Sosyal Bilimler Enstitüsü, Ankara

Oğuzhan Kemal/Seliçi Özer/Oktay Özdemir Saibe (2006) *Eşya Hukuku*, 11. Baskı, Filiz Kitabevi, İstanbul

Özbek, Veli Özer (2007) *Banka Ve Kredi Kartlarının Kötüye Kullanılması Suçu*, Dokuz Eylül Hukuk Fakültesi Dergisi, Cilt 9

Özbek, Veli Özer/Kanbur, M. Nihat/Doğan, Koray/Bacaksız, Pınar/Tepe, İlker (Ekim 2010) *Türk Ceza Hukuku; Özel Hükümler*, Seçkin Yayıncılık, Ankara

Özdilek Ali Osman (2002) *Bilgisayar Suçları Ne Kadar Ciddi*, Montreal

Özen, Muharrem/Baştürk, İhsan (Ekim, 2011) *Bilişim İnternet Ve Ceza Hukuku*, Adalet Yayınevi, Ankara

Özgenç, İzzet (Ocak 2006) *Türk Ceza Kanunu Gazi Şerhi (Genel Hükümler)* , 3. Bası, Adalet Bakanlığı Eğitim Dairesi Başkanlığı, Ankara

Öztan, Fırat (Kasım 2008) *Fikir Ve Sanat Eserleri Hukuku*, Turhan Kitabevi, Ankara

Parlar, Ali/Hatipoğlu, Muzaffer (Nisan 2010) *5237 sayılı T.C.K.'da Özel Ve Genel Hükümler Bakımında Sulh Ceza Davaları*, Adalet Yayınevi, Ankara

Pallı, Hayati (Kasım 2008) *Türk Hukukunda Ve Mukayeseli Hukukta Bilişim Suçları,* Yüksek Lisans Tezi, Kayseri

Parlar, Ali/Hatipoğlu, Muzaffer (2006) *5237 Sayılı Yeni Türk Ceza Kanunu"nda Malvarlığına Karşı İşlenen Suçlar,* Kartal Yayınları, Ankara

Parlar, Ali (Ocak, 2011) *Türk Ceza Hukukunda Bilişim Suçları*, Bilge Yayınevi, Ankara

Polat, Halil (Eylül 2009,) *Teori Ve Uygulamada Cumhuriyet Savcısının El Kitabı*, Ankara,

Soyaslan, Doğan (2005) *Ceza Hukuku Genel Hükümler* 3. bası, Yetkin Yayınları, Ankara

Soyaslan, Doğan (2005) *Ceza Hukuku Özel Hükümler* 5. bası, Yetkin Yayınları, Ankara

Tanrıkulu Cengiz (*18-22 Mart 2013*) *Hakimler Ve Savcılar Yüksek Kurulu (HSYK) Bilişim Hukuku Semineri*, www.hsyk.gov.tr Erişim Tarihi: 01.06.2013

Taş, Kezban Atalıç (2010) *Bilişim Suçları Ve Adana İlinde 2006-2009 Yılları Arasında Meydana Gelen Bilişim Suçlarının Değerlendirilmesi,* Yüksek Lisans Tezi, Çukurova Üniversitesi Sağlık Bilimleri Enstitüsü Adli Tıp Anabilim Dalı, Adana

Taşdemir, Kubilay (2009) *Bilişim, Banka Veya Kredi Kartlarının Kötüye Kullanılması Ve Dolandırıcılık Suçları*, Cantekin Matbaacılık, Ankara, Temmuz

Taşkın, Şaban Cankat (Kasım 2008) *Bilişim Suçları,* 1. Bası, Beta Yayıncılık, İstanbul,

Tataroğlu, Bahadır (*18-22 Mart 2013*) *Hakimler Ve Savcılar Yüksek Kurulu (HSYK) Bilişim Hukuku Semineri,* www.hsyk.gov.tr Erişim Tarihi: 01.06.2013

Tezcan Durmuş/Erdem Mustafa Ruhan/Önok Rıfat Murat (2007) *Teorik Ve Pratik Ceza Özel Hukuku* 5. Bası, Seçkin Yayınevi, Ankara

Toroslu, Nevzat (Ekim 2005) *Ceza Hukuku; Özel Kısım*, 1. Baskı, Savaş Yayınevi, Ankara,

Toroslu, Nevzat (Şubat 2005) *Ceza Hukuku*, 7. Baskı, Savaş Yayınevi, Ankara,

Tulum, İsmail (2006) *Bilişim Suçları İle Mücadele*, Yüksek Lisans Tezi, Isparta

Yayla, Mehmet (2004) *Uluslararası Platformlarda ve Türkiye'de Bilişim Suçları, Ankara İl Jandarma Komutanlığında Alan Çalışması,* Yayımlanmamış Yüksek Lisans Tezi, Ankara

Yazıcıoğlu, Yılmaz (2004) *Bilişim Suçları,* Hukuki Perspektifler Dergisi, Sayı 2

Yazıcıoglu Yılmaz (1997) *Bilgisayar Suçları, Krimonolojik Sosyolojik ve Hukuki Boyutları ile*, 1. Baskı, İstanbul, Alfa Basım Yayım Dağıtım

Yıldız, M. Emre (Aralık 2010) *İnternet Bankacılığı Hakkında Yargıtay"ın 17.11.2009. Tarih, 2009/11-193 Esas Sayılı Kararının İncelenmesi*, Ceza Hukuku Dergisi, Seçkin Yayıncılık, Aralık 2010

Yılmaz, Sacit *5237 Sayılı T.C.K.'nın 244. maddesinde Düzenlenen Bilişim Alanındaki Suçlar*, http://tbbdergisi.barobirlik.org.tr/m2011-92-669

Ansiklopediler,
Büyük Larousse, Sözlük Ve Ansiklopedisi, Milliyet Gazetecilik A.Ş.

İçtihat ve Mevzuat Programları
Uyap Mevzuat Programı
Açıklamalı Kanun - İçtihat Programı (Akip), 2010

Web Adresleri

Bilişim Terimleri Sözlüğü, Http://Tdkterim.Gov.Tr/Bts/
Güncel Türkçe Sözlük, Http://Tdkterim.Gov.Tr/Bts/
Türk Dil Kurumu Web Sitesi, Www.Tdk.Gov.Tr
Türkiye Barolar Birliği, Http://Tbbdergisi.Barobirlik.Org.Tr
VİKİPEDİ, Özgür Ansiklopedi, Http://Tr.Wikipedia.Org
www.hukuki.net
http://www.adali.net
http://ekonomi.haberturk.com