T.C.
ATILIM ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
AVRUPA BİRLİĞİ ANABİLİM DALI
YÜKSEK LİSANS TEZİ

AVRUPA BİRLİĞİ ÜLKELERİ VE TÜRKİYE'DE BİLİŞİM SUÇLARININ CEZA HUKUKUNDAKİ UYGULAMALARI

Fatma Burcu NACAR

TEZ DANIŞMANI
Prof. Dr. Bülent OLCAY

Ankara, 2010

Atılım Üniversitesi Sosyal Bilimler Enstitüsü Müdürlüğüne

Fatma Burcu Nacar tarafından hazırlanan **"Avrupa Birliği Ülkeleri ve Türkiye'de Bilişim Suçlarının Ceza Hukukundaki Uygulamaları"** başlıklı bu çalışma 14.01.2010 tarihinde yapılan savunma sınavı sonucunda Oybirliği ile başarılı bulanarak jürimiz tarafından Avrupa Biriliği Anabilim Dalında Yüksek Lisans Tezi olarak kabul edilmiştir.

Jüri Başkanı
Prof. Dr. Yılmaz Özkan

Danışman
Prof. Dr. Bülent OLCAY

Üye
Yrd. Doç. Ahmet Ersen

Atılım Üniversitesi Sosyal Bilimler Enstitüsü Müdürlüğüne

Fatma Burcu Nacar tarafından hazırlanan **"Avrupa Birliği Ülkeleri ve Türkiye'de Bilişim Suçlarının Ceza Hukukundaki Uygulamaları"** başlıklı bu çalışma 14.01.2010 tarihinde yapılan savunma sınavı sonucunda Oybirliği ile başarılı bulanarak jürimiz tarafından Avrupa Biriliği Anabilim Dalında Yüksek Lisans Tezi olarak kabul edilmiştir.

Jüri Başkanı
Prof. Dr. Yılmaz Özkan

Danışman
Prof. Dr. Bülent OLCAY

Üye
Yrd. Doç. Ahmet Ersen

ÖNSÖZ

Tezimizde Türk Ceza Kanunu'ndaki ve bazı özel kanunlardaki bilişim suçları anlatılmış Avrupa Siber Suçlar Sözleşmesindeki Uluslararası Sözleşmelerdeki düzenlemeler ve Karşılaştırmalı Hukuk'taki durum değerlendirilmiş, tartışılmıştır.

Tezimin oluşumunda desteğini ve fikirlerini esirgemeyen, kendisine rahatlıkla ulaşma imkanı tanıyan çok iyi bir şekilde rehberlik eden Tez Danışmanım Prof. Dr. Bülent Olcay'a teşekkür ederim.

Tez Jürimde bulunan Jüri Başkanı Prof. Dr. Yılmaz Özkanve Jüri Üyesi Yrd. Doç. Ahmet Ersen Özsoy'a tez savunmam sırasında bana verdikleri değerli fikirleri nedeniyle teşekkür ederim.

Fatma Burcu NACAR

İÇİNDEKİLER

KISALTMALAR

ABD : Amerika Birleşik Devletleri

AİHM : Avrupa İnsan Hakları Mahkemesi

AİHS : Avrupa İnsan Hakları Sözleşmesi

ATM : Automatic Teller Machine

AÜSBFD : Ankara Üniversitesi Siyasal Bilgiler Fakültesi Dergisi

Bkz. : Bakınız

BM : Birleşmiş Milletler

C : Cilt

CD : Compact Disc

CD : Ceza Dairesi

CGK : Ceza Genel Kurulu

CMK : Ceza Muhakemesi Kanunu

DNS : Domain Name Systems

EİK : Elektronik İmza Kanunu

ETCK : Eski Türk Ceza Kanunu

f : Fıkra

FSEK : Fikir ve Sanat Eserleri Kanunu

HTML : Hiper Text Markup Language

IP : Internet Protocol

İ.B.D : İstanbul Baro Dergisi

İÜHFMD : İstanbul Üniversitesi Hukuk Fakültesi Mecmuası

İÜHFM : İstanbul Üniversitesi Hukuk Fakültesi Mecmuası

ODTÜ : Orta Doğu Teknik Üniversitesi

s : Sayfa

S : Sayı

SBE : Sosyal Bilimler Enstitüsü

SK : Sayılı Kanun

SÜHFD : Selçuk Üniversitesi Hukuk Fakültesi Dergisi

TBMM : Türkiye Büyük Millet Meclisi

TCK : Türk Ceza Kanunu

TÜBİTAK : Türkiye Bilimsel ve Teknik Araştırma Kurumu

vb : ve benzeri

vd : ve devamı

YCD : Yargıtay Ceza Dairesi

YTCK : Yeni Türk Ceza Kanunu

GİRİŞ

Bilişim teknolojisinin 20. yüzyılın ikinci yarısından sonra hızla gelişmesi ile beraber toplumun her kesimi de bu teknolojinden çeşitli yönleriyle etkilenmiştir. Bilişim teknolojilerinin dünyada ve ülkemizde çok hızlı bir şekilde yaygınlaşması bilişim suçlarının artmasına ve suç işlenmesinin kolaylaşmasına sebebiyet vermiştir.

Bilişim teknolojisi hayatı kolaylaştırıp insanlara fayda sağlarken bazen de insanların zarar görmesine sebep olmuştur.

Bilişim suçlarının işlenmesi bilişim teknolojinin gelişimi ile paralel olarak hızlı bir şekilde artmaktadır. Klasik suçların da bilişim sistemleri üzerinden işlenmeye başlanması ile pek çok ülke yeni oluşan bu duruma ve bilişim ortamında oluşan suç tiplerine göre hukuk ve ceza mevzuatlarında düzenleme yapmaya başlamıştır.

Bilişim suçlarının bu kadar hızlı yayılması uluslararası platformda da devletlerin ortak kurallar içeren önlemler almasına sebebiyet vermiştir.

Bilişim suçlarına ilk defa Avrupa Siber Suç Sözleşmesinde geniş çaplı yer verilmiş ve ortak imza atan ülkelerde geçerli olacak kararlar alınmıştır.

Siber Suç Sözleşmesiyle beraber birçok ülke gibi Türkiye de bilişim suçlarıyla mücadele etmek için 765 sayılı TCK ya bilişim suçlarını ilave ederek düzenleme altına almıştır. 765 sayılı TCK'nın 525a vd maddelerinde düzenlenip daha sonra 1 Haziran 2005 tarihinde 5237 sayılı TCK'nın yürürlüğe girmesi ile beraber bilişim suçlarına da; bilişim alanında suçlar başlıklı bölüm altında geniş yer verilmiştir. Bilişim suçları 5237 sayılı TCK'nın 243 vd. maddelerinde düzenlenmiştir. Yine Fikir ve Sanat Eserleri Kanununun 2. maddesinde değişiklik yapılarak bilgisayar programları da kanun kapsamında koruma altına alınmıştır.

Avrupa Birliği ülkeleri ve Türkiye'de Bilişim Suçlarının ceza hukukundaki uygulamaları isimli yüksek lisans tezimde bilişim sistemleri

yoluyla işlenen suçların Türk Mevzuatında ve Avrupa Birliği Ülkeleri ile diğer bazı dünya ülkelerindeki mevzuatlarda bulunan yasal düzenlemeleri ve Türkiye'deki mevzuatla bu ülkelerdeki yasal düzenlemelerin karşılaştırılması yine Türkiye'deki mevzuatın uluslararası mevzuata uygunluğu tartışılmıştır.

Ana hatlarıyla bilişim suçlarına ilişkin temel kavramlardan bahsedilmiş bilişim suçlarının işleniş biçimleri ve Avrupa Siber Suç Sözleşmesin den alınan kararların içeriğine değinilmiştir.

765 Sayılı TCK ve 5237 Sayılı TCK'da ki bilişim suçları ile ilgili kanun maddeleri ve maddelerin uygulanmasından doğan eksiklikler irdelenip çalışmamız tamamlanmıştır.

BİRİNCİ BÖLÜM

1. TEMEL KAVRAMLAR VE TANIMLAR

1.1. Bilgisayar

Dış ortamdan çeşitli yöntemlerle aldığı verileri içerisinde bulundurduğu programlar doğrultusunda depolayan, işleyen, bu verilerden yeni sonuçlar üreten, ürettiği sonuçları kullanıcıya sunan ve veri iletişimini sağlayan bir makine olarak belirtmemiz mümkündür[1]. Dünya da bilgisayar İngilizcedeki "computer" sözcüğüyle en yaygın kullanıma, sahiptir[2]. Türkçe sözlükte ise aritmetiksel ve mantıksal işlemlerden oluşan bir işi önceden verilmiş bir programa göre yapıp sonuçlandıran elektronik araç elektronik beyin olarak tanımlanmaktadır[3].

1.2. Donanım

Bilgisayarın elle tutulan fiziki bileşenlerine verilen addır. Donanım çevre giriş çıkış birimleri ROM, RAM, mikro işlemci donanım olarak adlandırılmaktadır.

Çevre giriş çıkış birimleri: Türlü nitelikteki verilerin işlemden önce bilgisayara ulaşması gerekir. Bu işlemleri yapmamızı sağlayan ünitelere giriş birimleri denir. Bilgisayara ulaşan verilerin bizim anlayacağımız şekle dönüştürülmelerini sağlayan ünitelere de çıkış birimleri denir[4]. Yazıcı, klavye, ekran, optik okuyucu giriş-çıkış birimlerine vereceğimiz örnektir.

RAM: Geçici bellek de denir. Bilgisayara gelen akım kapatıldığı zaman gücün kesintiye uğramasıyla tüm kayıtlarının silindiği, yapılan işlemlerinin depolanmadığı bellektir.

---

[1] R.Yılmaz Yazıcıoğlu Bilgisayar Suçları Kriminolojik Sosyolojik ve Hukuki Boyutları İle, Alfa Yayınları, İstanbul, 1997, s.26
[2] Dr. Ali Karagülmez Bilişim Suçları ve Soruşturma ve Kovuşturma Evreleri, Seçkin Yayınları, Ankara, 2005, s.32
[3] Türkçe sözlük, http://www.tdk.gov.tr
[4] Bilgisayar Ansiklopedisi, Milliyet Yayınları, İstanbul, 1991, s.39

ROM: Okunur bellektir. Kullanıcı tarafından değiştirilemez. Bilgisayarın bu parçasına herhangi bir kayıt yapılamaz. Bilgisayara gelen gücün kesintiye uğramasından etkilenmez, deformasyona uğramaz.

SİSTEM YAZILIMI: Bilgisayarın fonksiyonunu yerine getirebilmesi için kullandığı yazılımdır. Belli bir görevi yerine getirmek için önceden bilgisayara yerleştirilmiş, olan kodlar bütünüdür.

MİKRO İŞLEMCİ: Bilgisayarın beynidir. Giriş birimlerinden gelen veriler ve komutlarla ilgili işlemleri yapar.

UYGULAMA YAZILIMI: Belli bir fonksiyonu yerine getirmek için bilgisayarda kurulu bulunan işletim sistemi üzerine yüklenen program türüdür. Paket şeklinde hazırlanmıştır.

1.3. Veri

Bir bilgisayar sisteminde bilgilerin belirli bir formata dönüştürülmüş halidir[5]. Bir bilgisayar sisteminde işlenmeye uygun her türlü bilgiyi ihtiva eder.

1.4. Program

İstenilen sonucu almak için bilgisayar tarafından işletilen bir talimatlar bütünüdür[6].

1.5. İnternet

Birden fazla haberleşme ağının birlikte meydana getirdiği büyük bir ağdır. Dünyada geçerli olan TCP/IP protokolü ile bilgisayar sistemlerini dünya çapında birbirine bağlayan ağdır[7]. Dünya üzerindeki birden çok bilgisayar ağına bağlantı kurulan büyük bir ağdır. TCP/IP bilgisayarın ve yerel ağların

---

[5] R, Yılmaz Yazıcıoğlu, Bilgisayar Suçları Kriminolojik, Sosyolojik ve Hukuksal Boyutları ile, Alfa Yayınları, İstanbul, 1997, s. 30

[6] Deniz Helvacıoğlu, 2004 “Avrupa Konseyi Siber Suç Sözleşmesi Temel Hükümlerin İncelenmesi, İnternet ve Hukuk İstanbul Bilgi Üniversitesi Yayınları, İstanbul, 2004, s.280

[7] Ali Karagülmez, Bilişim Suçları ve Soruşturma- Kovuşturma Evreleri, Seçkin Yayıncılık Ankara, 2005, s.36)

birbirleri ile iletişim kurmalarını sağlayan ortak bir anlaşma dilidir[8]. İnternet üzerindeki bilgi iletimi ve paylaşımı bazı kurallar dahilinde yapılmaktadır. Bu kurallara internet protokolleri denir. "TCP" iletim kontrol protokolü "IP" internet protokolü anlamına gelir[9].

Protokollere bazı örnekler verirsek, internet üzerindeki dosya alma/gönderme protokolü (FTP: File Transfer Protokol) elektronik posta iletişim protokolü (SMTP: Simple Mail Transfer Protokol) TELNET protokolü (internet üzerindeki başka bir bilgisayarda etkileşimli çalışma için geliştirilen protokoldür) www (world wide web) ortamında birbirine bağlanmış farklı türden objelerin iletilmesini sağlayan protokol ise Hyper Text Transfer protokol (http) olarak adlandırılmaktadır[10].

İnternete bağlı her bilgisayarın bir adresi bulunur. İnternete bağlı bilgisayar sistemleri "domain name system" (DNS) ile isimlendirilir. Bu isimlere örnek verirsek ac: Akademik kuruluşlar, com: Ticari kuruluşlar, org: sivil toplum kuruluşları, edu: eğitim kuruluşları, int: uluslararası kuruluşlar, gov: Hükümet kuruluşları, mil: askeri kuruluşlar, net: kendi özel ağları olan ve bunu dış kullanıma sunabilen gruplardır.

Her internet adresine 4 haneli bir numara karşılık gelir. a,b,c,d şeklindeki bu numaralara IP (İnternet Protokol) numaraları denir. Buradan a,b,c,d 0-255 arasında değişen bir tam sayıdır. İnternet adresinin ilk kısmı bulunduğu domain'in network adresini son kısmı ise makinenin (host) numarasını verecek şekilde ikiye bölünür. İnternet üzerindeki her bilgisayarın o anda sadece kendisine ait olan adresi vardır. Bu adres her internet bağlantısında değişmektedir. Statik IP, sürekli size ait olan bir IP adresinin olması ve bilgisayarınıza tanımlanmasıdır[11].

---

[8] Kayıhan İçel, Kitle Haberleşme Hukuku, İstanbul, 1998, s. 407
[9] Murat Volkan Dülger, Bilişim Suçları, Seçkin Yayınevi, Ankara, 2004, s.48
[10] Özgür Eralp, ''Bilişim Suçlamasına Giden Yol – IP'',http://www.turkhukuksitesi.com.,03.05.2009
[11] İsmail Ergün, Siber Suçların Cezalandırılması ve Türkiye'de Durum, Turhan Kitabevi, Ankara, 2008, s.9

İnternet bağlantısı Türkiye'de ilk kez 1993 yılında gerçekleşmiştir. ODTÜ ve TÜBİTAK' ın ortak projesi ile sağlanmıştır. Alan adı ve IP numarası dağıtımı TTnet, ODTÜ ve ULAKNET tarafından yapılmaktadır.

Avrupa'da IP numarası dağıtımı yerel internet kayıt merkezleri (Local İnternet Registries) tarafından yapılmaktadır. ABD'de bulunan Global İnternet Registry Avrupa bölgesindeki IP numarası dağıtım yetkisini RIPE NCC (Reseux IP Europens Network Coordination Center) kuruluşuna vermiştir[12].

1.6. Bilişim Kavramı

Türk Dil Kurumunun güncel sözlüğünde bilişim insanoğlunun teknik, ekonomik ve toplumsal alanlardaki iletişiminde kullandığı ve bilimin dayanağı olan bilginin özellikle elektronik makineler aracılığıyla düzenli ve akla uygun bir biçimde işlenmesi bilimi olarak tanımlamaktadır[13]. Bilişim sözcüğünün kökeni, Fransızcadan Türkçeye geçen "informatique" kelimesine dayanmaktadır.

Türkçeye enformasyon olarak geçen kelime daha sonra bilişim kavramı olarak değişmiştir. Bilişim verilerin toplanmasını, işlenmesini, değerlendirilmesini, dağıtımını ve aktarılmasını sağlayan bilim dalıdır.

1.7. Bilişim Suçu Kavramı

Elektronik bilgi işlem kayıtlarına yasadışı yollarla erişilmesi, bu kayıtların yasal olmayan şekilde değiştirilmesi, silinmesi veya bu tür kayıtlara girilmesi veyahut bilgi tecavüzü için hazırlık yapılmasıdır[14]. Bilişim Suçları konusunda herkesin kabul ettiği bir tanımlama yoktur.

---

[12] İsmail Ergün, a.g.e, s.9
[13] TDK "Güncel Türkçe Sözlük" www.tdk.gov.tr, 05.10.2009
[14] Aydın Emin Doğan, Bilişim Suçları ve Hukukuna Giriş, Doruk Yayınları, Ankara, 1992, s.27

Dülger, bilişim suçunu, verilere karşı ve veri işlemlerine bağlantısı olan sistemlere karşı bilişim sistemleri aracılığıyla işlenen suçlar olarak tanımlamıştır[15].

Avrupa Ekonomik Topluğu uzmanlar komisyonunun Mayıs 1983 tarihinde Paris toplantısında yapılan tanımlamada bilgileri otomatik işleme tabi tutan veya verilerin nakline yarayan bir sistemde gayri kanuni gayri ahlaki veya yetki dışı gerçekleştirilen her türlü davranıştır[16].

Avrupa Ekonomik Topluğu bu suçları beşe ayırmıştır. 1- Bilgisayarda mevcut olan kaynağa veya herhangi bir değere gayri meşru şekilde ulaşarak transferlerini sağlamak için kasten bilgisayar verilerine girmek, bunları bozmak, silmek, yok etmek, 2- Bir sahtekarlık yapmak için kasten bilgisayar verilerine veya programlarına girmek, bozmak, silmek, yok etmek 3- bilgisayar sistemlerinin çalışmasını engellemek için kasten bilgisayar verilerine veya programlarına girmek bozmak 4-ticari anlamda yararlanmak amacı ile bir bilgisayar programının yasal sahibinin haklarını zarara uğratmak 5- Bilgisayar sistemi sorumlusunun izni olmaksızın konulmuş olan emniyet tedbirlerini aşmak suretiyle sisteme kasten girerek müdahalede bulunmaktır[17].

Bilişim suçları çok geniş bir yelpazeye yayılmıştır. Bilgisayarın ve internetin yaygınlaşması ile bu suçlar gündeme gelmiştir. Bilişim suçları ilk 1960'lar da ortaya çıkmıştır. Bilinen ilk bilişim suçu 18 Ekim 1966 tarihli Minneapolis Tribune'de yayınlanan "Bilgisayar uzmanı Banka hesabında tahribat yapmakla suçlanıyor başlıklı makale ile kamuoyuna yansımıştır[18].

---

[15] Murat Volkan, a.g.e, s.67

[16] Cevat Özel, Bilişim ve İnternet Suçları Üzerine Bir İnceleme İnternet Hukuku, www.law.ankara.edu.tr/yazi 03.05.2009

[17] Cevat Özel, ''Bilişim Suçları ile İletişim Faaliyetleri Yönünden TCK Tasarısı'' İstanbul Barosu Dergisi C.75 S. 3, s.2-3

[18] Emin Aydın, a.g.e, s.13.

1.8. Siber Suç Kavramı

Siber suç kavramı bilişim suçu ve bilgisayar suçunun bileşimidir. Siber suç deyimi bilgisayarlar aleyhine veya bilgisayarlar aracılığıyla işlenen suçlar olarak tanımlanmaktadır[19]. Siber suç internet ortamında ve elektronik ortamda işlenebilen hukuka aykırı eylemleri gerçekleştirmek için işlenen suçlardır. Avrupa konseyi siber suç sözleşmesinin orijinal başlığında yer alan "cyber" kelimesi Türkçeye "siber" olarak çevrilmiştir[20].

2. BİLİŞİM SUÇLARININ İŞLENME ŞEKİLLERİ

2.1. Salam Tekniği

Bankaların bilişim sisteminde yaygın olarak gerçekleştirilen bir bilişim suçu metodudur. Bu yöntemle banka hesaplarına yatırılan paraların küsuratlı kısmı başka bir başka hesabına aktarılır. Küçük miktardaki paralar başka bir hesapta birikerek büyük bir meblağ olur. Bu yöntem Truva atı programı ile kullanılır.

2.2.Truva Atı (Trojan Horse)

Gizli kapaklı işler yapan bir program olup kullanıcının yerine kendiliğinden süreç başlatan bir fonksiyondur[21]. Masum bir program gibi görünen program, içerisinde zararlı yıkıcı komutlar içerir. Bilgisayar kullanıcısı farkında olmadan bilgisayarının kontrolü başka bir kullanıcının eline geçer, truva atı yazılımı yazılımcısının komutları doğrultusunda işlemler yapar.

---

[19] R.Yılmaz Yazıcıoğlu, "Bilgisayar Ağları ile ilgili suçlar konusunda Türk Ceza Kanunu 2000 Tasarısı" Uluslar arası internet Hukuku Sempozyumu 21-22 Mayıs 2001, Dokuz Eylül Üniversitesi Yayını, İzmir

[20] Aslı Deniz Helvacıoğlu, a.g.e, s. 277.

[21] Levent Kurt, Açıklamalı İçtihatlı Tüm yönleriyle Bilişim suçları ve Türk Ceza kanundaki uygulaması, Seçkin Yayınları, Ankara, 2005, s.63

2.3. Gizli Kapılar (Trap Door)

Hile kapısı, arka kapı da denir. Programcısı tarafından sistemin içine bırakılan koruyucu güvenlik kontrollerine takılmadan geçen ve sisteme yerleşen bir programdır. Bu programın çalışması için bir şifre gerekmektedir. Bu da yazılımı yapan kişide bulunur.

2.4. Ağ Solucanları (Network Worm)

Ağ solucanları kendi kendilerine çoğalırlar başka bir programa ihtiyaç duymazlar. Herhangi bir kullanıcı müdahalesine ihtiyaç duymadan kendi kendini çalıştırabilen ve tam bir kopyasını ağa bağlı olan diğer bilişim sistemlerine de kopyalayabilen bir programdır[22].

2.5. ÇÖPE DALMA (Scavenging)

Artık toplama da denilen bu teknikte bir bilgisayar sisteminin çalışmasında geriye kalan veri ve bulguların toplanması işlemi ifade edilmektedir[23].

2.6. Bilişim Korsanlığı (Hacking)

Bilişim sistemine girip hedefle ilgili keşif yapılarak önemli bilgilere ulaşmaktır. Hacking eylemine gerçekleştirene hacker denir. Hacker ise bilişim sistemine müdahale eden kişiye verilen isimdir, aynı zamanda bilişim korsanı da denir.

2.7. Veri Aldatmacası (Data Didding)

Basit ve güvenilir olması yanında ortaya çıkarılması zor olduğu için en çok tercih edilen yöntemlerden biridir. Veri bilişim sistemine girilirken değiştirilmesi, yanlış veri girilmesi ve bazı verileri bilgisayarda bırakarak mevcut veriler üzerinde istediği gibi değişiklik yapılmasıdır.

---

[22] Levent Kurt, a.g.e, s.68
[23] R.Yılmaz Yazıcıoğlu, (1997), a.g.e, s159

2.8. Mantık Bombaları

Truva atı yazılımının bir türüdür. Bilişim sistemini şaşırtmak, bozmak veya felç etmek, için programlanmaktadır ve bunu gerçekleştirebilmek; için bilgisayara ya mantık dışı ya da yapılan işlemin aksine sürekli bilgi göndermektir[24]. Sistem için yıkıcı, zarar vericidirler.

2.9. Gizlice Dinleme (Eavesdropping)

Bilişim sistemlerinin veri naklinde kullandığı ağlara girilerek veya bilişim sistemlerinin az da olsa yaydığı elektromanyetik dalgalarını yakalayarak verilerin tekrar elde edilmesi tekniğidir[25].

2.10. Tarama (Scanning)

Bilişim sistemlerine değeri her seferinde değişen verileri hızlı bir şekilde girerek sistemin olumlu cevap verdiği durumların tespitine yönelik bir tekniktir. Tarama, bilişim sistemlerinin telefon numaralarını veya internete bağlı sistemlerinin IP numaralarını bulmaya yönelik olabileceği gibi IP numaraları belli olan fakat bir şifre ile korunmuş sistemlerin geçerli şifresini bulmaya yönelikte olabilir[26].

2.11. Süper Darbe (Super Zapping)

Bilgisayar programlarının sistemlerinin çalışırken kendiliğinden oluşan hatalar nedeniyle sistemin kilitlenmesi durumunda yeniden eski haline getirilmesi amacıyla kullanılmaktadır. Sistem kilitlendiğinde bu program güvenlik duvarlarını aşarak sistemin yeniden çalışmasını sağlar.

---

[24] R.Yılmaz Yazıcıoğlu, (1997), a.g.e, s157.
[25] Olgun Değirmenci, "Bilişim Suçları ", Marmara Üniversitesi Sosyal Bilimler Enstitüsü Yayınlanmamış yüksek lisans Tezi . İstanbul, 2002, s77.
[26] Levent Kurt, a.g.e, s.65

2.12. Eş Zamansız Saldırılar

Birçok sistemin programları eşzamanlı yani aynı anda kullanamamasından hareket eden bazı failler geliştirdikleri saldırı teknikleri ile bilgisayar işletim sistemlerinde daha doğrusu programdaki veriler üzerinde çeşitli ihlaller meydana getirmektedir[27].

2.13. İstem Dışı Alınan Elektronik Postalar (Spam)

Bir bülten veya haber grubu üzerinden ticari amaç taşımayan bu forum konuları ile ilgili olmayan ve gönderilmesine açıkça izin verilmeyen reklam olarak tanımlanmaktadır[28]. Türkçesi "baharatlı domuz eti ve Jambon" olarak tercüme edilebilecek bir ürünün adı olan spam (spiced park and ham) bilgi bankalarından tartışma formlarından veya herhangi bir yolla elde edilen elektronik posta adreslerine kişilik haklarına yönelik bir ihlal teşkil etmese de rahatsız edici ve istem dışı olarak atılan her türlü ileti ve eklere denir[29].

E-postanın içeriğinde hakaret, tehdit, hukuka uygun olmayan her türlü propaganda varsa ülkemizde Türk ceza yasasında bulunan çeşitli davaları oluşturur. Elektronik posta sistemi engelleyecek boyuta ulaştığı taktir de 5237 sayılı TCK'nın 244 maddesinde düzenlenen "bilişim sisteminin engellenmesi kapsamında değerlendirilebilecektir[30].

2.14. Tavşanlar (Rabbits)

Girdikleri sistem içinde sürekli ve hızlı üreyen yerleştiği bellek veya diskteki alanı koloni kurmak suretiyle sürekli dolduran sistemin bilgi işleme gücünü zayıflatan bilgisayar veya sisteme sürekli gereksiz komutlar veren kendi kendilerine yetip virüsler gibi asalak olmayan programlardır[31].

---

[27] İsmail Ergün, a.g.e, s.23
[28] Memiş Tekin, ''Hukuki açıdan kitlelere E-posta Gönderilmesi'', http://bilisimsurasi.org.tr/dosyalar/14.doc, 13.02.2009.
[29] Levent Kurt, a.g.e, s.72
[30] Levent Kurt, a.g.e, s.72
[31] Levent Kurt, a.g.e, s.75

2.15. Bukalemun (Chameleon)

Sistem için normal çalışan ve zararsız bir yazılım gibi davranan ve onun niteliklerin sahipmiş gibi görünen bukalemunlar, sistemin içine girdikten sonra gerçek kimliğini ortaya çıkarmakta ve hukuka aykırı eylemlerine başlamaktadır. Kendisini saklamaktaki başarısı nedeniyle bu adı almıştır[32].

3. BİLİŞİM SUÇLARININ TASNİFİ

Avrupa Konseyinin 2001 Siber Suç Sözleşmesinde siber suçlar:

1- Bilgisayar veri sistemlerinin ulaşılabilirliği bütünlüğü ve gizliğine karşı işlenen suçlar (Kanunsuz Erişim (md2) Kanunsuz Araya Girme (md3) veriye müdahale (md4) sistem engellemeleri (md5) Cihazları kötüye kullanma (md6)

2- Bilgisayar Bağlantılı suçlar (Bilgisayar Bağlantılı Sahtekârlık (md7) Bilgisayar Bağlantılı Dolandırıcılık (md8)

3- İçerik Bağlantılı suçlar (çocuk pornografisi ile bağlantılı suçlar (md9)

4- Telif hakları ve bununla bağlantılı hakların ihlaline ilişkili suçlar olarak sınıflandırılmıştır.

Avrupa Ekonomik Topluluğunda bir tavsiye kararında bilişim suçları beşe ayrılmıştır

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

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

[32] Murat Volkan, a.g.e, ,s.48

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

4- Ticari manada yararlanmak amacı ile bilgisayar programının yasal sahibinin haklarını zarara uğratmak,

5- Bilgisayar sistemi sorumlusunun izni olmaksızın konulmuş olan emniyet tedbirlerini aşmak sureti ile sisteme girerek kasten müdahalede bulunmaktır[33].

Birleşmiş Milletler 10. Kongresinde de suçları, dar anlamda bilişim suçları ve geniş anlamda bilişim suçları olmak üzere iki alt kategori içinde değerlendirilmektedir. Dar anlamda bilişim suçları bilişim sisteminin güvenliğini veya veri işlemini hedef alan eylemlerdir. Geniş anlamda bilişim suçları ise bilişim sistemi ve ağı marifetiyle bu sistem veya ağda gerçekleşen herhangi hukuk dışı eylemlerdir[34].

Görüldüğü üzere bilişim suçları ile ilgili herkesin birleştiği ortak bir tasnif yok kısaca; bilişim sistemi içinde işlenen tüm suçlar olarak bilişim suçlarının tasnifi mümkündür.

[33] Yzb. Onur Şehitoğlu, ‘’Bilgisayar ve Ağ Üzerinden İşlenen Siber Suçlarla Müdahalenin Hukuksal ve Güvenlik Boyutu’’ İsimli Yayınlanmamış Yüksek Lisans Tezi , Kara Harp Okulu Savunma Bilimleri Enstitüsü Güvenlik Bilimleri Ana Bilim Dalı, Ankara, 2005, s.31
[34] R.Yılmaz Yazıcıoğlu, (2001), a.g.e, s.460.

4. BİLİŞİM SUÇ TİPLERİ

4-1 Veri Suçları

Konusu bilişim sistemindeki bulunan verilerin bozulması değiştirilmesi çalınması ve durdurulması oluşturmaktadır.

4.1.1 Verilerin Durdurulması (Müdahale Edilmesi)

Verinin iletilmesi anında hukuka aykırı olarak müdahaleye maruz kalması, değiştirilmesi ve ulaşılmasının engellenmesi şeklinde işlenebilir.

4.1.2 Veri Korsanlığı

Verilerin klasik hırsızlık suçunun objesi olan taşınabilir bir mal özelliğinde olmaması ve hırsızlık suçunun veri sahibinin veriyi kullanma imkânını ortadan kaldırmamasından dolayı verilerin kopyalanması, aktarılması ya da alınması eylemleri cezalandırılmaktadır. Verilerin verinin sahibine veya başkalarına zarar vermek veya failin kendisine veya başkalarına haksız kazanç sağlamak amacıyla bulunduğu yerden alınması ve kopyalanması veri hırsızlığı suçunun oluşumu için yeterli unsurları oluşturmaktadır[35].

4.1.3. Verilerin Değiştirilmesi

Bilişim sistemlerinde bulunan bilgilerin veri güvenliğinin tahrip edilmesi, bozulması ve değiştirilmesidir.

Özellikle sahtekârlık ve dolandırıcılık suçlarında kullanılır.

[35] Hülya Pekşirin ve diğerleri, '' Türkiye Bilişim Şurası Hukuk Çalışma Grubu Raporu, G. ÜZEL (Ed) Türkiye Bilişim Şurası, Ankara, 10-12 Mayıs 2002, s.80.

4.2. Bilişim Ağlarına Yönelik Suçlar

4.2.1. Ağ Engellenmesi

Ağın tamamına veya bir kısmına kullanıcının erişiminin girişinin önlenmesidir. Yönlendirilmiş bilgisayarda sürekli veri gönderilerek işlenir.

4.2.2. Ağ Sabotajı

Sistemin fiziki bileşenlerine yönelmiş bir hareket vardır. Burada ortaya konulan suç ceza kanunumuzda düzenlenen Nas-ı ızrar suçunun özel bir çeşidini oluşturmaktadır[36]. Bilişim sisteminin veya ağın değiştirilmesi fiziki zarara uğraması neticesinde meydana gelmektedir.

4.3. Yetkisiz Giriş Suçları

Tehlike suçlarının bilişim alanındaki şekli kastedilmektedir. Bilişim sistemi sahibinin alanına izinsiz olarak giriş suç olarak öngörülmüştür.

4.3.1. Bilişim Sistemlerine İzinsiz Giriş

Bilişim sistemine ulaşarak yetkili olmayan kişinin bilgisayardaki sistemde kayıtlı bilgilere ulaşarak onları kullanmasıdır. Yetkisiz dinleme ve hesap ihlali eylemleri bu suçlara örnek verilebilir.

4.3.2. Virüs Yayılması

Zararlı programların sistem veya verilere zarar vermek üzere harekete geçirilmesidir. Virüsler sayesinde sistem, veri ve programlar zarara uğratılır. Virüslerin yayılması müstakil bir suç olmayıp genelde sonuçları itibariyle suç haline gelmektedir[37].

---

[36] Yasin Beceni, Özgür Uçkan, "Bilişim İletişim Teknolojileri ve Ceza Hukuku" İnternet ve Hukuk, İstanbul Bilgi Üniversitesi Yayınları, İstanbul, 2004, s.429

[37] Levent Kurt, a.g.e, s.83

4.4. Bilgisayarla İlgili Diğer Suçlar

4.4.1. Dolandırıcılık

Bilişim sistemindeki programın verinin değiştirilmesi, oynama yapılması hileli işlemler yapılması suretiyle bilişim sisteminin işleyişi değiştirilerek işlenir.

4.4.1.1. Girdi/Çıktı Program Hileleri

Sisteme yanlış veri giriş ve çıkışı yapılarak işlenen suçtur. EFT Suçları bu suça girer. Sisteme hayali faturalar girilir ve daha sonra ödenir. Kimsenin dikkatini çekmeyen düşük meblağlar olur. Bu tür dolandırıcılıklar bu suç kapsamına girer.

4.4.1.2. İletişim Servislerinin Yetkisiz Olarak Kullanılması

Kendisine veya başkasına ekonomik menfaat sağlamak maksadıyla iletişim sistemlerindeki protokol ve prosedürlerin açıklarını kullanarak iletişim servislerine veya diğer bilgisayar sistemlerine hakkı olmadan girmek bu suç grubuna girer. Kişi veya firmayı kandırabilmek için plan içerisinde web sitesinin, sohbet (chat) odalarının ve e-posta hesaplarının kullanılmasıdır.

4.4.1.3. Kredi Kartı Dolandırıcılığı

İnternet üzerinde bir başkasının hesabından başkalarının hesaplarına para aktarılmasıdır. Bu durum daha çok internet bankacılığında görülür. Kredi kartı bilgileri, numarası ve kişisel bilgiler öğrenilerek işlenir.

4.4.2. Bilgisayar Sahteciliği

Elektronik belgeler üzerinde hukuka aykırı yapılan değişiklikler bu suçu oluşturur. Sahte kredi kartı, materyal, senet, belge ve rapor gibi belgeler üzerinde bilgisayar sitemini kullanarak değişiklik yapmaktır.

4.4.3. Kanunla Korunmuş Bir Yazılımın İzinsiz Kullanımı

Telif hakkı ihlali gerekçesiyle kanunla korunmuş yazılımların izinsiz olarak çoğaltılması yasadışı yöntemlerle elde edilen bilgisayar yazılımlarının satışı kopyalanması dağıtımı ve kullanımı yasaklanmıştır.[38]

4.4.4. Yasadışı Propaganda

Kanun tarafından yasaklanmış her türlü materyalin sanal ortamda bulunan web siteleri, elektronik posta gibi unsurlar kullanılarak saklanması, yayınlanması ve dağıtılması yasaklanmıştır[39].

4.4.5. Verilerin Suistimali

Kişisel bilgiler, ticari bilgiler, gibi verinin sahibinin rızası dışında kendisine başkasına ekonomik bir menfaat sağlamak zarar vermek için verinin kullanılmasıdır.

[38] Emniyet Genel Müdürlüğü Bilişim Suçları Çalışma Güvenliği Raporu 2 1999 b 10.02.2004 < http://www.egm.gov.tr/docs/ RAPOR1 pdf >
[39] Yzb. Onur Şehitoğlu, a.g.e, s. 39.

İKİNCİ BÖLÜM

1. AVRUPA ÜLKELERİNDE BİLİŞİM SUÇLARI

1.1. Fransa

Fransa'da veri ceza kanunu 01.03.2003 tarihinde yürürlüğe girmiştir.

Fransız Ceza kanununda 226-16 ile 226-24. maddeleri kişilik haklarının bilişim sistemi aracılığıyla ihlalini düzenlemektedir. Aynı kanunun 323-1 ile 323-7. maddeleri ise otomatik sisteme bağlı kişisel verilerin ihlalini suç olarak düzenlemektedir. Fransız Ceza Kanunu'nun 226-8. maddesi kişilerin resim ve sözlerinin kişinin rızasına aykırı biçimde montajının yayınlanmasını, 227-23. maddesi küçüğün resminin pornografik nitelikte kullanılmasını, 227-24. maddesi küçük tarafından görülmeye elverişli şiddet ve pornografik nitelikli mesaj yayımı eylemini, 323-1. maddesi otomatik bilişim sistemine tamamen veya kısmen haksız biçimde girmeyi, girilen sisteme kaydedilmiş verileri silme, değiştirme veya sistemin fonksiyonlarını değiştirmeyi, 323-2. maddesi ise bilişim sistemlerindeki verileri hukuka aykırı biçimde silme, değiştirme gibi eylemleri suç olarak düzenlemiştir[40].

Fransa'da bilişim suçları ayrı bir fasıl halinde düzenlenmeden önce bu tarz eylemler Fransız Ceza Kanunundaki hırsızlık (md. 379), inancı kötüye kullanma (md 408) ve dolandırıcılık (md 405) gibi mal aleyhine işlenen bazı suçlarla karşılanmaya çalışılmaktaydı[41].

Fransa'da internete özgülenmiş bir ceza hukuku düzenlemesi yoktur. İnternet üzerindeki suç içerikli yayınlardan dolayı kimin sorumlu tutulacağı sorununa ilişkin henüz özgün bir düzenleme yoktur.

Bilişim suçlarıyla mücadele amacıyla devletin birden fazla kurumunda özel birimler kurulmuştur.

---

[40] Yener Ünver, ''Türk Ceza Kanunun ve Ceza Kanunu Tasarısının İnternet Açısından Değerlendirilmesi'', İstanbul Üniversitesi Hukuk Fakültesi Mecmuası sayı:1-2,İstanbul, 2001, s. 67.

[41] Levent Kurt, a.g.e, s.102.

a. Başbakana bağlı Milli Genel Sekreterliği (SGDN) bünyesinde kurulun Haberleşme Sistemleri Güvenliği Merkez Birimi (DCSSI)

b. Haberleşme Teknolojisi kullanılarak yapılan dolandırıcılıkların soruşturulması birimi (SEFTI)

c. Bilgisayar ortamında işlenen suçların bastırılması birimi (BCRCI)

d. Jandarma Genel Komutanlığı Seç Araştırmaları Enstitüsü (IRCGN)

e. Fransız İstihbarat Örgütü (DST)

f. İletişim ve Enformasyon ve Teknolojilerinin kullanımı suretiyle işlenen Suçlarla Mücadele Bürosudur. [42]

Fransız Ceza Kanununda 5 Ocak 1988 günlü, 88-19 sayılı "relative a la fraude informatique" isimli Kanun ile ilk kez bilişim suçlarına ilişkin müstakil bir düzenleme yapılmıştır. 88-19 Sayılı kanunda,

1- Suça teşebbüs (md 462, 7) ve iştirak (md. 462, 8) gibi genel hükümlerin yanında

2- Haksız yere bir bilgisayara girme veya sistemde haksız yere kalma.

3- Sistemdeki verileri tahrip etme, değiştirme, yok etme veya başka veriler yükleme.

4- Sistemin işleyişini engelleme veya bozma

5- Bilgisayar belgelerinde sahtekârlık yapma

6- Böyle bir belgeyi bilerek kullanma suçu oluşturulmuştur.[43]

Fransa'da veri koruma kanunu 1978 yılında yasalaşmıştır. Bunlar:

[42] E.G.M Raporu http://www.bilisimsurasi.org.tr/dosyalar/10.doc)
[43] Ali Karagülmez, a.g.e, s. 114.

1- Otomatikleşmiş veriyi toplamak için gerekli olan resmi ön şartlara uyum sağlamadan veriyi toplamak,

2- Otomatikleşmiş veriyi depolamak için gerekli olan tüm güvenlik tedbirlerini almadan toplamak,

3- Otomatikleşmiş veriyi hileli haksız ve kanun dışı yollar ile toplamak veya bir kişiyi ilgilendiren bilginin şahsın makul itirazlarına rağmen toplanması

4- Sağlık kayıtlarını ilgili kişiye erişim, tasfiye ve itiraz konularındaki haklarını bildirmeden toplamak veya kişinin itirazlarına rağmen tutmak

5- Kişini doğrudan ya da dolaylı olarak ırksal kökenini, politik görüşünü, dini inancını, felsefi görüşünü, bağlı olduğu sendikayı veya ahlaki değerlerini ortaya çıkarabilecek verileri ilgili kişinin açık bir onaylaması olmadan tutmak

6- CNLI (bilgi işlem ve özgürlükleri üzerine denetleme yapmak amacıyla kurulmuş bağımsız bir ulusal komisyon) tarafından belirtilen süreden daha fazla süre verileri depolamak.

7- Verilerin tutulmasında niyetlenilen maksattan ayrılarak verileri tutmak.

8- Verileri görmemesi gereken üçüncü şahısların verileri görmesini sağlamak (etkilenen insanın rızası olmadan)

Bu kapsamda belirtilen suç tipleri bilişim suçlarından ziyade bilişim alanında suçlarından ziyade bilişim alanında işlenebilecek klasik anlamdaki kişilik haklarının ihlalleri ile ilgilidir. Yukarıdaki suç tiplerinin cezası bir ile beş yıl hapis cezasının yanında 15.000 ile 100.000 Fransız frangı para cezası olmaktadır[44].

[44] Yener Ünver, a.g.e, s.68

Yeni Ceza Kanununda Bilişim Suçları

1- Bilgileri Otomatik İşleme Tabi Tutmuş Bir Sistemin Tamamına veya Bir Kısmına Aldatıcı Hareketlerle Erişmek (Girmek) Veya Kalmaya Devam Etmek (m. 323-1)

Bir sisteme hukuka aykırı olarak yetkisi olmadan girmesi ve hakkı olmadan kalınması suç haline getirilmiş, yapılan eylemler sistemdeki verilerin zarar görmesine, değişmesine, bozulmasına sebep olursa ceza artmaktadır; bu suç kasten işlenebilen bir suçtur. Bilinçli olarak sisteme yasadışı girip eylemde bulunması gerekir.

Ülkemizde kabul edilen 5237 sayılı TCK'nun 243. maddesinin 1 numaralı fıkrasında "bir bilişim sisteminin bütününe veya bir kısmına hukuka aykırı olarak giren veya orada kalmaya devam eden" ibaresindeki suçun maddi unsuru ile Fransız Ceza Kanunu'nun 323-1 maddesindeki "erişmek (girmek) veya kalmaya devam etmek" ibaresindeki maddi unsur, ciddi şekilde farklıdır. Fransız Ceza Kanunu'nun 323-1 maddesinde "girme" ile "kalmaya devam etme eylemleri" suçun seçimlik hareketleri olup yalnızca "girme" fiili ile suç gelişirken, 5237 sayılı TCK'nun 243/1 maddesindeki suçun oluşumu için tek başına "girme" fiili yeterli değildir. [45]

2- Bilgileri Otomatik İşleme Tabi Tutmuş Bir Sistemin Fonksiyonunu Bozucu veya Engelleyici Hareketlerde Bulunmak (m. 323-2)

Bilişim sistemleri kullanılarak işlenen suçlara Nas-ı Izrar Eylemleri de denir.

[45] Ali Karagülmez, a.g.e, s. 115.

323-2 Maddesinde, bilgileri otomatik işleme tabi tutmuş bir sistemin fonksiyonunu bozucu veya engelleyici hareketlerde bulunmak, üç yıla kadar hapis ve 300.000 Franka kadar para cezasıyla cezalandırılmaktadır. [46]

Bilgisayarda sistemde bulunan bilgilerin verilerin değiştirilmesi, tahribi, silinmesi, çalışmasını engellemek suretiyle sistemin zarara uğramasına sebebiyet vermek mala zarar verme suçunu oluşturur. Yeni Fransız Ceza Kanununda 323-2 maddesinde sisteme girerek müdahale ederek verilen zararla sisteme veri ekleyip eksilterek verilen zarar sorumlu tutulmuştur. Kasten işlenebilen bir suçtur.

3- Bilgileri Otomatik İşleme Tabi Tutmuş Bir Sistemdeki Bilgileri Aldatıcı Hareketlerle Değiştirmek veya Yok Etmek. (m. 323-3)

323-3 maddesinde, bilgileri otomatik işleme tabi tutmuş bir sistemdeki bilgileri aldatıcı hareketlerle değiştirmek veya yok etmek, üç yıla kadar hapis ve 300.000 Franka kadar para cezasıyla cezalandırılmaktadır[47].

4- Bilişim Sistemleri Kullanılarak Sır Aleyhine İşlenen Eylemler

Bilişim Sistemleri Kullanılarak bireysel mahremiyet ve gizlilik ihlalleri de yaptırım altına alınmaktadır. Nas-ı ızrar eylemlerinin dışında bilgisayar ve sistemlere girerek buralardaki veri ve programlara ulaşmak suretiyle mevcut bilgilerin elde edilmesi her ne suretle olursa olsun kullanılması veya ifşa edilmesi sır aleyhine cürüm kabul edilerek ya kanunların sırrın masuniyeti aleyhine cürümleri düzenleyen fasıllarında ya da ancak sır aleyhine işlenen cürüm olarak ele alınmakla beraber bilişim alanını ilgilendiren kısım özel hükümlerin içinde karşılanmaktadır. [48]

[46] Ali Karagülmez, a.g.e, s. 115.
[47] Ali Karagülmez, a.g.e, s. 116.
[48] Yzb. Onur Şehitoğlu, a.g.e, s. 75.

5- Bilişim sistemleri Kullanılarak İşlenen Dolandırıcılık ve Sahtecilik Eylemleri;

Fransız Ceza Kanunu (md 147) özel hükümler içinde dolandırıcılık suçunun elektronik ortamda işlenmesini düzenlemektedir. 441-1'deki maddelerde de düzenlenen sahtecilik suçuna ilişkin hükümler artık bilişim alanındaki sahtecilik eylemlerini de kapsamaktadır.[49] Bu suçlara teşebbüs ve iştirak 88-19. maddelerle cezalandırılmıştır.

Bu suçları icra ederken oluşturulan bir gruba veya manevi iştirak (Hazırlık) Anlaşmasına katılımla suç işlemek (md. 324-4) Suç olarak düzenlenmiştir. [50]

325-6. madde de tüzel kişilerin bu alanda işlenen suçlardan dolayı sorumluluğu düzenlemektedir.

01.08.2000 tarih ve 2000-179 sayılı kanunla iletişim özgürlüğü ile ilgili 30.09.1986 tarih ve 86-1067 Sayılı kanuna "Link üzerinde özel haberleşme dışındaki iletişim servisleriyle ilgili hükümler" eklenerek internet sujelerinin ceza sorumluluğu açısından bir ceza sistemi de oluşturulmuştur.[51]

16 Aralık 1992 günlü 1336 sayılı Kanunla değişik 30 Eylül 1986 günlü 86/1067 sayılı iletişim özgürlüğü Kanunu'nun 79-1 ile 79-6 maddelerinde ise şifreli kanal korsanlığı hükme bağlanmıştır.[52]

1.2. İngiltere

İngiltere'de bilişim suçları 29.08.1990 tarihinde yürürlüğe giren "Bilgisayarın Kötüye Kullanılması Kanunu" (Computer Misuse Act) ile düzenleme altına alınmıştır. Kanun 3 bölüm ve 18 kısımdan oluşmaktadır. Bu kanun ile yetkisiz olarak bilgisayarlara girilmesinin veya değişiklik

[49] R. Yılmaz Yazıcıoğlu, (1997), a.g.e, s.69.
[50] Ali Karagülmez, a.g.e, s. 116.
[51] T.Zeynel Kangal, "Fransa'da İnternet Yoluyla İşlenen Suçlardan Doğan Ceza Sorumluluğu" İstanbul Üniversitesi Hukuk Fakültesi mecmuası, c.lıx, İstanbul, 2001, s.228.
[52] Dijital platform İletişim hizmetleri A.Ş'nin Sunduğu Rapor, İletişim Şurası Notları, Ankara, 20-21 Şubat 2003,s.255.

yapılmasının yahut benzeri müdahalelerde bulunulmasının önlenmesi amaçlanmıştır.[53] Bu suç tiplerinden ilki, yetkisiz olarak bilişim cihazlarına veri ve programlarına girilmesi, ikincisi, başka bir suçun işlenmesini sağlamak ve kolaylaştırmak amacıyla yetkisiz olarak bilişim cihazına girmek, üçüncüsü ise, bilgisayar veri ve programlarının yetkisiz olarak değiştirilmesidir.[54]

1964 tarihli "Müstehcen Yayınlar Kanunu" ile 1984 tarihli "Telekomünikasyon Kanunu'nda yapılan değişikliklerle sanal alemde ki pornografi ve çocuk pornografisi alanına ilişkin düzenlemeler getirilmiştir.[55]

1978 tarihli Çocukların Korunması Kanunu'nda yer alan "fotoğraf" tanımı, 1994 tarihli Ceza Adaleti ve Kamu Düzeni Kanunu ile internetteki resimleri de kapsayacak şekilde değiştirilmiş, böylelikle internette veri halinde bulunan çocuk pornosu resimleri ve bunların montajla yapılmış şekillerini bulundurmak suç haline getirilmiştir.[56]

1- Bilişim Sistemlerine Hukuka Aykırı Erişim Veya Kullanılmasına Yönelik Eylemler Bakımından

Computer Misuse Act adlı kanunun 1. maddesinde incelenir. Bir bilgisayara veya programa kasten yetkisiz erişmek suç sayılmıştır. Bu suç için altı ayı geçmemek üzere hapis veya para cezası veya her iki cezaya birlikte hükmedilebilecektir.

Bir sisteme yetkisiz olarak erişim yapılmaya çalışılmış, ancak başarısız olunursa da suç oluşur. Yetkisiz erişimde zarar olmasa bile eylem cezalandırılmaktadır. Başka bir kullanıcıya alt bilgileri kullanarak yetkisiz bilgisayara erişip verileri bilgileri kullanmak çıktı almak gibi eylemler bu suça girmektedir.

---

[53] R.Yılmaz Yazıcıoğlu, (1997), a.g.e, s. 193,194.
[54] Hatine Akıncı, A. Emre Alıç, Er Cüneyd Er, "Türk Ceza Kanunu ve Bilişim Suçları" İnternet ve Hukuk, İstanbul Bilgi Üniversitesi Yayınları, İstanbul, 2004, s. 65
[55] Murat Volkan Dülger, a.g.e, s. 97.
[56] Fatih Selami Mahmutoğlu, "Bankacılık Suçları Bağlamında Çıkar Amaçlı Suç Örgütü", Avrupa Birliğine Uyum Süreci Bağlamında organize Suçlulukla Mücadele, Panel, 5 Ekim 2001, Bildiriler ve Tartışmalar, Yönetici Kayıhan İçel, İstanbul, 2002, s. 208.

2- Bilişim sistemleri Kullanılarak İşlenen Mala Zarar Verme Suçu

Bilgisayar sistemindeki verileri dosyaları değiştirmek, silmek, kasıtlı olarak arıza yaratmak için sisteme virüs göndermek, virüs sokmak bu bölümdeki suçları oluşturur.

Bilgisayardaki içerik veri ve bilgiler yetkisiz olarak değiştirilerek erişim engellenerek bu suçlar işlenir. Programı bozmak için mantık bombası atmak, solucan koymak, şifre koymak bu suç kapsamına girer. Bu suçlardan dolayı faile 5 yıla kadar hapis ve adli para cezası verilir. Burada para cezasının belirlenmesin de zarar çok önemlidir.

Bilişim sistemleri kullanılarak kişilere ait verilerin elde edilmesi de İngiltere'de suç kapsamında değerlendirilerek veri koruma kanunu çıkarılmıştır. Bu yasa ile veri sahibinin izni dışında verilerle ilgili işlem yapılması kullanılması ve elde edilmesi suç olarak düzenlenmiştir. Burada tüzel kişilerinde sorumluluğu düzenlenmiştir. Sadece şifreyi kıran ve verileri çalan kişi sorumlu tutulmamaktadır.

Bilişim sistemi kullanılarak dolandırıcılık ve Sahtekârlık eylemleri konusunda Computer Misuse Act. Adlı kanunda düzenleme yapılmış bilgi hırsızlığı ve yetkisiz erişim Computer Misuse Act'ın 1. ve 2. maddesinde cezalandırılır. Birisinin banka kayıtlarına girmek ve şifrenin kırılması hebasında oynamalar yapılması bu kapsamda değerlendirilir. İngiltere'de bir kimsenin banka hesabı ile ilgili yetkisiz bağlantı kurularak dolandırıcılık yapmak amacı ile bağlantı kurulması suç olarak kabul edilip suçu işleyip işlemediğine bakılmaz. Bir kimsenin başkasını ikna etmek için sahte belge düzenlemesi suç olarak düzenlemiş. Bunu resim, disket, ses bantları üzerindeki verileri değiştirerek işlemesi durumunda bilişim sistemi kullanılarak işlenen sahtecilik eylemleri oluşur.

1.3. İtalya

İtalya'da bilişim Suçlarına İlişkin düzenlemeler 23 Aralık 1993 tarihli 547 sayılı kanunla düzenlenmiştir.

İtalyan ceza kanunu bir bilişim programını tamamen veya kısmen tahrip etmek, değiştirmek, silmek veya bilişim ya da telematik sistemin işlenmesini engelleme veya bozma eylemlerinin mala zarar verme suçu olarak düzenlemiştir. Bilişim sistemlerine hukuka aykırı olarak girme veya bilişim sisteminde rıza göstermeye yetkili kişinin rızası olmaksızın kalma eylemlerini de suç olarak tanımlamaktadır.[57]

İtalya'da 03.08.1998 tarih ve 269 sayılı Kanunun ilgili maddesi, küçüklerin pornografik yayınlar da kullanılması suçunun internet aracılığıyla işlenmesi halini özel olarak düzenleme altına almıştır. Bu düzenleme ile her ne kadar küçüklerin pornografik materyaller de kullanılmasının önlenmesi çalışılsa da internet üzerinde bir denetim sistemi getirilerek kişi özgürlüklerinin sınırladığı için pek çok eleştiriye maruz kalmıştır.[58]

İtalya'da mala zarar verme suçu 392/3 maddesinde düzenlenmiştir. Bilişim sistemini tamamen değiştirmek, silmek, yok etmek, tahrip etmek, programın işlemesine engel olmak. Suç olarak düzenlenmiştir. Kamusal yararı bulunan bilişim veya Telematik sistemlere zarar verme veya yok etme İtalya Ceza Kanunun 420/2 maddesinde düzenlenmiştir. Bu maddede kamusal yararı bulunan bilişim sistemine zarar verme cezalandırılmaktadır. Eylem teşebbüs aşamasında kalsa bile ceza alır.

Bilişim veya Telematik Haberleşmenin Dinlenmesi, Engellenmesi veya Araya Girilmesi 617 quarter maddesinde düzenlenmiştir. Bilişim veya telematik haberleşmelerinin hukuka aykırı olarak; dinlenmesi, engellenmesi veya araya girilmesiyle ilgilidir. İletişimin içeriğinin herhangi bir kitle iletişimi aracıyla ifşa edilmesi de suç olarak düzenlenmiştir. Bu suç şikayete tabidir;

---

[57] Yener Ünver, a.g.e, s. 67, 68.
[58] Hasan Sınar, İnternet ve Ceza Hukuku, Beta Yayınevi, İstanbul, 2001, s. 96, 97.

ancak özel ağırlatıcı sebepler varsa resen kovuşturma yapılmaktadır. Bu özel ağırlaştırıcı nedenler;

1- Suçun devlet, kamu kuruluşu veya kamu hizmeti gören kuruluşların kullandığı bilişim sistemi veya telematik bir sistem zararına işlenmiş olması veya

2- Bir kamu görevlisi veya hizmetlisinin görev ve yetkilerini kötüye kullanarak veya sistem operatörlerinin bu sıfatlarını kötüye kullanarak işlemesi veya

3- Özel dedektiflik yetkisinin kötüye kullanılarak işlenmesi.[59] Suç olarak kabul edilmiştir.

Bilişim sistemi, veri veya programın özel olarak Tahrip Edilmesi 635 bis maddesinde düzenlemiştir. Başkasına ait bilişim sistemi programı verilerinin tamamen tahrip edilmesi ve kullanılamaz hale getirilmesi suç olarak düzenlenmiştir. Eylemin sistem operatörlüğü sıfatının kötüye kullanılması suretiyle işlenmesi halinde cezayı arttırmak gerekir.

Bilişim Dolandırıcılığı da 640bis maddesinde düzenlenmiştir. Bilişim sistemi yoluyla işlenen dolandırıcılığı düzenlemektedir. Bir bilişim sistemini veya telematik sistemin işlemesini herhangi bir şekilde değiştirerek veya bu tür sistemlerdeki veri veya programlara hukuka aykırı şekilde müdahale ederek başkasının zararına veya başkasının yararına haksız kazanç elde edilmesi suç sayılmış bu suçun basit hali suçta zarar görenin şikar yeti üzerine kovuşturmaya tabidir. Bu fiil bir sistem operatörü görevinin kötüye kullanılması suretiyle işlenmişse, resen takip yapılır ve cezada artırım söz konusudur.[60]

[59] Ali Karagülmez, a.g.e, s. 108.
[60] Yener Ünver, a.g.e, s.67, 68.

Bilişim sistemleri kullanılarak kara para aklama suçlarının ve hazırlık hareketlerini dahi cezalandırılmasını sağlayan 356/1992 sayılı kanun kabul edilmiştir.[61]

1.4. Almanya

Bilişim alanın da internet ortamında işlenen suçlarla ilgili kimlerin sorumlu tutulacağı konusunda, Kıta Avrupa'sındaki ilk çalışma ve düzenlemeler Almanya tarafından yapılmış. Bu tür yayınlarda kimlerin sorumlu tutulacağını açık bir biçimde saptayan 13.06.1997 tarihinde kabul edilen ve 1.8.1997'de yürürlüğe giren Tele Servisler Yasası 5. paragrafında internet yayınlarındaki süjelerin durumuna cezai açıdan açıklık getirmiştir.[62] Yu yasada internetteki herhangi bir yayının içeriğini hazırlayan içerik sağlayıcı, o yayında yer alan yazı, resim ve diğer materyaller suç unsuru taşıyorsa bunları kendisi hazırladığından genel hükümlere göre sorumlu olacaktır. Yasa'da, erişim sağlayıcılarının ceza sorumluluğu altında bulunmadıklarını hükme bağlamıştır. Servis sağlayıcılar ise ana bilgisayarda depoladıkları başkalarına ait suç içerikli bilgilerin bu niteliğinden haberdar olmaları ve ayrıca bu bilgilerin internet üzerinden erişilebilir kılınmasını teknik olarak önleme olanağına sahip bulunmaları halinde bu bilgilere erişimi önlemezlerse, belirtilen ihmali davranışından dolayı sorumlu tutulabilecektir.[63]

Veri casusluğu (m. 202 a) maddesindeki 1 numaralı fıkrasına göre her kim yetkisiz şekilde, kendisi veya başkası için yetkisiz erişime karşı özel olarak korunan sistemden veri elde ederse, üç yıla kadar hapis veya para cezasıyla cezalandırılmaktadır. 2 numaralı fıkraya göre ise 1 numaralı fıkrada

---

[61] Yener Ünver, a.g.e, s. 68, 69.

[62] Fatih Selami Mahmutoğlu, "Karşılaştırmalı Hukuk Bakımından İnternet Sujelerinin Ceza Sorumluluğu "İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, C. lıx. S. 1-2, İstanbul, 2001,s 43.

[63] Schreibaver Marcus, Strafrechtliche Verantwortliclikeit für Delikte im İnternet, Handbucuh Zum internetrecht 2. Auflage, Düsseldarf, 2002, S. 618, Levent Kurt Açıklamalı-İçtihatlı Tüm Yönleriyle Bilişim Suçları ve Türk Ceza Kanunundaki Uygulaması, Seçkin Yayınları, Ankara, 2005, s. 108.

sözü edilen veri tanımlanmıştır. Buna göre veri, elektronik, manyetik veya gözle görülemeyen herhangi bir şekilde depolanan ve iletilen şeylerdir.[64]

Verilerin depolandığı ve işlendiği bilişim sistemi ağına hukuka aykırı olarak girmek ve burada bulanan verileri hukuka aykırı olarak ele geçirmek suçuna, sır aleyhine işlenen suçlar arasında yer verilmiştir.[65] 263 a fıkrasında delil niteliği taşıyan belgelerde yapılan sahtecilik eylemlerini sahtekârlık suçları kapsamında 269 ve 270. maddelerde incelenmektedir. Yani bilgisayar programına girilerek bir belge sahte olarak üzerinde değişiklik yapılarak temin edilip kullanılırsa sahtekârlık suçu kapsamında değerlendirilir.

Veri Değiştirme, m. 303a maddesine göre her kim hukuka aykırı şekilde verileri siler, yok eder, kullanılamaz hale getirir veya değiştirirse, iki yıla kadar hapis veya para cezasıyla cezalandırılmaktadır.[66] Bu madde Nas-ı Izrar mala zarar verme suçunu düzenleyen hükümler çerçevesinde cezalandırılmaktadır.

Bilgisayar sabotajı, m. 303b maddesine göre her kim idareye veya kuruluşa ya da teşebbüse ait temel öneme haiz bir veri sürecini engellerse (yok ederse) beş yıla kadar hapis veya para cezasıyla cezalandırılmaktadır.[67] Bu 303 maddesinin b fıkrasına göre fail bir iş ya da işyeri için veya devlet otoritesi için çok önemli olan bilgi işlemi engellerse cezalandırılmaktadır.

14.12.2001 Tarihinde Tele servisler Kanununda değişiklikler yapılarak internet kişilerinin sorumluluk alanları genişletilmiştir.[68] 01.08.1996 yılında yürürlüğe giren Telekomünikasyon Kanunu 12.07.1996 tarihli Telekomünikasyon Hizmeti Girişimleri Bilgi Koruma Yönetmeliği ve

---

[64] Ali Karagülmez a.g.e, s. 119.
[65] Ayhan Önder, Şahıslara ve Mala Karşı Cürümler ve Bilişim Alanında Suçlar, Filiz Yayınevi, İstanbul, 1994, s. 505.
[66] Ali Karagülmez, a.g.e, s. 119.
[67] SchJolberg, Stein "The Legal Framework-Unauthorized Access To Computer Systems, penal Legislation in 44 Countries", (Updated April 7, 2003), http:/ www. Mosstingrett.no/info/legal.html (8.8.2004), Ali Karagülmez, a.g.e,s. 119.
[68] R. Barış Erman, ''Alman Hukukunda İnternetten Kaynaklanan Ceza Sorumluluğu'', İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, cilt 59, İstanbul, 2001, s. 204

01.08.1997'de yürürlüğe giren bilişim ve İletişim Servisleri Kanunu mevcuttur.[69]

Alman Teleservisler Kanunu'nun 6, Haksız Rekabet Kanunun 4, 6c, 17; Fikri Haklar Kanunu'nun 106, 107, 108, 108a, Telekomünikasyon Müşterilerin Korunmasına İlişkin Tüzük'ün 18, İlaçlar Hakkında Kanun'un 43, Tütün Vergisi Hakkında Kanun'un 20, Tütün Vergisi Hakkında Kanun'un Yürürlüğüne İlişkin Tüzük'ün 22b, Medeni Kanun'un 312 e, 318 ve 661a, Federal ve Federe nitelikteki çeşitli/basın kanunlarının ilgili hükümleri, verilerin korunması hakkında kanun Gençliği Tehlikeye Sokan Yayınlar Hakkında Kanun ve Gençliğin Toplum içinde korunmasına ilişkin kanun'un ilgili hükümleri. [70]

1.5. Danimarka

Danimarka'da bilişim suçlarına ilişkin hukuki düzenleme mevcut Ceza Kanununda 05. Haziran 1985 tarih ve 229 sayılı kanunla yapılan değişikliklerle oluşturulmuştur.[71] Bu kanunun 284, 280, 283, 193 maddeleri değiştirilerek ve 279a maddesi eklenerek bilgisayar marifetiyle dolandırıcılık yapılması, bilgisayar veri ve programları üzerinde gerçekleştirilen işlemler marifetiyle bilgisayarların fonksiyonları üzerinde değişikliklere sebebiyet verilmesi ve ticari ve kişisel nitelikteki sır aleyhine işlenecek eylemler Ceza yaptırımı altına alınmıştır.[72]

Danimarka CK'nun 235/1. paragrafı çocuklara ilişkin pornografik film, fotoğraf ve benzeri şeylerin satışını dağıtımını materyalin bu amaçla üretimini veya çoğaltılmasını cezalandırırken, 235/2 paragrafı ise, hem çocuklarla cinsel ilişkiyi gösteren fotoğraf, film ve benzeri materyali bulundurmayı hem de çocuklarla hayvanlar arasındaki cinsel ilişkiyi gösteren benzer materyalin bulundurulmasını suç olarak düzenlemektedir. Aynı kanunun 263/2. paragrafı

[69] Murat Volkan Dülger, a.g.e, s. 96.
[70] Yener Ünver, a.g.e, s.70.
[71] Hatice Akıncı, a.g.e, s. 159-275.
[72] R. Yılmaz Yazıcıoğlu, (2001), a.g.e, s.72

başka kimselerin elektronik verilerin depolandığı sistemdeki verilere veya programlara yetkisiz olarak girilmesi eylemini cezalandırmaktadır. Danimarka CK'nun ırk, renk, ulus, inanç, cinsel tercih ayrımcılığı nedeniyle geniş bir çevreye yönelik yapılan tehdit eylemlerinin suç olarak düzenleyen 266.b paragrafındaki tanım, interneti de kapsayacak genel ifadeler kullanmış ve keza 267/3. paragrafı da aynı şekilde, hakaret suçunun yazılı olarak veya (internet dahil) başka bir tarzda işlenmesinin hakim tarafından o suça ilişkin cezanın tespit ve tayininde dikkate alınacağı hükmünü içermektedir. Nihayet Danimarka CK'nun 279a maddesi doktrinde "bilgisayar dolandırıcılığı" diye adlandırılan suç tipini düzenlemiş ve Nas-ı Izrar suçunun düzenleyen 291 vd paragraflarında kullanılan terimler ise bilgisayar ve interneti de kapsayan terimler olduğundan bu şekilde yapılacak eylemler anılan maddeler kapsamında değerlendirilir.[73]

1.6. Avusturya

Avusturya ceza kanununda da bilişim suçları için genel düzenleme yapılmıştır.

Avusturya ceza kanunun 126a paragrafı verilere zarar verilmesini suç olarak düzenlemektedir. Bilişim sistemindeki verileri haksız surette değiştiren, silen veya başka bir şekilde kullanılamaz hale getiren veyahut gizleyen kimseyi cezalandırmaktadır. (f.1). Veriler olarak gerek kişisel ve kişisel olmayan gerek programları tanım ve kabul eden (f.2). Bu hükme göre, eylemin verdiği zararın belirli bir miktarı aşması hali cezayı ağırlatıcı nedendir. (f.3)

Avusturya Ceza Kanunun 148a paragrafı ise bilişim sisteminin kötüye kullanılması suretiyle işlenen dolandırıcılık eylemlerin, cezalandırmaktadır. Madde metni Avusturya Ceza Kanunun 126a/2 paragrafındaki eylemlere atıfla bu eylemlerin yapılmasıyla gerçekleştirilen dolandırıcılık niteliğindeki eylemleri cezalandırırken, hem dolandırıcılık hem de bilişim sistemine zarar

[73] Yener Ünver, a.g.e, s. 73.

verici eylemleri aynı normla cezalandırmaktadır.(f.1). Diğer yandan zararın belirli bir miktarı aşması bu suç açısından da cezayı ağırlatıcı nedendir. (f.2)

Avusturya Ceza Kanunu'nun ispat araçlarında sahtecilik (prg.293) ve ispat araçlarının koğuşturma organlarına ibrazından kaçınma, bunlara zarar verme ve gizleme (prg. 295) suçunu düzenleyen hükümlerde kullanılan terimler; bilgisayar ve internetin araç olarak kullanıldığı tipik eylemleri de içeren terimlerdir.[74]

1.7. İsveç

İsveç'te 1973 tarihinde veri korunması Kanunu çıkarılmış bu kanunun 22. maddesi 1982 yılında değiştirilerek veriler üzerinde tahrifat yapılması suç haline getirilmiştir.[75] İsveç Ceza Kanununda bilgi hırsızlığı ve bilgi sistemlerinin ihlal etme bilgisayarlara yasa dışı giriş ya da verileri kötüye kullanma şeklinde düzenlenmiştir.[76]

İsveç Ceza Kanunu'nun 4. babının 9c paragrafı elektronik bilişim sistemine izinsiz girilmesi, verilerin izinsiz değiştirilmesi, silinmesi, başka bir yere nakli, kopyalanması, 10. paragrafı verilere müdahaleye teşebbüs ve hazırlık yapılması, 9. babın 1/2 paragrafı bilişim sistemi aracılığıyla dolandırıcılık, 16. babın 10a ila 12. paragrafları çok ayrıntılı olarak çocuk pornografisi eylemlerini suç olarak düzenlemektedir.[77]

1.8. Polonya

Polonya CK'nun 267. maddesi bilgi naklede iletişimin elektronik, manyetik veya diğer özel güvenliğine müdahaleyle bilgilerin ele geçirilmesini ve 268. maddesi bilişim sistemlerindeki enformasyona müdahale eylemlerini cezalandırırken 269/1. maddesi ise bilgisayardaki ülke savunması trafiğin güvenliği, hükümetin veya devlet idaresindeki başka bir organın yönetim

[74] Yener Ünver, a.g.e, s. 72.
[75] Hatice Akıncı, a.g.e, s. 203
[76] Yener Ünver, a.g.e, s. 73, 74.
[77] İsmail Ergün, a.g.e, s. 71.

yeteneği veyahut mahalli idare için özel önemi olan bilgilere zarar vermek, silmek, değiştirmek, verilerin muhafazası veya naklinin engellemek veya yavaşlatmak eylemlerini cezalandırmaktadır. Aynı kanunun 269/2 maddesi bu tür cihazları veya onların işlem yapma yeteneğine zarar vermek v.b. eylemleri suç olarak düzenlemekte 278. maddesi kazanç elde etmek amacıyla başkalarının bilgisayar programlarına müdahaleyi ve 287. maddesi de bilgisayar dolandırıcılığı eylemlerini suç olarak düzenlemiştir. Polonya ceza kanununun malvarlığına ilişkin hükümleri arasında düzenlenen 293. maddesi ise, bilgisayar programlarını zarar verici eylemlerden koruyucu hükümleri ihtiva etmektedir. Polonya Ceza Kanunun 202/3 maddesinde ise çocuklarla ve hayvanların görüntülerinin pornografik eser üretiminde kullanılması eylemini cezalandırmaktadır.[78]

1.9. İsviçre

İsviçre'de 01.01.1995 tarihinde yürürlüğe giren 17.06.1994 tarihli kanunla "Federal Ceza Kanunu"nda değişiklik yapılmış ve bilişim suçları düzenlenmiştir.[79] Federal Ceza Kanunu yasal olmayan yollardan teknolojik bilgi edinme bilgi çalma ve bilgileri bozma gibi suçların cezalandırılmasını içermekte "Haksız Rekabet Kanunu" ise ticari amaçlı bilişim suçlarını içermektedir.[80]

İsviçre Ceza Kanununun 143 bis, 144 bis maddeleri bazı bilişim suçlarını, 27ıter, 27 quarter ve 340ter maddeleri internet sujelerini düzenlemektedir. Bu kanundaki 143.madde verilerin aşırılmasını, 143-bis madde bir bilişim sistemine izinsiz girilmesini, 147. madde bir bilgisayarın hileli kullanımını 148. madde banka ve kredi kartlarının kötüye kullanılmasını düzenlemektedir.[81]

---

[78] Yener Ünver, a.g.e, s. 74
[79] Levent Kurt, a.g.e, s. 111
[80] Levent Kurt, a.g.e, s. 111.
[81] İsmail Ergün, a.g.e, s. 71.

1.10. Hollanda

HOLLANDA 01.03.1993 yürürlük tarihli 20 Aralık 1992 tarih ve 33 sayılı kanunla ceza kanununda değişiklik yapılmış ve bilişim suçlarında düzenleme yapılması yoluna gidilmiştir. Bu değişiklikle siber suç sözleşmesindeki maddeler karşılanmıştır.

Hollanda Ceza Kanununun 80- quinquires, 80 sexies, 98, 98a 98b, 138a, 139b, 139c, 139d 139e, 161-sexies, 161-septies, 232, 273, 317, 318, 326, 326c, 350a, 350b, 351, 374-bis, 441a, gibi maddeleri kısmen değiştirilmiş, kısmen de yeni hükümler eklenerek bilişim sistemindeki kamusal sırlara ilişkin bilgilerin hukuka aykırı olarak elde edilmesi, bilişim sistemine hukuka aykırı olarak girilmesi, kapalı yerlerin bilişim cihazlarıyla dinlenmesi, iletişim veya veri nakline müdahale yapılması, hukuka aykırı, olarak verilerin kaydedilmesi bilgileri otomatik olarak işleme tabi tutan ve bir arşiv sisteminin tahrip edilmesi veya engellenmesi, manyetik kartlar marifetiyle sahtecilik yapılması, üretime ilişkin sırların ortaya çıkartılması, telekomünikasyon sistemlerine yönelik ihlal eylemleri, bilgileri otomatik olarak işleme tabi tutan veya nakline yarayan sistemlerdeki verilerin değiştirilmesi, silinmesi, tahrip edilmesi, bu sistemlere yönelik nası ızrara eylemleri müeyyide altına alınmıştır.[82]

1.11. İrlanda

Ülkede yatırım yapan ABD firmalarının da etkisiyle bilgisayar üretimi, satışı, program yazılımı ve enformasyon teknolojisine yatırım açısından Avrupa Birliğinin en önde gelen ülkesi konumunadır.

Bilişim Suçları ile ilgili temel kanunlar olmasa da 1991 yılında yasalaşan “Criminal Damage Act” bilişim suçları ile ilgili geniş tanımlamalar yapmaktadır. Bu yasa dört temel suçu ortaya koyar.

1- Mülkiyete zarar verme (bilgisayarlar ve veriler dahil)

[82] R. Yılmaz Yazıcıoğlu, (1997), a.g.e, s. 174.

2- Mülkiyete zarar vermek amacıyla tehdit etmek

3- Bilgisayara yetkisiz giriş

4- Bilgisayara zarar vermek niyetiyle sahip olunan her şey (Ör. Virüsler).[83]

İrlanda da bilişimle ilgili diğer kanunlar ise 1963 tarihli The Copyright Act. 1992 tarihli The Criminal Evidence Act, 1988 tarihli Teh Data protection Act, 1983 tarihli The postal and Telecommunications Services Act, 1998 tarihli The Child Trafficking and Pornography Act'dır.[84]

1.12. İspanya

İspanyada bilişim suçları ile ilgili ceza kanunundaki genel maddeler uygulanmaktadır, özel bir düzenleme yapılmamıştır.

İspanya Hükümeti, İçişleri Bakanlığı, Emniyet Genel Müdürlüğü bünyesindeki bir birim oluşturup enformasyon teknolojilerindeki Suçları Araştırma Birimi adı altında faaliyet gösteren emniyet görevlileri teknoloji iletişim telekomünikasyon ve çocuk pornografisi alanında işlenen suçları ve ortaya çıkan şikayetleri takip eder. Bunun dışında şirketler, firmalar ve şahıslar tarafından, bilişim suçlarından korunma amaçlı hazırlanmış yazılımlar aracılığıyla korunmaktadır.

2. DİĞER DÜNYA ÜLKELERİNDEN BAZILARINDA BİLİŞİM SUÇLARI

2.1. Japonya

Japonya'da teknolojisinin gelişmiş olması nedeniyle bilişim suçları ile erken tanışmış ve erken tedbir alan ülkelerden biridir. Japonya Ceza Kanununa 22 Haziran 1987 tarihinde bilişim suçları ile ilgili maddeler

[83] EGM Raporu, www. Bilişimşurası.org.tr/dosyalar/10.doc.
[84] Hatice Akıncı, a.g.e, s. 203.

eklenmiştir. 13.02.2000 tarihinde de "İnternete Haksız Girmenin Yasaklanması Hakkındaki Kanun" yürürlüğe girmiştir.[85]

Japonya'da var olan mevzuata göre bir sisteme izinsiz giriş yapmak o izinsiz giriş ile elde edilen bilgiler satılmadıkça ya da bozulmadıkça suç sayılmamaktadır.[86]

Japon ceza kanununun 246. maddesinde, düzenlenen bilgisayar dolandırıcılığını, Alman Ceza Kanunu ile büyük oranda benzerlik göstermektedir. 75. maddesinde de Cyber-pornografy eylemleri düzenlenmiştir.[87]

2.2. Rusya

Rusya G-8 ülkelerinin 1997 yılında Washington'da yaptıkları Adalet ve İçişleri Bakanları toplantısında kabul edilen bildiri ile "Ulusal Temas Noktaları" oluşturulmasına karar verilmesinden sonra İçişleri Bakanlığı bünyesinde ulusal temas noktası oluşturup bilişim suçları ile ilgili düzenlemelere yer vermiştir. Rus Ceza Kanununun haberleşme özgürlüğünü koruyan 138. maddesindeki tanımda kullanılan terimler bilgisayar ve interneti de içeren terimler olup bu araçlar da madde metni kapsamındadırlar. Rus Ceza Kanununu 242. maddesi Çocuk-Yetişkin ayrımı yapmadan ve internet ile bilgisayarı da kapsar tarzda genel ifadelerle kanuna aykırı pornografik materyalin çoğaltılması ve üretimi cezalandırılmaktadır. Aynı Kanunun 152. maddesinde çocuk ticareti ve kaçırılması eylemleri suç olarak düzenlenmiştir. Rus CK'nun 28. babı enformasyon alanındaki suç tiplerine yer vermekte ve 272. maddesinde bilgisayar verileri ve programlarına hukuka aykırı biçimde müdahale etme 273. paragrafında bu veri ve programlara zarar verecek programların üretimi, kullanımı ve çoğaltılması eylemlerini yapmak ve 274.

---

[85] Yener Ünver, a.g.e, s. 75,76.
[86] Önder Demir, İnternet Servis Sağlayıcısının Cezai Sorumluluğu, http://bilişimşurası.org.tr./dosyalar/28.txt, 12.08.2009.
[87] Yener Ünver, a.g.e, s. 76.

paragrafında ise, bilişim sistemine ilişkin kuralların ihlali suç olarak düzenlenmiştir.[88]

2.3. Malezya

Bilişim teknolojisinin hızla geliştiği ülkelerden biridir. Malezyadaki bilişim suçlarına ilişkin kanunlar "Digital Signature Act", Multimedia Convergence Act", "Telemedicine Development Act"'tir. Bu kanunlarda yer alan bilişim suçları;

1- Bilgisayara izinsiz nüfus etme hasar verme

2- Kullanıcı şifresi alışverişi

3- Telif haklarının ihlali

4- Marka Sahteciliği

5- Ticari sırları çalma

6- Çocuklara yönelik istismar ve müstehcenlik

7- İnternet dolandırıcılığı

8- İnternet tacizi

9- İnternet ile tehdit, korku, panik, huzursuzluk yayma suçları düzenlemiştir.[89]

2.4. Singapur

Bilgisayar üzerinde işlenen suçlarla mücadelede "Computer Misuse Act"! isimli kanun ile elektronik ticareti düzenlemek ve yapılan işlemleri hukuka uygun hale getirmek için "Elektronik Transaction Act" yasaları

[88] Yener Ünver, a.g.e, s. 75.
[89] EGM Raporu: http://www. bilisimsurası.org.tr./dosyalar//10.doc

düzenlenmiştir.[90] Computer Misuse Act'de bilişim suçları şu şekilde sıralanmıştır.

1- Yetkisiz olarak bir bilgisayara veya sisteme girmek.

2- Suça yardımcı olmak maksadıyla veya bu amaçla sisteme girmek

3- Bilgisayarda saklı bilgileri yetkisiz değiştirmek, silmek.

4- Bilgisayar kullanımını önlemek ve işlenemez hale getirmek.

5- Yetkisiz bir bilgisayar hizmetinden yararlanmak.

6- Şifreleri çalmak veya bunları açıklamak.[91]

2.5. Kanada

Kanada'da Temel Ceza Kanununda 1985 yılından itibaren yapılan değişikliklerle bilişim suçları tanımlanmış. Ceza Kanununun 342. maddesinde hakkı olmadan ve sahtekârlık yoluyla elektromanyetik, akustik, mekanik veya başka bir cihaz yoluyla bir bilgisayar sistemini dolaylı veya doğrudan kesintiye uğratan herkesin cezalandırılacağının hükme bağlanacağını belirtmiştir.[92]

2.6. Finlandiya

28 Ağustos 1990 yılında temel Ceza Kanununda bazı değişiklikler yapılmıştır. Bunlar;

1- Bilişim cihazına hukuka aykırı olarak girilme.

2- Koruma altındaki bilişim sistemine girerek endüstriyel casusluk yapma,

3- Delil niteliği taşıyan bilişim verilerine ilişkin sahtecilik

[90] Levent Kurt, a.g.e, s. 112, 113.
[91] EGM Raporu, www. bilisimşurası. Org.tr/dosyalar//10.doc
[92] Levent Kurt, a.g.e, s. 111.

4- Bilişim sistemlerindeki verilere ilişkin nas-ı ızrar ve bilişim marifetiyle işlenen dolandırıcılık eylemleri cezai yaptırım altına alınmıştır. Ceza kanunun 28. kısmına 7, 8, 9. maddeler, 30. kısmına 4. madde, 33. kısmını da 1, 2, 3 ve 6. maddeler 35. kısmına da 1, 2, 3. ve 36. kısmına da 1, 2, 3. maddeler ilave edilmiştir.[93]

2.7. İsrail

1995 yılında yürürlüğe giren Bilgisayar Kanunu ile bilişim suçlarını düzenleme altına almış ve İsrail bilişim suçları ile mücadele etmek için ABD başta olmak üzere birçok Avrupa ülkesiyle işbirliği ortak mücadele antlaşması imzalamıştır.

2.8. Avustralya

Avustralya'da bilişim sahtekârlığıyla ve organize olmuş bilişim suçlarıyla ilgili olarak araştırma ve çalışmalar yapan National Crime Authonity (NCA). (Ulusal suç Dairesi) bulunmaktadır.[94]

Avustralya Ceza Kanunu (Criminal Code Act 1995) "The Cybercrime Act 2001" adlı kanun ile 2001 yılında değiştirilmiş ve mevcut bilişim suçları güncellenmiştir. Avustralya Ceza Kanunun 477.1 maddesinde yetkisiz erişim veriler de değişiklik yapmak ve veri erişimini engellemek suçu düzenlenmiştir. Buna göre bir kimse;

1- Bilerek ve isteyerek

2- Yetkisiz erişim veya verilerde değişiklik veya erişimi engelleme yaparsa

3- Bu fiiller aşağıdaki hallerde bir veya daha fazlasıyla ilgili olursa

a- Eyalet bilgisayarında bir veriyle ilgiliyse

---

[93] R. Yılmaz Yazıcıoğlu, (1997) a.g.e, s. 175.
[94] Ali Karagülmez, a.g.e, s. 95.

b- Eyalet namına bir bilgisayardaki veriyle ilgiliyse

c- (B)'deki fiiller, telekomünikasyon hizmetleri vasıtasıyla gerçekleştirilmiş ise suç işlenmiş sayılır; 2 yıl hapis cezası verilir. Bahsetmiş olduğumuz yukarıdaki fıkraların bulunduğu koşullardaki erişim veri değişikliği veya engelleme veya bozma, telekomünikasyon hizmetleri vasıtasıyla yapılmış ve elektronik iletişimin herhangi bir şekliyle gerçekleştirilmiş ise, en az beş yıl hapis cezası öngörülmüştür; (m. 477; 2, 477. 3)[95]

Avustralya da en çok görülen suçlardan biride kredi kartı kopyalanmasıdır. Bunun yanında ATM ve EFT POS makinelerine elektronik yolda müdahale ile bilgi iletişimini keserek de kartlara ulaşmakta Avustralya da görünen suçlardır.

2.9. Amerika Birleşik Devletleri

Teknoloji devi Amerika bilgisayarında anavatanı olması sebebiyle bilişim suçlarıyla ilk defa Amerika'da karşılaşılmıştır.

Amerika Federal bir yapıya sahip olduğundan dolayı her eyalette bilişim suçları ile ilgili düzenleme vardır.

Amerika'da 1984 yılında Erişim Aygıtlarını Taklit Etme ve Bilgisayar Dolandırıcılığı ve Bilgisayarı kötüye kullanma kanunu düzenlenmiştir. Bu kanun birkaç kez değişikliğe uğramış özel nitelikteki bilişim suçları düzenlenmiştir. Bu kanun ile kamu kuruluşlarının ve özel kuruluşlarının bilgisayarlarına karşı yapılan korsanlık eylemleri önlenmek istenmiştir.[96]

Korumalı bir bilgisayara hukuka aykırı olarak erişim ve bilgisayar verilerinin tahrip edilmesi ve değiştirilmesi eylemleri suç haline getirilmiştir.[97]

---

[95] Ali Karagülmez, a.g.e, s. 96, 97.
[96] Murat Volkan Dülger, a.g.e, s. 91-92.
[97] Hüseyin Çeken, Amerika Birleşik Devletlerinde Siber Suçlar, http://www. jura.uni-sb.de/turkish/HÇeken html 18.07.2009.

08.02.1996 tarihinde "İletişim Ahlaki Kanunu" İnternetin hukuksal sorunlarla ilgili çıkardığı ilk yasadır. Bu yasa internet üzerinde müstehcen içeriğe sahip resim, yazı, video klip vb. materyallerin yayınlanması ve iletilmesi ile şiddet içeren yayınların gerçekleştirilmesini suç olarak düzenlemiştir.[98]

30.09.1996 tarihinde de çocuk pornografisi konusunda "Çocuk pornografisi konusunda "Çocuk pornografisinin önlenmesi Kanunu" çıkarılmıştır. 1998 yılında da "Çocukların on-line olarak korunması Yasası" internet üzerindeki çocuk pornografisi ticaretini engellemeyi amaçlamıştır.[99] Bu kanun düşünce ve fikir özgürlüğünün ihlal ettiği ve temel yasaya aykırı olduğu gerekçesi ile iptal edilmiştir.[100]

ABD'de kişilerin kimlik bilgilerine hukuka aykırı olarak ulaşılmasını engellemek için Hüviyet Hırsızlığı Yasası 1998 yılında kabul edilmiştir.23.07.2007 tarihinde de internet kumarının yasaklanması yasası çıkarılmıştır.[101]

Bu kanunun çıkarılmasında ki amaç kişilerin sosyal güvenlik numarası ile ulaşılan kişisel bilgilerinin hukuka aykırı kullanılmasını engellemektir.

ABD'de elektronik haberleşmenin gizliliğini hukuka aykırı bir şekilde ihlal edilmesinin önlenmesi için 1986 yılında "Elektronik Haberleşmenin Gizliliği Yasası" çıkarılmıştır.[102]

Bilişim suçları ile mücadele etmek için CIA "Information Warfore Center" adında FBI ise "National Infrasturucture proterction Center" ve "Computer Crime Scuad" isimli çalışma gruplarını kurmuştur.[103]

---

[98] Fatih Selami Mahmutoğlu, (2001), a.g.e, s.41,42.
[99] Fatih Selami Mahmutoğlu, a.g.e, s. 42-43.
[100] Kayıhan İçel, Kitle Haberleşme Hukuku, Basın, Radyo- Televizyon, Sinema, İnternet, Beta Yayınları, İstanbul, 2001, s. 414, 415
[101] Hüseyin Çeken, ABD de İnternet Yoluyla İşlenen Suçlara İlişkin Düzenlemeler, Askeri Adalet Dergisi sayı:114, İstanbul, 2002, s. 95.
[102] Hasan Sınar, a.g.e, s. 96.
[103] Hüseyin Çeken, a.g.e, 18.07.2009

Görüldüğü üzere bilişim suçları ile mücadelede Amerika Birleşik Devleti önlem almada en önde gelen devletlerden biridir. Bilişim suçları açısından bütün dünyaya da örnek oluşturmaktadır.

3. SİBER SUÇ SÖZLEŞMESİ

Avrupa Konseyi Siber suç sözleşmesi denir. Avrupa Konseyinin ilk çalışması 1980'li yıllarda yapılmıştır. Avrupa Konseyi Bilişim Suçları ile ilgili bir takım tavsiye karaları almıştır. Bunlar;

1- Suç içerikli konularda karşılıklı yardımlaşmayla ilgili Avrupa konseyinin uygulamaya ilişkin R (85) sayılı Tavsiye kararı

2- Telif ve telife ilişkin haklar üzerinde korsanlığı düzenleyen R (88) 2 sayılı Tavsiye kararı

3- Güvenlik kuvvetlerinin şahsi bilgileri kullanmasını düzenleyen R (87) 15 sayılı Tavsiye Kararı

4- İletişim hizmetleri ve bu çerçevede özellikle telefon hizmetleri alanında kişisel verilerin korunması hakkındaki R (95) Sayılı Tavsiye Kararı.

5- Bilgisayarla işlenen suçların tanımlanmasına ilişkin olarak ulusal yasama organlarına yol gösteren ve bilgisayarla ilgili suçlar hakkındaki R (89) 9 Sayılı Tavsiye kararı

6- Bilgi Teknolojisi ile bağlantılı Ceza Muhakemeleri usul hukukunun açıkları hakkındaki R (95) 13 Sayılı Tavsiye Kararıdır.[104]

Avrupa Konseyi tarafından bilişim suçları ile mücadele için bir uzman komite kurulmasına karar verip 1997 yılında Avrupa Konseyi bakanlar Komitesi uzmanlarından Siber Suç kapsamına giren konulara ilişkin bağlayıcı

[104] Levent Kurt, a.g.e, s. 310

özelliğe sahip olacak bir metin hazırlamasını talep etmişler ve sözleşme gündeme gelmiştir.[105]

Uzmanlar tarafından hazırlanan sözleşmede yukarıdaki tavsiye kararları göz önünde bulundurularak bilgisayar aracılığıyla işlenen dolandırıcılık, sahtecilik, çocuk pornografisi, şiddet telif haklarına, tecavüz gibi eylemleri içeren ilk sözleşme olması bakımından önemlidir.

Uzmanlar komitesi 8. Haziran 2001de Avrupa Siber Suç Sözleşmesine son şeklini vermiş, 8 Kasım 2001 tarihinde de sözleşme Avrupa Konseyi Bakanlar Komitesince onaylanmıştır.[106]

23 Kasım 2001 tarihinde Macaristan'ın Başkenti Budapeşte de imzaya açılan otuz sekiz/Avrupa Konseyi üyesi ve dördü üye olmayan ülkelerde olmak üzere toplam 42 ülke tarafından imzalanmıştır.[107]

Sözleşme Avrupa konseyi üyelerinden Arnavutluk, Bosna Hersek, Danimarka, Ermenistan, Avusturya, Belçika, Bulgaristan, Hırvatistan, Kıbrıs, Estonya, Finlandiya, Fransa, Almanya, Yunanistan, Macaristan, İtalya, Lüksemburg, Malta, Moldovya, Hollanda, Norveç, Polonya, Portekiz, Romanya İrlanda İspanya, İsveç, İsviçre, İzlanda, Makedonya Slovakya, Slovenya, Ukrayna ve İngiltere üye olmayan ülkelerde ise Kanada, Japonya, Güney Afrika ve ABD sözleşmeyi imzalamıştır.[108] Türkiye henüz sözleşmeyi imzalamamıştır.[109]

Siber suç sözleşmesini Türkiye imzalamamakla beraber bu sözleşmenin Giriş bölümünde yollama yapılan temel uluslararası sözleşmeleri Türkiye imzalamıştır.

---

[105] Aslı Deniz Helvacıoğlu, a.g.e, s.59.

[107] Koray Doğan, Bilişim Suçları ve Yeni Türk Ceza Kanunu, http// adlibilisim.ite.edu.tr./AdliBilisim 2005 web/file/koraydogan.pdf.19/07/2009

[108] Aslı Deniz Helvacıoğlu, a.g.e, s. 278.

[109] Kayıhan İçel, "Avrupa Konseyi Siber Suç Sözleşmesi Bağlamında Avrupa Siber Suç politikasının Ana İlkeleri" İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, C. Iıx.s. 1-2, İstanbul, 2001,s. 9.

Sözleşmelerden bir kısmı bireyin düşüncelerini ifade etmesi her türlü bilgiye ulaşmak, bilgiyi iletmek ve özel yaşama saygıyı özellikle vurgulayan A.İ.H.S. (1950) B.M. Siyasal ve Sivil haklar Sözleşmesi (1996) Çocukları korumayı Amaçlayan B.M. Çocuk Haklarına Dair Sözleşme (1989), kötü koşullardaki çocuk işçiliğinin Yasaklanması ve ortadan kaldırılmasına ilişkin Acil önlemler Hakkında 182 Sayılı İLO Sözleşmesi (2001) gibi.[110]

3.1. Avrupa Konseyi Siber Suç Sözleşmesi Ve Temel Hükümlerinin İncelenmesi

3.1.1. Siber Kavramı

Sözleşmenin orijinal başlığında yer alan "cyber" kelimesi Türkçe'ye O siber olarak çevrilmiştir. Bunun en önemli nedeni siber sözcüğünün gelişimi içerisinde yüklenmiş olduğu kültürel ve dönemsel anlam bütünlüğüdür[111]. Merriam-Webster sözlüğünde “Cyber” kelimesinin etimolojik olara kökeninin “cybernetic”ten geldiği ifade edilmektedir. “Cybernetic”, otomatik kontrol sistemleri “sinir sistemi gibi) çerçevesinde iletişim ve kontrol teorisinin yer aldığı bilim dalı olarak tanımlanmaktadır. “Cyber” ise, “cybernetic”ten türemiş ve bilgisayar ağları için kullanılmıştır. 1980’li yıllarda, bilgisayar ağlarının çevrimiçi dünyası “Cyber space” olarak adlandırılmıştır[112].

Siber suç kavramı, “siber uzay ortamında işlenen suç” olarak tanımlanmaktadır. Dünyada bilgisayar ağlarında işlenen suçlara (crimes related to computer Networks) siber suçlar (cyber crime) tabiri kullanılmaktadır.” Siber suç deyimi, bilgisayarlar aleyhine veya bilgisayarlar aracılığıyla işlenen suçlar olarak ta tanımlanmaktadır[113].

---

[110] Füsun Sokullu Akıncı, “Avrupa Konseyi Siber suçlar sözleşmesinde yer alan Maddi Ceza Hukukuna İlişkin Düzenlemeler ve Özellikle İnternette Çocuk Pornografisi” İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, C LIX, S: 1-2, İstanbul, 2001. s. 35.
[111] İsmail Ergün, a.g.e, s. 13.
[112] Cengiz Tavukçuoğlu, Bilişim Terimleri sözlüğü, Asil Yayın Dağıtım, Ankara, 2004, s. 286.
[113] Hüseyin Çeken, a.g.e, 20.07.2009.

3.1.2. Avrupa Konseyi Siber Suç Sözleşmesi'nin Temel Hükümlerinin İncelenmesi

3.2.1.1. Sözleşmede Yer Alan Terimler

Sözleşmede bilgisayar sistemi, bilgisayar verisi, hizmet sağlayıcı ve trafik bilgisi tanımlarına yer verilmiştir. Bu terimlere açıklık getirilmesi ve tanımların kapsamlarının net bir şekilde belirlenmesi, sözleşme hükümlerinin anlaşılabilmesi ve etkin bir şekilde uygulanabilmesi açısından büyük önem taşımaktadır. Ayrıca Avrupa Konseyi Siber Suç Sözleşmesinin bu alanda kabul edilen ilk uluslararası anlaşma olması, sözleşmede yer verilen terimlere ülkeler arasında işbirliğini hızlandırma ve kolaylaştırma görevini de yüklemektedir.

3.2.1.2. Bilgisayar Sistemi

Bilgisayar sistemi ile ifade edilen donanım ve dijital verinin otomatik olarak işlenmesi için geliştirilmiş olan yazılımdan oluşan cihazdır. Bu tanım, girdi, çıktı ve saklama özelliklerini de kapsamaktadır. Sistem tek başına olabileceği gibi kendine benzer cihazlardan oluşan bir ağa da bağlı olabilmektedir.

Otomatikten kastedilen insan müdahalesinin bulunmamasıdır. Verinin işlenmesinden anlaşılması gereken, bir bilgisayar programı tarafından işletilen bilgisayar sistemi içersinde çalışan veridir. Bilgisayar programı istenilen sonucu almak için bilgisayar tarafından işletilen bir talimatlar bütünüdür. Bilgisayar farklı programlar işletebilir[114].

Bilgisayar sistemi genellikle farklı parçalardan oluşmaktadır; merkezi işletim ünitesi ve çevreselleri. Buna göre çevresel cihazlar işletim üniteleri ile karşılıklı ilişki içerisinde işleyen yazıcı, tarayıcı, CD okuyucu, yazıcı ya da diğer saklama cihazlarıdır.

---

[114] İnternet ve Hukuk Platformu, Ankara Barosu, Avrupa Konseyi Siber Suçlar Sözleşmesi Taslağı, Ankara, 2007. s. 65.

Ağdan anlaşılması gereken, bir veya daha fazla bilgisayar arasındaki ara bağlantıdır. Bu bağlantı kablo veya tel ile olabileceği gibi telsiz yani radyo, infrare veya uydu vasıtasıyla veya her iki yolla da olabilmektedir.

Ağ coğrafi olarak küçük bir alanla sınırlı kalabileceği gibi (yerel ağ), geniş bir alan içerisinde de geçerli olabilmektedir. Bu ağlar kendi aralarında da bağlantılı olabilirler. Internet birçok ara-bağlantılı ağdan oluşan küresel bir ağdır. Tüm ağlar aynı protokolleri kullanırlar.

Bilgisayar sistemleri ağlara son noktalar olarak bağlanabilecekleri gibi ağ üzerinde iletişimi sağlamaya yardımcı olmak amacıyla da ara bağlanmış olabilirler.

Farklı tiplerde de ağlar bulunmakta olup ister internete bağlı olsan, ister olmasın bilgisayar sistemleri arasında bilgisayar verisinin iletişimini sağlamaktadırlar.

3.2.1.3. Bilgisayar Verisi

Bilgisayar verisi tanımı "suitable for processing" "işlenmeye uygun" ifadesini içermektedir. Bu ifadeden anlaşılması gereken verinin bir bilgisayar sistemi tarafından doğrudan işlenecek formda bulunmasıdır. Bu sözleşme kapsamında veri, elektronik veya diğer doğrudan işlenebilir formda olan veri anlamında kullanılmaktadır[115].

3.2.1.4. Hizmet Sağlayıcı

Hizmet sağlayıcı tanımı, bilgisayar sistemlerindeki verinin işlenmesinde veya iletişiminde rol oynayan kişilere yönelik olarak kullanılan oldukça geniş kapsamlı bir ifadedir.

Hizmet sağlayıcı tanımı hem kamu hem de özel sektörü kapsamaktadır.

[115] İnternet ve Hukuk Platformu, a.g.e, s. 66.

Öte yandan hizmet sağlayıcı tanımı içerisinde, hizmetleri kullanan kişiler için verileri işleyen veya depolayan işletmeleri de bulundurmaktadır. Örneğin, ağa bağlantı sağlayan ve hosting hizmeti veren bir işletme bu kapsam içerisinde yer almaktadır[116].

3.2.1.5. Trafik Bilgileri

Trafik bilgileri özel bir hukuki rejime tabi olan bilgisayar verisi olup, iletişim zincirinde, iletişimi başlangıcından varış noktasına kadar sürdüren bilgisayarlar tarafından oluşturulmaktadır.

Trafik bilgisi suça yönelik soruşturmalarda kanıtların elde edilmesinde kullanılmaktadır.

Trafik bilgileri içerisinde iletişimin başlangıç noktası (telefon numarası, İP adresi gibi), rotası, zamanı, tarihi, büyüklüğü, süresi ve hizmetin sağlanma şekli (dosya transferi, e-posta gibi) bulunmaktadır[117].

3.2.1.6. Ulusal Düzeyde Alınacak Önlemler

Sözleşmenin hazırlanma sürecinde suç olarak kabul edilecek fiillerin tespitinde taraflar arasında görüş birliği sağlanması konusuna büyük önem verilmiş, bu nedenle OECD, Avrupa Konseyi, Birleşmiş Milletler gibi uluslararası kurumların çalışmalarından yararlanılmıştır.

Sözleşme, Kısım II altında Madde 2 ile 13 arasında yer alan suçlara karşı ortak asgari standartların oluşturularak bilgisayar veya bilgisayarla ilişkili suçların önlenmesini hedeflemektedir. Bu tip bir uyumun hem ulusal düzeyde hem de uluslararası düzeyde gerçekleştirilmesi gerekmektedir.

Ulusal düzeyde alınacak olan önlemler kapsamında maddi ceza hukuku bölümü 5 başlık altında toplanmıştır.

---

[116] İnternet ve Hukuk Platformu, a.g.e, s. 67.
[117] İnternet ve Hukuk Platformu, a.g.e, s. 68.

İlk başlıkta bilgisayara ilişkin temel suçlar (gizlilik, bütünlük ve bilgisayar verisi ile sistemin kullanıma açık olmasına yönelik temel tehditler) bulunmaktadır. 2, 3 ve 4'üncü başlıklar ise bilgisayarla ilişkili diğer suçlan kapsamaktadır. Bu suçlarda eylem öne çıkmakta ve bilgisayar ve teleko-münikasyon sistemleri hâlihazırda ceza hukuku ile korunan menfaatlere saldırmak amacıyla kullanılmaktadır. 2'inci başlıkta bilgisayarla ilişkili sahtecilik ve sahtekârlık, 3'üncü başlıkta ise bilgisayar sistemlerinin kullanılması ile çocuk pornografisinin kanunsuz olarak üretimine ve dağıtımına ilişkin fiiller yer almaktadır. Bu kapsam içerisinde taslağı hazırlayan komite ırkçı içeriklerin de bilgisayar sistemleri vasıtasıyla dağıtımının yapılmasını tartışmış, ancak nihai karara ulaşamayarak, bunun ek bir protokolde yer almasını kararlaştırmıştır. 4'üncü başlıkta ise, telif ve ilgili hakların ihlallerine ilişkin suçlar bulunmaktadır. Telif hakları ihlalleri bilgisayar veya bilgisayarlarla ilişkili suçlarda geniş olarak görülmektedir ve uluslararası etkilere sahip olmaktadır. 5'inci başlık suça yardım, teşvik ve teşebbüse yönelik hükümler içermektedir.

Sözleşme taslağı bilişim teknolojilerini kullanan suçlarla ilişkili olması nedeniyle nötr bir dil kullanarak hazırlanmış, ceza hukukunda yer alan fiillerin hem hâlihazırda hem de gelecekte kullanılacak olan teknolojilere uygulanabilmesi amaçlanmıştır.

Sözleşmede yer alan fiillerin temel özelliği, hakka sahip olmadan gerçekleştirilmiş olmalarıdır. Fiillerin suç olarak kabul edilebilmesi için gerekli unsur budur. Sözleşmeye konu olan fiiller rıza, meşru müdafaa veya gereklilik gibi durumlarda, suç kapsamı dışında bırakılacaklardır.

Aynı şekilde, kamu düzenini sağlamak, ulusal güvenliği korumak veya suça konu fiilleri araştırmak ve soruşturmak amacıyla gerçekleştirilen eylemler de suç kapsamı dışında kalmaktadır.

Sözleşmede suç olarak kabul edilen eylemlerin tümü kasıtlı olarak yapılmış olmalıdır[118].

3.2.1.7. Bilgisayar Veri ve Sistemlerinin Gizliliğine, bütünlüğüne ve Kullanımına Açık Bulunmasına Yönelik Suçlar

a. Yasadışı Erişim

Yasadışı erişim, bilgisayar sistemlerinin ve verisinin güvenliğine (gizlilik, bütünlük ve kullanıma açık bulunması) yapılan saldırıları ve tehlikeli tehditleri kapsamaktadır.

Yasadışı erişime yönelik en etkin korunma güvenlik önlemlerinin alınmasıdır. Oluşturulacak mevzuat ise caydırıcı bir etkiye sahip olmalıdır.

Erişim, bir bilgisayar sistemi veya bir parçasına yapılan giriş anlamına gelmektedir. Bilgisayar sistemi, donanım, parçalar, saklanan veri, trafik ve içerik verilerini kapsamaktadır. Ancak e-posta göndermek erişim tanımı kapsamında yer almamaktadır. Erişim, bir diğer bilgisayar sistemine veya aynı ağda yer alan bir diğer bilgisayara kamu telekomünikasyon ağları üzerinden yapılan giriştir.

Erişim, fiile izin veren hakka sahip olmadan ve kasıtlı olarak yapılmalıdır[119].

b. Yasadışı Müdahale

Madde 3, veri iletişiminin gizlilik hakkını korumaktadır. Yasadışı müdahale fiili telefon konuşmalarının kayıt edilmesi ile aynı ihlale dayanmaktadır. Sözleşmede suçun elektronik formdaki veriye yönelik müdahaleler şeklinde işlenmesi ifade edilmektedir. Burada bilgisayar sisteminin kullanılması ile gerçekleştirilmektedir.

---

[118] İnternet ve Hukuk Platformu, a.g.e, s. 68-74.
[119] İnternet ve Hukuk Platformu, a.g.e, s. 75-78.

"Kamuya açık olmayan bilgisayar verisi yayını", Madde 3 kapsamındaki suçlar için belirleyici özellik taşımaktadır. Kamuya açık olma, verinin değil, yayının özelliğidir. Örneğin, kamuya açık olan bir bilgi taraflarca gizlilik içerisinde iletilmek istenilebilir veya veri kablolu TV gibi, ticari amaçlar nedeniyle hizmet bedeli ödeninceye dek gizli tutulmak istenilebilir. Bu nedenle kamuya açık olmayan ifadesi kamu ağlarından yapılan iletişimler haricinde yapılan iletişimlerdir gibi bir genelleme yapılamayacaktır.

Çalışanların aralarında yaptıkları, iş dışı konular dâhil olmak üzere, bilgisayar verisinin kamuya açık olmayan yayını olarak kabul edilen iletişimler de Madde 3 kapsamında korunmaktadır.

Müdahale, fiile izin veren hakka sahip olmadan ve kasıtlı olarak yapılmalıdır[120].

c. Verilere Müdahale

Bu hükmün amacı, bilgisayar verisinin ve bilgisayar programlarının kullanımına, bütünlüğüne ve tam olarak işleyişine kasıtlı olarak zarar verme eylemlerine karşı korumaktır. Zarar verme ve bozma eylemleri, programların ve verinin bütünlüğüne zarar verecek şekilde değiştirilmesi, verinin silinmesi ve veriye erişimin engellenmesi veya virüs gibi zarar verici kodların yüklenmesi, Madde 4 uyarınca söz konusu sözleşme kapsamında suç olarak kabul edilmektedir.

Müdahale, fiile izin veren hakka sahip olmadan ve kasıtlı olarak yapılmalıdır.

d. Sistemlere Müdahale

Sistemlere müdahale bilgisayar sabotajı olarak nitelendirilmektedir. Madde 5'te yer alan hükümler bilgisayar sistemlerinin yasal kullanımının kasıtlı olarak engellenmesini suç olarak kabul etmektedir. Buna göre,

[120] İnternet ve Hukuk Platformu, a.g.e, s. 78-82.

bilgisayar sisteminin tam olarak işleyişini engelleyecek her türlü müdahale suça yönelik fiil olarak değerlendirilecektir. Ancak, söz konusu engellemenin ciddi olması gerekmektedir. Ciddiyet tanımına taraf ülkeler tarafından açıklık getirilmesi öngörülmüştür[121].

e. Cihazların Kötüye Kullanımı

Madde 6, bilgisayar sistemlerinin ve verisinin gizlilik, bütünlük ve kullanıma açıklığına karşı işlenen suçlarda bazı cihaz ve erişim verisinin kötüye kullanılmasına yönelik fiilleri içermektedir. Bu fiiller "hacker araçları" olarak bilinen erişim araçlarına sahip olmayı gerektirmektedir[122].

3.2.1.8. Bilgisayarlarla İlişkili Suçlar

Bir bilgisayar sisteminin kullanılması vasıtasıyla işlenen suçlara yönelik hükümler, 7 ile 10'uncu Maddeler arasında yer almaktadır. Birçok ülke bu maddelerde yer alan fiilleri suç olarak kabul etmektedir. Bu nedenle anılan maddelerin uygulanması esnasında devletlerin, bilgisayar sistemleri veya ağlarının yer aldığı suçlarda, yürürlükteki mevzuatlarını uygulayıp, uygulayamayacakları konusunu incelemeleri gerekmektedir. Yürürlükteki mevzuatlarda bilgisayarlarla ilişkili suçlar yer alıyor ise kanunda değişiklik yapmaya ihtiyaç duyulmayacaktır[123].

a. Bilgisayarlarla İlişkili Sahtecilik Fiilleri

Madde 7 ile amaçlanan maddi belge sahteciliği ile paralellik oluşturulması ve böylece geleneksel ceza hukukunda yer alan boşlukların doldurulmasıdır. Zira, elektronik olarak saklanan veriye yönelik sahtecilik fiilleri de geleneksel sahtecilik fiilleri ile aynı sonuçları doğurmaktadır.

Bilgisayarlarla ilişkili sahtecilik, veride yer alan bilginin gerçekliğine ve güvenilirliğine dayanan yasal işlemlerde delil teşkil eden değerin, saklanan

[121] İnternet ve Hukuk Platformu, a.g.e, s. 84-86.
[122] İnternet ve Hukuk Platformu, a.g.e, s. 86-90.
[123] İnternet ve Hukuk Platformu, a.g.e, s. 90-92.

verinin yetkisiz olarak değiştirilmesi veya oluşturulması sonucunda kaybolmasıdır. Burada korunan yasal menfaat, elektronik verinin güvenliği ve güvenilirliliğidir.

Sahtecilik farklı şekilde yorumlanabilmektedir. Yorumlardan biri belgenin yazarına göre gerçekliğine dayanmaktadır. Diğer yorumlar ise belgede yer alan ifadenin doğruluğuna dayanmaktadır. Ancak, yazara göre gerçeklik prensibi, verinin içeriğinin doğruluğu ya da gerçekliğini dikkate almamaktadır. Bu nedenle taraflar "verinin orijinal hali" ifadesi ile verinin gerçekliğini de kapsama yoluna gidebilirler.

Madde 7'de yer alan veri ifadesi, yasal etkiye sahip, özel veya kamuya ait olan belge anlamına gelmektedir. Veriye yetkisiz olarak, doğru veya doğru olmayan bir veri ilave edilmesi, sahte belgenin ortaya çıkmasına neden olacaktır. Aynı şekilde değiştirme (farklılaştırma, kısmi değişiklikler), silme (verinin çıkartılması), ve erişimin engellenmesi de ortaya sahte bir belge çıkartacaktır[124].

b. Bilgisayarlarla İlişkili Sahtekârlık Fiilleri

Teknoloji devrimi kredi kartı yolsuzluklarında belirgin bir artışa neden olmuştur. Bununla birlikte bilgisayar sistemlerinde bulunan elektronik fonlar ve mevduatlar da, sahtekârlık fiillerinin hedefi haline gelmiştir. Sahtekârlık fiili, doğru olmayan verinin sisteme ilave edilmesi yoluyla yapılan değişiklikler veya veri işlenmesine yönelik müdahaleler vasıtasıyla yapılan kanuna aykırı mal transferi şeklinde karşımıza çıkmaktadır.

Bilgisayarlarla ilişkili sahtekârlık fiilleri, bir diğer kişinin mal varlıklarında doğrudan bir zarara yol açmış ve suçu işleyen kimse kaşıdı olarak kendi veya başka bir kimse için yasadışı ekonomik fayda sağlamak amacıyla hareket etmiş ise, suç olarak kabul edilmektedir. "Mal kaybı" ifadesi geniş bir

[124] İnternet ve Hukuk Platformu, a.g.e, s. 92-94.

anlam taşımakta olup, para ile ekonomik değere sahip maddi ve manevi tüm varlıkların kaybı anlamına gelmektedir.

Suça konu olan fiil, bu eyleme izin veren bir hakka sahip olmadan, haksız gerçekleştirilmiş olmalı ve kazanılan ekonomik fayda da haksız kazanılmış olmalıdır. Ancak meşru ticari eylemler, hakka sahip olarak gerçekleştirildikleri sürece suç kapsamının dışında tutulacaklardır. Örneğin, sözleşme uyarınca bir web sitesinin kullanılmaz hale getirilmesi suç olarak kabul edilmemektedir.

Madde 8'de yer alan bir diğer önemli ifade de "kasıt"tır. Bilgisayar sisteminde ya da veride değişiklik yapan kişinin kendisinin ya da bir başkasının ekonomik fayda kazanmak niyeti ile kasıtlı olarak davranmış olması gerekmektedir. Benzeri sahtekârlık niyeti de suç kapsamı içerisinde yer almaktadır. Ancak bu ifade, piyasanın rekabetçi ortamı içerisinde bir tarafa ekonomik fayda sağlarken, bir diğerinin kaybına neden olan ancak hiçbir kasıt veya sahtekârlık niyeti taşımayan eylemleri kapsamamaktadır[125].

3.2.1.9. İçerikle İlişkili Suçlar: Çocuk Pornografisi İle İlişkili Suçlar

Madde 9 çocuk pornografisini konu almaktadır. Maddenin amacı çocukları özellikle cinsel sömürüden koruyacak önlemlerin güçlendirilmesi ve ceza hukukunun ilgili maddelerinin modernizasyonu ile çocuklara yönelik cinsel suçlarda bilgisayar sistemlerinin kullanılmasına karşı daha etkin hükümlerin oluşturulması hedeflenmektedir.

Madde 9 uyarınca çocuk pornografisine ilişkin materyallerin elektronik olarak üretimi, dağıtımı ve sahip olunması suç olarak kabul edilmektedir.

Madde 9 kapsamında suç olarak kabul edilen fiillere çeşitli ifadelerle açıklık kazandırılmıştır. Paragraf I (b)'de yer alan "teklif etme" ifadesi, çocuk pornografisinin bir bilgisayar sistemi üzerinden sunulması anlamına gelmektedir. Burada önemli olan, teklifte bulunan kişinin ilgili materyali

[125] İnternet ve Hukuk Platformu, a.g.e, s. 92-94.

sağlayabileceğidir. Örneğin, çocuk pornografisi siteleri kurarak, başka kişilerinin online kullanımına yönelik olarak çocuk pornografisinin kullanımını açık hale getirmek veya çocuk pornografisi sitelerine ulaşımı kolaylaştıracak bağlantılar oluşturmak ya da bu tip bağlantılara yer vermek Madde 9 kapsamında suç olarak nitelendirilmektedir.

Paragraf I(c)'de çocuk pornografisinin bir bilgisayar sistemi üzerinden yayınının veya dağıtımının suç olarak kabul edileceği ifade edilmektedir. Çocuk pornografisinin bir bilgisayar sistemi üzerinden bir başka kişiye gönderilmesi de çocuk pornografisi yayını olarak kabul edilecek ve suç kapsamına girecektir.

"Kendisi veya bir başkasının kullanımı için elde etmek" fiili de aktif olarak çocuk pornografisine sahip olmak anlamına gelmektedir. Bu kapsamda çocuk pornografisi indirmek suç olarak kabul edilmektedir.

Paragraf I (e) uyarınca çocuk pornografisine bir bilgisayar sisteminde veya bir disket veya CD-ROM gibi bir veri taşıyıcısında sahip olmak suçtur. Zira çocuk pornografisine sahip olmak bu tip bir talebin göstergesi olarak kabul edilmektedir. Çocuk pornografisini önlemede en etkin yol, üretimden sahip olmaya kadar zincirde yer alan her kişinin suçun bir parçası olduğu prensibinin kabul edilmesidir[126].

3.2.1.10. Telif ve İlgili Hakların İhlaline Yönelik Suçlar

Fikri mülkiyet haklarına yönelik ihlaller, özellikle internet ortamında sıklıkla görülen telif haklan ihlalleri Madde 10 kapsamında ele alınmaktadır. Internet ortamında telif hakkına sahip olan kişinin rızası dışında korunan eserlerin (edebiyat, fotoğraf, müzik, görsel-işitsel ve diğer) taklitlerinin yapılması ve dağıtımı, yetkisiz kopyalarının dijital teknolojilerin kullanımı ile çok daha hızlı ve kolay üretilebilmesi nedeniyle yaygınlaşmakta ve dağıtım alanı elektronik ağlar ile çok daha geniş tutulabilmektedir. Bu nedenle

[126] İnternet ve Hukuk Platformu, a.g.e, s. 94-100.

uluslararası işbirliği ve gerekli cezai hükümlerin varlığı bir ihtiyaç haline gelmiştir.

Madde 10, bir bilgisayar sistemi vasıtasıyla yapılan telif hakları ihlallerine yönelik olarak taraf devletlerin cezai yaptırımları içeren düzenlemeleri, taraf oldukları diğer uluslararası anlaşmalardan üstlenmiş oldukları yükümlülükler ile uyumlu olacak şekilde gerçekleştirmelerini öngörmektedir[127].

3.2.1.11. Sözleşme Kapsamında Suç Olarak Değerlendirilen Diğer Fiiller

Madde 11, sözleşmede yer alan suçlara ilaveten suça yardım, teşebbüs ve teşvik etme eylemlerinin de suç kapsamında ele alınmasını öngörmektedir. Sözleşmede suç olarak kabul edilen eylemi gerçekleştiren kişiye yardım veya teşvikte bulunan kişi de, suçun işlenmesinde sorumlu bulunmaktadır. Ancak, yardımda bulunan tarafın niyeti de önem taşımaktadır.

Örneğin internette zarar verici içerik verisi veya zararlı kod yayını hizmet sağlayıcıların yardımını gerekli kılsa da, hizmet sağlayıcının suça yönelik bir niyetinin bulunmaması, hizmet sağlayıcının sorumlu olmadığını gösterecektir[128].

3.2.1.12. Sorumluluk

Madde 12, tüzel kişilerin sorumlulukları ile ilgilidir. Kurumlar, dernekler ve benzer tüzel kişiliklerin de işlenen suçlardan sorumlu tutulabileceğine işaret eder. Suç, lider konumda olan bir gerçek kişi tarafından, tüzel kişiye fayda sağlamak amacıyla işlenmektedir.

Paragraf l'de "sorumluluk"un geçerli olacağı dört koşula yer verilmektedir: (1) sözleşmede yer alan suçlardan birinin işlenmesi; (2) suçun bir tüzel kişiye fayda sağlamak amacıyla işlenmiş olması; (3) suçun lider

[127] İnternet ve Hukuk Platformu, a.g.e, s. 100-104.
[128] İnternet ve Hukuk Platformu, a.g.e, s. 100-106.

konumda olan (üst düzey yönetici gibi) bir gerçek kişi tarafında işlenmesi; (4) lider konumdaki kişinin, temsil, karar alma ve kontrol yetkilerine dayanarak davranmış olması.

Paragraf 2'de ise sadece lider konumda olan gerçek kişi değil, bu kişinin idaresi altında çalışan diğer kişileri de kapsamaktadır. Böylelikle çalışan tarafından işlenen suçlar, lider konumdaki kişinin, çalışanların tüzel kişiye fayda sağlamak amacıyla suç işlemelerini önleyecek gerekli önlemleri alamamasından kaynaklanması nedeniyle sorumluluk kapsamında değerlendirilecektir[129].

3.2.1.13.Depolanmış Bilgisayar Verisinin Hızlandırılmış Muhafazası

Avrupa Konseyi Siber Suç Sözleşmesi'nin en önemli özelliği, uluslararası ortamda siber suçlara yönelik olarak ortak bir yaklaşım belirlemesidir. Birçok ülkede verinin muhafaza edilmesi yeni bir kavram olmakla birlikte, bilgisayarlarla ilişkili suçlara yönelik soruşturmalarda önemli rol oynamaktadır. Bu çerçevede suça yönelik fiili ve sahibini tespit etmede, ülkeler arasında ortak bir tutum oluşturulması amacıyla depolanmış verinin muhafaza edilmesi konusuna açıklık kazandırılmıştır. Madde 16 ve 17 verinin muhafazasını konu almaktadır.

Öncelikle, verinin muhafazası, hâlihazırda depolanmış olan verinin, kalitesini veya durumunu değiştirecek veya bozacak her türlü şeyden korunması anlamına gelmektedir. Verinin muhafaza edilmesi ifadesi verinin güvenli bir şekilde depolanma işleminin sürdürülmesi için kullanılmaktadır.

Veri muhafazasını gerekli kılan üç temel neden bulunmaktadır: (1) bilgisayar verilerinin kolaylıkla değiştirilebilmesi; (2) bilgisayarlarla ilişkili suçların büyük çoğunluğunun bilgisayar sistemleri vasıtasıyla yapılan iletişim yayınlarından kaynaklanması; (3) yasadışı içerik veya suça yönelik fiilin

[129] İnternet ve Hukuk Platformu, a.g.e, s. 106-108.

kanıtını taşıyan iletişimin muhafazasının, soruşturmalarda da kanıt özelliği taşıması.

Madde 16, yetkili ulusal idarelerin, yürütülen bir soruşturma veya takibat ile bağlantılı olarak belirtilen depolanmış bilgisayar verilerinin hızlandırılmış muhafazasını sağlamalarına yöneliktir. Ancak, Madde 16 verinin nasıl muhafaza edileceğine açıklık getirmeyerek, bu hususu tarafların kararına bırakmıştır.

Paragraf 2'de ilgili tarafın muhafazayı bir emir yolu ile yürürlüğe sokması halinde, muhafaza emrinin, emri alan kişinin kontrolü altında bulunan veya sahip olduğu, belirtilen depolanmış bilgisayar verisi ile ilişkili olmasının gerektiği ifade edilmektedir. Emri alan kişi, bu bilgisayar verisinin bütünlüğünü, asgari 90 gün olmak üzere gerekli olduğu sürece sağlamak ve muhafaza etmekle yükümlüdür.

Paragraf 3'te ise muhafaza etme işlemlerinin yerine getirilmesinde gizlilik prensibinin uygulanması yükümlülüğü ifade edilmiştir.

Madde 17, Madde 16 kapsamında trafik bilgilerinin muhafazasına ilişkin özel yükümlülükler getirmekte ve belirtilen iletişimin yayınında yer almış olan hizmet sağlayıcıların tanınabilmesi için trafik verisinin bir kısmının hızlandırılmış ifşasına ait gerekli hukuki altyapıyı sağlamaktadır.

Depolanmış trafik verileri, geçmiş iletişimler ile bağlantılı olarak, geçmiş iletişimlerin kaynağının veya varış noktasının tespit edilmesinde ve böylelikle suçu işlemiş olan kişilerin (çocuk pornografisi veya bilgisayar virüsleri dağıtımında bulunmuş gibi) tanımlanmasında büyük önem taşımaktadır.

İletişimin yayınlanmasında genellikle birden fazla hizmet sağlayıcı yer almaktadır. Her biri trafik bilgisinin bir kısmına sahip olabilir ve bu bilgilerin toplanması ile sonuca ulaşılabilir. Madde 17'de birden fazla hizmet sağlayıcının, iletişimin yayınında yer aldığı durumlarda, trafik verisinin

hızlandırılmış muhafazasının tüm hizmet sağlayıcılar için geçerli olacağı ifade edilmektedir. Ancak, bu işlemin nasıl yapılacağı iç hukuka bırakılmış olup yetkili idareler tercih ederler ise her hizmet sağlayıcısına muhafaza emrini ayrı ayrı da gönderebileceklerdir.

Bununla birlikte, muhafaza emrini veya benzer bir önlem emrini alan hizmet sağlayıcılarının, iletişim yayını esnasında hangi hizmet sağlayıcılarının yer aldığını tespit etmelerini sağlayacak trafik bilgisini ivedilikle yetkili idarelere veya ilgili kişiye açıklamaları gerekmektedir.

Madde 18'in birinci paragrafı, tarafların yetkili idarelerini kendi topraklarında bulunan bir kişinin belirtilen depolanmış bilgisayar verisini sağlaması veya kendi topraklarında faaliyette bulunan bir hizmet sağlayıcının abone bilgilerini yetkili idareye vermesi için gerekli olan yasal düzenlemelerde bulunmasını öngörmektedir.

Üretim emri, söz konusu yasal düzenlemelerin uygulanmasına esneklik kazandırmakta ve özellikle internet hizmet sağlayıcılarının yetkililere kontrolleri altındaki verileri gönüllü olarak sunmalarında yasal bir dayanak sağlamaktadır.

Abone bilgisi ile anlatılmak istenilen hizmet sağlayıcının idari bölümü tarafından hizmetlerine abone olan kişi ile ilgili olarak tutulan bilgidir. Soruşturmalarda abone bilgisine iki durumda ihtiyaç duyulmaktadır: (1) abonenin hangi hizmetlerin kullanıldığının tespit edilmesi (mobil bağlantı, telefon numarası gibi); (2) teknik adresin bilinmesi halinde kişinin tespit edilebilmesi için abonelik bilgilerinden yararlanılması[130].

[130] İnternet ve Hukuk Platformu, a.g.e, s. 124-131.

3.2.1.14. Depolanan Bilgisayar Verisinin Aranması ve Buna El Konulması

Madde 19, soruşturmalarda ve takibatlarda kanıtların bulunmasına yönelik arama ve el konma işlemlerine ait iç hukuk kurallarının bilgisayarlarla ilişkili suçları da kapsayacak şekilde modernizasyonunu öngörmektedir.

Paragraf I uyarınca taraflar, kanunları uygulamakla yükümlü idareleri, bir bilgisayar sisteminde veya sistemin bir parçasında veya bağımsız bir saklama aracında (CD-ROM, disket gibi) bulunan bilgisayar verisine erişimde bulunmak ve arama yapmak için yetkilendireceklerdir.

Madde 19, depolanmış veriye yöneliktir. Bu noktada, sahibi kendi bilgisayar sistemine yükleyene kadar bir internet hizmet sağlayıcısının posta kutusunda bekleyen açılmamış bir e-posta mesajının transfer edilecek veri mi yoksa depolanmış bilgisayar verisi mi olarak mı kabul edileceği sorusu ortaya çıkacaktır. Bu konuya açıklık ancak tarafların kendi kanunlarını gözden geçirerek, hangi yaklaşımın doğru olacağına karar vermeleri ile getirilebilecektir.

Paragraf 2 uyarınca soruşturmayı yürütmekte olan idare, arama veya benzer erişim işlemini, gerekli olan verinin o sistemde olduğuna inanıyor ise, başka bir bilgisayar sistemini veya sistemin bir parçasını kapsayacak şekilde genişletme yetkisine sahip olacaktır.

Paragraf 3, arama ve el koyma işlemine yönelik yetkileri, bilgisayar donanımını veya bilgisayar verisi saklama araçlarını kapsayacak şekilde genişletmektedir. Sözleşme metninde el koyma ifadesi bilgi veya verinin kayıtlı olduğu fiziksel aracı alıp uzağa götürmek veya bu veri veya bilginin bir kopyasına sahip olmak şeklinde kullanılmaktadır.

Paragraf 4 ise, arama ve el koyma işlemlerinin bilgisayar sistemi bilgisine sahip olan kişilerce yapılmasını veya bu kişilere danışılarak işlemlerin gerçekleştirilmesini öngörmektedir[131].

3.2.1.15. Bilgisayar Verisinin Gerçek Zamanlı Toplanması

Madde 20 ve 21 bir bilgisayar sistemi ile yayınlanan belirtilen iletişimle ilgili olan içerik verisine gerçek zamanlı müdahale ve trafik bilgisinin gerçek zamanlı olarak toplanması için gerekli olan yasal çerçeveyi sağlamaktadır.

Madde 20 ve 21'de kamuya ait veya özel telekomünikasyon veya bilgisayar sistemleri veya sistem kullanımı veya kamuya açık veya özel kişilerin kullanımına yönelik olarak sunulan iletişim hizmetleri arasında herhangi bir ayrıma gidilmemiştir.

Toplanacak olan veri, trafik bilgileri ve içerik verisi olarak iki başlık altında ele alınmıştır: trafik bilgisinin gerçek zamanlı toplanması ve içerik verisine müdahale[132].

3.2.1.16. Trafik Bilgisinin Gerçek Zamanlı Toplanması

Madde 20, soruşturmalar ve takibatlarda kullanılmak üzere trafik verisinin gerçek zamanlı olarak toplanması ve kaydedilmesi için gerekli düzenlemelerin yapılmasını öngörmektedir.

Söz konusu madde uyarınca, konu olan trafik verisinin ilgili tarafın toprakları içerisinde olan belirtilen iletişim ile bağlantısının bulunması gerekmektedir. İletişimin belirtilmiş olması şartı, trafik bilgisinin toplanması için büyük önem taşımaktadır.

Paragraf 2 uyarınca taraflar yetkili idarelerin trafik bilgilerini toplayacak ve kaydedecek teknik altyapıya sahip olması gerekmektedir.

---

[131] İnternet ve Hukuk Platformu, a.g.e, s. 138-148.
[132] İnternet ve Hukuk Platformu, a.g.e, s. 138-155.

Paragraf 3 ise, trafik verilerinin gerçek zamanlı toplanmasına ilişkin önlemlerin uygulanmasına yönelik bilgilerin internet hizmet sağlayıcılar tarafından gizli tutulmasını öngörmektedir[133].

3.2.1.17. İçerik Verisine Müdahale

İçerik verisinin telekomünikasyon imkânlarından yararlanarak toplanması (telefon konuşmaları gibi) uzun zamandır kullanılmaktadır. Bilgisayar iletişimi suça ilişkin kanıt toplanmasında önemli bir katkıya sahip olacaktır. Zira bilgisayar teknolojisi ile veri, metin, görsel malzeme ve ses olarak aktarılabilmektedir.

İçerik verisi, iletişimin içeriği olarak ifade edilmektedir. Madde 20'de yer alan hükümler Madde 21 için geçerli olmaktadır[134].

3.2.1.18. Sözleşme Kapsamında Yargı ile İlgili Hükümler

Madde 22, taraf ülkelerin suça yönelik fiillerin yargılanması ile ilgili yükümlülüklerini içermektedir. Paragraf l, yargı alanını belirlemekte ve taraf olan ülkenin kendi toprakları içerisinde işlenen suçlan yargılama yükümlülüğünü ifade etmektedir. Buna göre gemiler taşıdıkları bayrağın, uçaklar ise kayıtlı oldukları ülkenin toprağı olarak kabul edileceklerdir.

Paragraf 1'in d bendinde tabiiyet prensibi ele alınmıştır. Tabiiyet prensibi, vatandaşlarının, kendi ülke topraklarının dışında oldukları zamanlarda bile kendi ülkelerine ait kanunlara uymakla yükümlü tutulmaları anlamına gelmektedir. D bendi uyarınca bir vatandaşın kendi ülkesi dışında bir suça yönelik bir fiilde bulunması halinde, taraf ülke söz konusu eylem, gerçekleştirildiği ülke kanunlarına göre de suç olarak kabul ediliyor ise veya eylem herhangi bir ülkenin yargılama alanı içerisine girmiyor ise, o vatandaşı yargılamakla yükümlüdür[135].

---

[133] İnternet ve Hukuk Platformu, a.g.e, s. 155-162.
[134] İnternet ve Hukuk Platformu, a.g.e, s. 162-163.
[135] İnternet ve Hukuk Platformu, a.g.e, s. 163-167.

3.2.1.19. Avrupa Konseyi Siber Suç Sözleşmesi ve Uluslararası İşbirliği

Avrupa Konseyi Siber Suç Sözleşmesi'nin bir diğer dikkat çekici özelliği de, uluslararası işbirliğine ait genel kuralları belirlemesidir. Sözleşmede ülkelerin işbirliğini geliştirmeleri ve bilgi akışını engelleyecek uygulamalardan kaçınmaları öngörülmektedir. Söz konusu işbirliği, bilgisayar sistemleri ve veri ile ilişkili her türlü suçu kapsayacaktır. İşbirliği olabilecek en geniş şekilde sağlanmalıdır. İşbirliği hem bilgisayar sistemleri ve veri ile ilişkili suça yönelik fiillerde hem de suç hakkında elektronik formda kanıtların toplanması konularında yapılacaktır.

Suçluların iadesi, uluslararası işbirliği prensiplerine uygun olarak taraflar arasında yürürlükte olan uygulamalara göre gerçekleştirilecektir. Her iade talebinin olumlu sonuçlanacağı anlamına gelmemekle birlikte, iade seçeneğinin varlığının garanti altına alınması amacıyla, iadesi mümkün olan suçlan gelecekte yapacakları iade anlaşmalarına da dâhil etmekle yükümlü kılınmışlardır. İade anlaşmasına sahip olmayan ülkeler, bu sözleşmeyi kullanabileceklerdir[136].

3.2.1.20. Uygulamada Uluslararası Anlaşmanın Bulunmaması Halinde Karşılıklı Yardım Talepleri İle İlgili Prosedürler

Madde 27, uygulamada karşılıklı yardım antlaşmaları, kanunlar ve düzenlemelerin bulunmadığı durumlarda geçerli olacak hükümleri içermektedir.

Karşılıklı yardım taleplerini alma ve gönderme eylemlerinden sorumlu olacak merkezi idareler kurulacak, taraflar imza veya onay esnasında Genel Sekreterliğe kurulan idarelerin isim ve adreslerini bildireceklerdir.

Yapılacak talepler, yardım talep edilen ülkenin iç hukuk kuralları ile uyumlu olmalıdır. Yapılan karşılıklı yardım talepleri, taleplerin siyasi bir suç ile

[136] İnternet ve Hukuk Platformu, a.g.e, s. 167-181.

bağlantısının olması veya talepte bulunulan ülkenin güvenlik, birlik, kamu düzeni (ordre public) veya diğer hayati çıkarlarına zarar verdiği sonucuna varılır ise reddedilebilecektir. Yardım talebi, talepte bulunulan ülkenin yürüttüğü soruşturmalara zarar veriyor ise ertelenebilecektir. Gerekli değişiklikler yapılması kaydı ile yardım talebi yeniden gözden geçirilerek, yardım kısmen de olsa, sağlanabilecektir.

Yardım talebinde bulunan ülke, talebe ilişkin sonuç hakkında bilgilendirilecektir. Talebin reddi veya ertelenmesi halinde tüm nedenler ilgili tarafa sunulacaktır.

Yardım talebinin gizli tutulması istenilebilecektir. Acil durumlarda karşılıklı yardım talebi doğrudan hâkim ve davacı tarafından, diğer tarafın hakim ve davacılarına yapılabilecektir. Ancak, bundan her iki tarafın merkezi idarelerinin haberdar edilmesi gerekmektedir.

Ayrıca yardım talepleri Interpol üzerinden de yapılabilecektir. Taraflar arasında karşılıklı yardım anlaşması veya karşılıklı yardıma yönelik düzenlemeler bulunmadığı takdirde Madde 28 hükümleri uygulanacaktır.

Taraflar yardım talebine konu bilgileri gerekli ise gizli tutmak ve talebe konu bilgileri ilgili soruşturma ve takibat dışında kullanmamakla yükümlüdürler. Bilgi gönderilecek olan taraf, belirtilen koşullara uyum sağlayamayacak ise bunu karşı tarafa bildirmekle yükümlüdür[137].

3.2.1.21. Uluslararası İşbirliği Kapsamında Depolanmış Bilgisayar Verisinin Hızlandırılmış Muhafazası

Bu madde, Madde 16'da yer alan ve ulusal düzeyde uygulanması öngörülen hükümlerin uluslararası düzeyde uygulanmasına yöneliktir. Buna göre taraflar, bir diğer taraf ülkenin topraklarında depolanan verinin hızlandırılmış muhafazasını o ülkeden talep edebileceklerdir.

[137] İnternet ve Hukuk Platformu, a.g.e, s. 181-193.

Talep verinin muhafazası için gerekli olan asgari bilgiyi içermeli, muhafaza talebinde bulunan idare ve konu olan suçu tanımlamalıdır. Verilen bilgilerde muhafazanın gerekliliği ifade edilecek ve karşılıklı yardım talebinde bulunulmalıdır[138].

3.2.1.22. Uluslararası İşbirliği Kapsamında Muhafaza Edilmiş Trafik Bilgisinin Hızlandırılmış Açıklaması

Madde 30, Madde 17 hükümlerinin uluslararası düzeyde uygulanmasını konu almaktadır. Buna göre, suçun işlendiği taraf, suçu işleyeni tespit etmek ve önem taşıyan kanıtlara erişebilmek amacıyla diğer taraftan bilgisayarlar arasındaki yayına ait trafik bilgilerini muhafaza etmesini talep edebilecektir. Ancak talep, verinin muhafazası için gerekli olan asgari bilgiyi içermelidir. Yayının üçüncü bir ülkeden geldiği durumlarda, talepte bulunan taraf, üçüncü tarafa da karşılıklı yardım ve veri muhafazası talebinde bulunabilecektir.

Talepte bulunulan taraf, trafik bilgisinin açıklanmasının ülkenin birlik, güvenlik, kamu düzeni ve diğer hayati menfaatlerine zarar verdiğini düşünüyor ise, talebi reddetme hakkına sahiptir[139].

3.2.1.23. Uluslararası İşbirliği Kapsamında Depolanan Bilgisayar Verisine Erişime Yönelik Karşılıklı Yardım

Sözleşme, sözleşmeye taraf olan her ülkenin, diğer bir tarafa fayda sağlamak amacıyla, kendi topraklarında yer alan bir bilgisayar sisteminde depolanan veriyi açıklamak, erişim sağlamak ve araştırmak kabiliyetine sahip olmasını öngörmektedir. Depolanan bilgiye erişim konusunda karşılıklı yardım talebi yapıldığında, ilgili taraf talebe cevap verirken uygulamadaki antlaşmalar, düzenlemeler ve karşılıklı yardım konusunu düzenleyen iç hukuk kurallarına uygun olarak davranacaktır.

---

[138] İnternet ve Hukuk Platformu, a.g.e, s. 193-198.
[139] İnternet ve Hukuk Platformu, a.g.e, s. 198-199.

Taraflardan birinin bir başka taraf ülkede bulunan bilgisayar verisine tek taraflı olarak erişimine, karşılıklı yardım talebine gerek olmadan olanak sağlanması iki durumda mümkündür; (1) erişilen verinin kamu erişimine açık olması (2) taraflardan birinin kendi toprakları dışında bulunan bir veriye kendi toprakların bulunan bir bilgisayar sistemi vasıtasıyla erişim sağladığında veya bu bilgiyi aldığında, bu sistem ile veriyi ilgili tarafa açıklama yetkisi bulunan kişinin kanuni ve gönüllü rızası alınmış olması.

Ancak, kanunen veriyi açıklama yetkisine sahip olan kişinin kimliğine uygulamadaki kanunlar çerçevesinde açık kazandırılması gerekmektedir. Örneğin, bir kişinin e-postası hizmet sağlayıcı tarafından bir başka ülkede tutuluyor olabilir veya bir kişi veriyi kasıtlı olarak başka bir ülkede saklıyor olabilir, Madde 32 uyarınca bu kimselerin yetkililerin verilere erişim sağlamalarına izin vermeleri ya da gönüllü olarak veriyi açıklamaları gerekmektedir[140].

3.2.1.24. Uluslararası İşbirliği Kapsamında Trafik Bilgilerinin Eş Zamanlı Toplanmasına Yönelik Karşılıklı Yardım

Birçok soruşturmada, yetkililer iletişimin kaynağını bulmakta güçlük çekmektedirler. Daha önce yapılan yayınların kayıtları otomatik olarak servis sağlayıcılar tarafından silindiği için trafik bilgisi soruşturmalarda kilit bilgi olarak kabul edilmektedir. Bu nedenle, Madde 33 kapsamında trafik bilgilerine gerçek zamanlı olarak ulaşılması için, tarafların birbirleri için gerçek zamanlı trafik bilgilerini toplamaları yükümlülüğüne yer verilmiştir.

Ancak işbirliğine yönelik şartlar, uygulamadaki antlaşmalar, düzenlemeler ve ilgili kanunlar ışığında oluşturulacak ve tarafların çekincede bulunma hakları saklı kalacaktır[141].

[140] İnternet ve Hukuk Platformu, a.g.e, s. 199-201.
[141] İnternet ve Hukuk Platformu, a.g.e, s. 203-204.

3.2.1.25. Uluslararası İşbirliği Kapsamında İçerik Verisine Müdahale Hakkında Karşılıklı Yardım

Müdahaleye yönelik tecavüzlerin ve kötüye kullanma eylemlerinin oldukça yüksek bir potansiyele sahip olması nedeniyle, içerik verisine müdahalede karşılıklı yardım yükümlülüğü uygulamadaki antlaşma ve kanunlarla sınırlandırılmıştır.

İçerik verisine müdahale için işbirliği, karşılıklı yardım içerisinde yeni bir alan olduğu için, yardım yükümlülüğünün kapsamı, hâlihazırda var olan karşılıklı yardım rejimlerine ve iç hukukun ilgili hükümlerine bırakılmıştır[142].

3.2.1.26. Uluslararası İşbirliği Kapsamında 24/7 Ağı

Bilgisayar sistemlerinin kullanımı ile gerçekleştirilen suçlarla mücadelede elektronik şekildeki kanıtların toplanması büyük önem taşımaktadır. Bunun için polis teşkilatlan arasında işbirliği ve ikili yardım birimleri arasında özel kanallar oluşturulması gerekmektedir.

24/7 Ağı halen G8 ülkeleri arasında faaliyet göstermekte olan bir ağ deneyiminden yararlanılarak oluşturulmuştur. Buna göre anlaşmaya taraf olan her ülke günde 24 saat, haftada 7 gün kullanıma açık olacak bir irtibat noktasına sahip olacaktır. Böylelikle, soruşturmalarda ani yardım ihtiyacı olduğunda, bilgisayarlarla ilişkili suçlara yönelik olarak hizmet verecek etkin bir ağ kurulmuş olacaktır[143].

[142] İnternet ve Hukuk Platformu, a.g.e, s. 204-206.
[143] İnternet ve Hukuk Platformu, a.g.e, s. 204-206.

ÜÇÜNCÜ BÖLÜM

1. TÜRK CEZA KANUNUNDA BİLİŞİM SUÇU

Günümüzün bilgisayar çağı olması ve teknolojinin hızla gelişmesi karşısında dünyadaki çoğu ülke tarafından hızlı bir şekilde yayılan bilgisayarla ilgili hukuksal sorunlara önlem olması nedeniyle ülkemizde bilişim suçları ile ilgili önlemler almıştır.

1.1. 765 Sayılı (Eski) Türk Ceza Kanunu'nda Bilişim Suçları

765 sayılı Türk Ceza Kanununa 6.6.1991 günlü, 3756 sayılı Kanunla "Bilişimi Alanında Suçlar" adıyla 525/a 525/b, 525/c ve 525/d maddelerinin eklenmesiyle bilişim suçları yasal bir boyut kazanmıştır.[144]

765 Sayılı TCK'nun "On birinci Babı'n da 5 ayrı suç düzenlenmiştir. Bunlar sistemde yer alan ve sır teşkil eden bir bilgiyi hukuka aykırı olarak ele geçirip öğrenmek (525/a-1)

Başkasına zarar vermek için sistemin içeriğini kullanmak nakletmek veya çoğaltmak (525/a-2)

Başkasına zarar vermek veya kendisine veya başkasına yarar sağlamak maksadı ile sistemi veya unsurlarını tahrip etmek değiştirmek, silmek, sistemin işlenmesine engel olmak, yanlış biçimde işlemesini sağlamak (525/b/1)

Sistemi kullanarak kendisi veya başkası lehine hukuka aykırı yarar sağlamak, (bilgisayar marifetiyle dolandırıcılık) (525/b-2)

Sistemi kullanarak sahtecilik yapmak.[145]

---

[144] Ali Karagülmez, a.g.e, s. 123

[145] Türkiye Bilişim Şurası Hukuk Çalışma Grubu raporu, s. 67 www. bilişimşurası.org.tr. 28.07.2009

765 sayılı TCK'nun 525/a maddesinde verilerin ele geçirilmesi suçu düzenlenirken "bilgileri otomatik işleme tabi tutan sistem" ibaresine yer verilmiş; ancak bunun ne anlama geldiği konusunda söz konusu kanunda bir açıklama yapılmamıştır. Düzenlemeye ilişkin gerekçede "bilgileri otomatik olarak işleme tabi tutan sistem" ibaresinin yanına (bilgisayar) eklemesi yapılmış olması nedeniyle kanun koyucunun amacının "bilgisayarı" işaret etmek olduğu belirtilmiştir.[146]

1.1.1. 525a Maddesindeki Suçlar

A Bilgileri Otomatik Olarak İşleme Tabi Tutmuş Bir Sistemde Programları, Verileri Veya Diğer Herhangi Bir Unsuru Hukuka Aykırı olarak Ele Geçirmek

Suç tanımındaki kavramlara bakarsak bilişim sistemi, en basit şekliyle veri veya bilgileri alan bu verileri işleme tabi tutabilen sonuçları ya da verileri çıktı şeklinde verebilen elektronik makinelerdir.[147]

Diğer herhangi bir unsuru ibaresini, bilgisayar verileri programları ve programların işlenmesi dışında kişisel nitelik gösteren bilgiler şeklinde anlamak gerekmektedir.[148]

Ele geçirme terimi de[149] verilere ulaşmak olarak tanımlanabilir.

Suçun koruduğu Hukuki değer konusunda doktrinde tam bir birlik yoktur. Bir görüşe göre suçla konuna hukuki değer bilişim sisteminin dokunulmazlığı ile ilgilidir. Bu dokunulmazlığın sonucu olarak bu sistemin güvenliğinin sağlanması ve bilgisayar casusluğunun önlenmesi amaçlanmaktadır.

---

[146] Mustafa Ekinci ve Sinan Esen, Anlatımlı ve Gerekçeli Yeni Türk Ceza Kanununda Yer Alan Hırsızlık Yağma, Güveni Kötüye Kullanma, Dolandırıcılık, Hileli ve Taksirli İflas, Karşılıksız Yararlanma, Belgelerde Sahtecilik ve Bilişim Alalında Suçlar, Adalet Yayınevi, Ankara, 2005, s. 347.
[147] Behçet Altay, Bilgisayarlar ve Basic ile Programlama, Filiz Kitabevi, İstanbul, 1985, s. 37.
[148] Ayhan Önder, a.g.e, s. 505-506.
[149] Sulhi Dönmezer, Kişilere ve Mala Karşı Cürümler, 16. baskı, Beta Yayınevi, İstanbul, 2001, s. 620.

Bir görüşe göre de suçla korunan hukuki yarar kişisel verilerin ve özel hayatın gizliliği de dahil hukukça korunan her türlü çıkarlardır.[150]

Verilerin ele geçmesinin hukuka aykırı olması suçun oluşması için yeterlidir. 01.06.2005 tarihinde yürürlüğe giren 5237 sayılı TCK'da 765 sayılı TCK'nun 525a maddesindeki "ele geçirmek" fiili, "Bilişim Alanında Suçlar" başlıklı Onuncu bölümde yer almamıştır. Bunun yerine, hırsızlık ve dolandırıcılık suçlarının bilişim yoluyla işlenmesi suçun nitelikli hali sayılmıştır.[151]

a. Suçun Maddi Unsuru

1. Hareket

Madde de ele geçirmenin yönetim açıklanmamıştır. Suç bilişim sisteminden depolanan unsurların dolaylı olarak ele geçirilmesi şeklinde de gerçekleşebilir.[152]

525a/1 maddesinde ele geçirme esasında yetkisiz erişilen bilişim sistemindeki elektronik bilginin öğrenilmesidir.[153]

Kısaca 525a/1 maddesinde bilişim sistemine yetkili olmadığı halde hukuka aykırı olarak girme suç sayılmamıştır. Ceza olması için bilgiye ulaşması gerekir.

5237 sayılı YTCK'da ise yetkisiz olarak bir kimse bilişim sistemlerinde girerse suç sayılır.

---

[150] Berrin Bozdoğan Akbulut, Türk Ceza Hukukunda Bilişim Suçları (Yayımlanmamış Doktora Tezi) Selçuk Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı Ceza ve Ceza Usul Hukuku Bilim Dalı, Konya, 1999, s. 547

[151] Ali Karagülmez, a.g.e, s. 131.

[152] İsmail Malkoç, Mahmut Üler, Türk Ceza Kanunu Özel Hükümler-IV, Adil Yayınevi, Ankara, (tarih belirtilmemiş), s. 4753.

[153] Ali Karagülmez, a.g.e, s. 131.

2- Netice

Bilişim sisteminde yer alan bilginin ele geçirilmesi yani öğrenilmesi fiili, neticesi harekete bitişik şekli bir suçtur. Öğrenme gerçekleşince neticede gerçekleşmiş sayılır. Hareket ile netice arasında bir zaman dilimi bulunmamaktadır.[154] Ancak güvenlik duvarları olan programlara yetkisiz olarak girerse girmesi ve öğrenmesi arasında zaman dilimi farkı olacağı için bu nedenle bu suç her zaman neticesi harekete bitişik değildir.

3- Teşebbüs

525a maddesindeki suça teşebbüs konusunda 765 sayılı TCK'nun teşebbüse ilişkin genel hükümleri uygulanır. Teşebbüs için özel bir düzenleme yoktur. Teşebbüs elverişlidir.

b. Suçun Manevi Unsuru

Bu suçlar kasten işlenebilen suçlardır. Bir fayda elde etmek veya birisinin zarar görmesi gerekmez. Suç oluşur.

B- Bilgileri Otomatik Olarak İşleme Tabi Tutmuş Bir Sistemden Programları, Verileri veya Diğer Herhangi Bir Unsuru Başkasına Zarar Vermek Üzere Kullanmak, Nakletmek ve Çoğaltmak

a- Korunan Hukuki Yarar

Korunan hukuki yararlar arasında "elektronik dokunulmazlık hakkı" "Özel hayatın dokunulmazlığı" hürriyet Hakkı" "mülkiyet hakkı" da yer almaktadır.[155]

b- Suçun Maddi Unsuru

525/2a maddesinde bilişim siteminden, program veri veya diğer unsurlarını, kullanılması veya nakledilmesi veya çoğaltılması suçu söz

[154] Ali Karagülmez, a.g.e, s. 132.
[155] Berrin Akbulut, "Bilişim Suçları", SÜHFD Milenyum armağanı c.8 sayı 1-2 , 2000, s. 122.

konusudur. Seçimlik hareketlik bir suçtur, somut olayda bütün hareketler aynı anda yapılsa bile bir suç oluşur. Suçta programı kullanan nakleden ve çoğaltan kişiler farklı ise her sanık için aynı suç işlenmiş olmaktadır.[156]

c- Suçun Manevi Unsuru

Yapılan eylem sonucunda başkasının zarar görmesi gerekmektedir. Zararın maddi veya manevi olduğu konusu madde de açıklanmamıştır.[157]

525a/1. fıkrada bilgilerin gayrimeşru şekilde ele geçirilmesi, ikinci fıkrada ise, zarar vermek özel kastıyla bunarlın gayrimeşru şekilde kullanımı cezalandırılmaktadır.[158]

Suçun oluşması için zararın meydana gelmiş olup olmaması önemli değildir.

1.1.2. 525/b Maddesindeki Suçlar

A- Başkasına Zarar Vermek veya Kendisine veya Başkasına Yarar Sağlamak Maksadıyla bilgileri otomatik İşleme Tabi tutmuş bir sistemi veya verileri veya diğer herhangi bir unsuru kısmen veya tamamen tahrip etmek veya değiştirmek veya silmek veya sistemin işlemesine engel olmak veya yanlış biçimde işlemesini sağlamak

a- Korunan Hukuki Yarar

Bilişim sisteminin donanımıyla ilgili değil yalnızca verilerle ilgili fiillerin cezalandırılması nedeniyle korunan hukuki değer kişinin mal varlığıdır.[159]

Bir görüşe göre de bu suç konusuyla ilgili olarak maliklerin rızaları dışında müdahaleye uğramalarının önlenmesi amaçlanmakta ve bunların dokunulmaz olmalarının bir sonucu olarak sistemin gerekli fonksiyon

[156] Ali Karagülmez, a.g.e, 2005, s. 134.
[157] Ali Karagülmez, a.g.e, s. 135.
[158] R.Yılmaz Yazıcıoğlu, (2001), a.g.e, s. 244.
[159] Yüksel Ersoy, "Genel Hukuki Koruma Çerçevesinde Bilişim Suçları", Ankara Üniversitesi Siyasal Bilimler Dergisi, Cilt:49, Say: 3-4, 1994, s. 166-167.

görmesinin temini amaçlanmaktadır. Ve kişilerin bilişim sistemi içerisindeki unsurlar bakımından sahip olduğu mülkiyet hakkı koruma altına alınmaktadır[160].

Suçun korunan değeri sadece sistemi tahrip etme işlemesine engel olmak değil aynı zamanda fiziksel zarar verilmesi de örneğin dış donanım vasıtalarına zarar verilmesi de korunmaktadır.

b- Suçun Maddi Unsuru

Tahrip etme silme, işlemesine engel olma, değiştirme, yanlış biçimde işlemesini sağlama şeklindeki seçimlik eylemleri gerçekleştirmek suçun maddi unsurunu oluşturur.

Bu seçimlik hareketlerin hepsi aynı anda gerçekleşse bile tek suç sayılır. Her eylem ayrı ayrı değerlendirilmez. Seçimlik hareketler tamamlandıktan sonra suç tamamlanır. Sonuçta zararın meydana gelmesi aranmaz.

c- Suçun Manevi Unsuru

Suçun manevi unsuru özel manevi zararın meydana gelmesi, başkasının zarar görmesi, eylemi gerçekleştirenin de kendisine bir fayda sağlaması gerekmektedir.

525a/2 maddesi kapsamında işlenen suçta zararın meydana gelmesi suçun zararın meydana gelmesi suçun gerçekleşmesi için aranmazken 525b/1 maddesin de ise sistemin kısmen veya tamamen tahrip edilmesi değiştirilmesi, sisteme müdahale ederek işlemesine engel olma, sistemdeki verileri yok etme gibi eylemlerin sonucunda zarar meydana gelmezse suç oluşmaz.

[160] Sulhi Dönmezer, a.g.e, s. 622.

Bilgileri Otomatik İşleme Tabi Tutmuş Bir Sistemi Kullanarak Kendisine veya Başkası Lehine Hukuka Aykırı Yarar Sağlamak

Bilişim sistemlerinin kullanılarak failin kendisine hukuka aykırı yarar sağlaması ile bu suç oluşur. Fail kendisine de yarar sağlayabilir bir başkasına da yarar sağlayabilir. Burada sağlanan yarar haksız hukuka aykırı bir yarardır.

Burada sağlanan yara ekonomikte olabilir ve maddi nitelikte de olabilir.[161]

Şifreli yayınlara ve telefon frekanslarına girme suçları bu madde kapsamında değerlendirilir. Şifreli yayın televizyon programlarına şifreli aygıt ile müdahale ederek seyredilmesinin engellenmesidir.

Şifreli yayınlara yönelik başlıca üç tip ihlal görülmektedir:

1- Decoder cihazı olan kişinin şifreli yayınları izleme imkânının başka TV kullanıcılarıyla paylaşımı

2- Kişisel olarak decoder kullanım hakkı olan kişinin ticari amaçla bu yanını toplu gösterime sunması

3- Kimi yerel yönetimler ve yerel televizyonların decoder vasıtasıyla şifreli yayınları çözerek yayın alanlarına yansıtmaları.[162]

Şifreli yayınlarda şifre çözümü bilişim sistemi kullanılarak yapılmışsa bu fiil TCK'nın 525b maddesindeki bilgileri otomatik işleme tabi tutmuş bir sistemi kullanarak kendisine veya başkası lehine hukuka aykırı yarar sağlamak suçunu oluşturur. Bilişim sistemi kullanılarak çözülmüş ve sonuçta

[161] Ali Karagülmez, a.g.e, s.139.
[162] Mazlum Bozkurt, Şifreli Yayınlar ve Bilişim Sistemleri Türkiye Ortadoğu Amme İdaresi Enstitüsü Adalet Yönetimi Yüksek Lisans programı, Ankara, 2003 s. 8.

şifreli televizyon yayınının kişinin kendisi ve başkaları tarafından hukuka aykırı olarak seyredilmesi söz konusudur.[163]

Yargıtay yerleşik içtihatlarında şifreli kanal sözleşmesindeki sözleşme hükümlerine aykırı davranarak başkalarının da haksız olarak bu şifreli kanaldan yararlanmasına olanak sağlaması eylemini bilişim suçu kapsamında değerlendirmeyip taraflar arasında yapılan akide aykırılık olarak değerlendirip Fikir ve Sanat Eserleri kanununa aykırılık veya güveni kötüye kullanma suçlarına girebileceğini kabul etmiştir.

Telefon frekanslarına girme suçu bir başkasına ait telefon frekanslarına girerek kendisine hukuka aykırı yarar sağlamaktır.

Bu suçun 525b maddesi kapsamında kalıp kalmadığı tartışmalıdır. Yargıtay Ceza Genel Kurulu bir kararında bu suçu taşınabilir bir malın çalınması suçunu oluşturduğunu kabul etmiştir.

1.1.3. 525/c Maddesindeki Suçlar

Bu madde de korunan hukuki yarar sâhtekarlık suçlarıyla korunmak istenen ile aynıdır, Bilişim sisteminin kullanılarak sahtekârlık suçlarının işlenmesi yaptırım altına alınmıştır.

Hukuk Alanında Delil olarak kullanılmak maksadıyla sahte bir belgeyi oluşturmak için bilgileri otomatik olarak işleme tâbi tutmuş bir sisteme, veriliri veya diğer unsurları yerleştirmek veya var olan verileri ya da diğer unsurları tahrif etmektir.

Suçun oluşması için sahte bir belge hazırlanmasına gerek yoktur, Bilişim sistemine girerek sahte belgeyi hazırlamakla suç oluşur, illa bunun kullanılması gerekmez.

Seçimlik hareketli bir suçtur. Bilgisayar sistemini kullanarak belgeleri değiştirmek yok etmek içine yeni bilgiler yerleştirmek olmayan bir şeyi

[163] Ali Karagülmez, a.g.e, s. 141.

bilgisayar ortamında varmış gibi göstermekle bu suç tamamlanır. Hazırlanan sahte belgeleri kullanmak niteliğine göre sahte belgeyi kullanma suçu olan TCK'nın 346. maddesindeki suçu oluşturur.

Tahrif edilmiş belgeyi kullanmak da 525 C maddesindeki suçu oluşturur. Burada özel kast aranmaktadır. Bilerek hazırlanan sahte belgeyi kullanması gerekmektedir. Burada bilişim sisteminde oluşturduğu sahte belgeyi kağıda döküp kullanırsa kişi eski 765 sayılı TCK'nın 346 ve devamı maddelerindeki sahte belgeyi bilerek kullanma suçu oluşur.

Bilişim sisteminde hazırlanan belgeyi hazırlayıp kullanan kişi aynı ise 525C maddesindeki suç oluşur. Farklı kişiyse sahte belgeyi kullanan kişi hakkında TCK'nın 346. maddesindeki suç oluşur.

1.1.4. 525/d Maddesindeki Suçlar

765 sayılı TCK'nın 525d maddesinde 525a ve 525b maddelerinden mahkum olanlar hakkında feri ek ceza olarak bir kamu hizmetinden veya meslek veya sanat veya ticaretten altı aydan üç yıla kadar yasaklanma cezasının verileceği belirtilmektedir.

525d maddesindeki fer'i cezalar, 525c maddesinden mahkûm olanlar hakkında verilemeyecektir. 525a ve 525b maddelerini ele alır. Burada bir hukuki boşluk vardır. 765 sayılı TCK'nın 25. maddesine göre bir meslek ve sanatın icrasının tatili üç günden iki yıla kadar. 525d maddesinde ise bir meslek ve sanatın icrasının tatili azami üç yıla kadardır.

525d maddesi ve TCK'nın 25. maddesi azami süre bakımından çelişmektedir. 765 sayılı TCK'nın 35. maddesine göre ise meslek ve sanatın icrasının tatili mahkûm olunan hürriyeti bağlayıcı cezaya eşit süreyle verilebilecektir.[164]

[164] Ali Karagülmez, a.g.e, s. 145.

Yukarıda bahsettiğimiz suçların faili herkes olabilir. Mağdur konusuna gelince bilişim sisteminin sahibi olabileceği gibi zilyet de olabilir. Bilgisayar kullanmayı bilmeyen kişi de bu suçun mağduru olabilir. Kişinin kayıtlı bulunan kişisel verileri bilişim ortamında fail tarafından kullanılarak hukuka aykırı eylem gerçekleştirilebilir, tüzel kişilerde bu suçun mağduru olabilir. En güzel Örneği de bankalardır. Failler bankalarda mağdurların hesap bilgilerini kullanarak kendilerine haksız yarar elde edebilir. Bankamatik kartları kullanılarak yapılan hukuka aykırı eylemleri örnek olarak değerlendirirsek; Yargıtay 6. Ceza Dairesinin ölen annesinin bankamatik kartıyla SSK'ndan paranın çekilmesini hırsızlık suçu olarak değerlendirmiş. Yine Yargıtay sanığın haksız ele geçirdiği başkasına ait bankamatik kartı ile para çekmesi ve şifreyi failin bilmemesi nedeniyle eylemi sahibinin terk ve kaybettiği anahtarla kilit açmak suretiyle hırsızlık TCK'nın 493/2, 61 maddelerinin uygulanması gerektiğine karar vermiştir. Yine Yargıtay ceza Genel Kurulu sanığın haksız olarak ele geçirdiği başkasına ait kart ve şifre ile bankanın makinelerinden para çekmesi eylemini TCK'nın 525/b maddesinin ikinci fıkrasındaki bilgileri otomatik işleme tabi tutmuş bir sistemi kullanarak kendisine hukuka aykırı yarar sağlamak suçunu yani bilişim suçunu oluşturacağını oy çokluğuyla kabul etmiştir. Yargıtayın 6. Ceza dairesi bir kararında da failin bir yakınına ait işyerine girerek ona ait kredi kartını çalıp, şifresini bildiği kartla yakının rızası dışında bankamatikten para çekmesi eylemini TCK'nın 525/b maddesindeki suç saymıştır.[165] Yargıtayın 11. Ceza Dairesi sanığın hizmetli olarak çalıştığı bankanın bilgisayar sistemine girerek usulüne uygun olarak bir maaş kredi limitli hesap açması eylemini TCK'nın 525/b maddesinin birinci fıkrasında yazılı suçu oluşturacağına karar vermiştir.[166]

Görüldüğü üzere 765 sayılı TCK bilişim suçlarına sınırlı olarak yer vermiş, kanuni bir sürü boşluk olduğu için bu da günlük hayatta uygulamada bir takım sorunları beraberinde getirmiştir. 1. Haziran 2005 tarihinde 5237

[165] Ali Karagülmez, a.g.e, s. 150.
[166] Ali Karagülmez, a.g.e, s. 150.

sayılı TCK yürürlüğe girmiş ve 765 sayılı TCK'da bilişim suçları ile eleştirilen kısımları bir nebze olsun gidermeye çalışmıştır.

1.2. 5237 Sayılı TCK'da Bilişim Suçları

5237 Sayılı TCK'da bilişim suçları 243 ve devamı maddelerinde düzenlenmiştir.

1.2.1. 243. Madde Bilişim Sistemine Girme Suçu

Madde 243 (1) Bir bilişim sisteminin bütününe veya bir kısmına hukuka aykırı olarak giren ve orada kalmaya devam eden kimseye bir yıla kadar hapis veya adli para cezası verilir.

(2). Fıkra-Yukarıda ki fıkrada tanımlanan fiillerin bedeli karşılığı yararlanılabilen sistemler hakkında işlenmesi halinde, 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.[167]

Bir bilişim sisteminin bütününe ve bir kısmına hukuka aykırı, olarak girilmesi ve orada kalmaya devam edilmesi suç olarak düzenlenmiştir. 243. maddede, 765 sayılı ETCK' da yer almayan "Bilişim sistemine girme" suçu düzenlemiştir. Böylece verilerin ele geçirilmesi şartı aranmaksızın bilişim sistemine hukuka aykırı olarak girilmesi ve bu suretle bilişim sisteminin güvenliğinin ihlal edilmesi suç, haline getirilmiştir. ETCK'nun 525a/1 maddesinde "verilerin ele geçirilmesi" suçu düzenlenmiş bilişim sisteminin güvenliğinin kırılarak sisteme hukuka aykırı olarak girilmesi ve orada kalınması eylemleri ise suç olarak tanımlanmamıştı.[168]

Bu suç tipiyle Avrupa Siber Suç Sözleşmesinin "Kanunsuz Erişim" başlıklı 2. maddesindeki "Her bir taraf devlet bir bilgisayar sisteminin her

[167] Türk Ceza Kanunu, Seçkin Yayınevi, Ankara, 2005 S.137
[168] Murat Volkan Dülger, a.g.e, s..213.

hangi bir bölümüne haksız ve kasıtlı olarak erişilmesini suç kapsamına almak için gerekli kanuni düzenlemeyi yapmalı, gerekli önlemleri almalıdır." düzenlemesine paralellik sağlamaktadır.

Sözleşmede bilişim sistemine haksız erişim suç sayılmasına rağmen, 243. madde de, yalnızca haksız erişim suç sayılmamaktadır.[169] Siber Suç sözleşmesindeki gibi 5237 sayılı TCK'nın 243. maddesinde de sisteme kasıtlı olarak yetkisi olmadığı halde giren kişinin cezalandırılması gerekir. TCK'nın hem Siber suç sözleşmesine hem de karşılaştırmalı hukuka tam olarak uyum sağlanması için.

Alman Ceza Kanununda (CK) sisteme yetkisiz girme suçunu düzenleyen 202a maddesi suçun oluşması için bilişim sisteminin yetkisiz erişime karşı özel olarak korunmuş olması aranmaktadır. Japonya'da Bilgisayara yetkisiz Erişim Kanunun 3. maddesinde düzenlenen suçun oluşması için de ilk koşul olarak bilgisayara erişimin kontrol altında olması aranmaktadır. İtalya Ceza Kanununda güvenlik önlemleriyle korunan bilişim veya telematik sisteme hukuka aykırı şekilde girme veya böyle bir sistemde rıza göstermeye yetkili kişinin rızası olmaksızın kalma fiilini suç saymaktadır. İrlanda da benzeri bir düzenleme vardır.[170]

Bu suç tipine mukayeseli hukukta birçok ülke hukukunda yer veriliyor. Fransa Ceza kanunun 323-1 Alman Ceza Kanunun 202a, Danimarka Ceza Kanunun 193 ve 263, Norveç Ceza Kanunun 145/2, İtalya Ceza Kanunun 616/2, 617, 618, Hollanda Ceza Kanunun 98, 98a, 98b, 98c ve 273, Lüksemburg Ceza Kanunun 309, İrlanda Ceza Kanunun 5/1 maddelerinde yer verilmiştir.[171]

Baktığımızda TCK'nın 243. maddesinin diğer karşılaştırmalı hukukta ki benzeri düzenlemelerden farkı bilişim sistemine hukuka, aykırı yetkisiz erişimi suç saymayıp suçun oluşması için bir süre sistemde kalması gerekiyor.

---

[169] İsmail Ergün, a.g.e, s..86
[170] Şaban Cankat Taşkın, Bilişim Suçları, Beta Yayınevi, Bursa, 2008, s.20.
[171] Murat Volkan Dülger, a.g.e, s.213

a. Suçla Korunan Hukuki Değer

Korunan hukuki değer bilişim sisteminin güvenliğinin sağlanmasıdır. Bunun yanında bilişim sisteminin kullanıcısı ve bu sistemden, yararlanan kişilerin farklı türden kişisel yararları da korunmaktadır.

Hukuka aykırı olarak bilişim sistemlerine girme ve sistemde kalma suçunda korunan hukuksal değer, özel hayatın gizliliği ve sırrın masumiyeti olarak belirtilebilir. Bir bilişim sistemine hukuka aykırı bir şekilde girilmesi ve orada kalmaya devam edilmesi bir kişinin veya bir kuruluşun çıkarlarına menfaatlerine zarar vermekte bu da o kişi veya kurumun verilerinin gizliliği özel hayatın dokunulmazlığı gibi hukuksal değerlerini ihlal edebilmektedir. Tüm bunlarda o sitemin güvenliğini etkilemektedir.[172]

Bir görüşe göre ise TCK'nın korunan hukuki yararı mal varlığının korunması olduğunu savunur.[173]

b. Suçun Maddi Unsuru

Suçun maddi unsurunu bilişim sistemi oluşturmaktadır.

Suçun işlenmesinde başvurulan hareketler, hareketlerin sonucunda ortaya çıkan sonuç ve bunlar arasındaki nedensellik bağıdır.[174] Bilişim sistemine hukuka, aykırı olarak girilmesi ve orada kalmaya devam edilmesi bu suçu oluşturmaya yetmektedir.[175] Bir görüşe göre TCK 243 maddedeki suçun maddi unsurunun hareket bölümünü hangi yolla olursa olsun bilişim sistemine girilmesi ya da sistemde kalmaya devam edilmesi hareketlerinin oluşturduğunu savunmaktadır. Bu eylemlerden herhangi birinin gerçekleşmesi ile suç meydana gelecek ve fail cezalandırılacaktır. O halde

---

[172] Murat Volkan Dülger, a.g.e,s.214
[173] Muammer Ketizmen, Türk Ceza Hukukunda Bilişim Suçları, Adalet Yayınevi. 1. Baskı, Ankara, 2008, s.99
[174] Doğan Soyaslan, Ceza Hukuku Genel Hükümler Güncelleştirilmiş 3. Baskı ,Yetkin Yayınevi, Ankara, 2005, s.200.
[175] Ali İhsan Erdağ, "Yeni Türk Ceza Kanununda Bilişim Suçları",www.adalet.gov.tr. 14.08.2009

bu suç seçimlik hareketli bir suçtur.[176] Bu suçun maddi unsuru hukuka aykırı olarak bilişim sistemine girip ve bir süre orada kalmak olduğundan dolayı TBMM Genel Kurulundaki metinde madde gerekçesinde de girme veya orada kalmaya devam etme fiillerinin bu suçun seçimlik hareketli bir suç olacağı ifade edilmiştir. Ancak burada sadece bilişim sistemine girilmesi yeterli olmayıp aynı zamanda bir müddet sistemde kalmayla suç oluştuğundan dolayı bağlı hareketli bir suçtur. Çünkü iki eyleminde beraber aynı anda gerçekleşmesiyle suç oluşmaktadır.

Suçun oluşumu için sistemin tamamına girilmesi gerekmemekte bir kısmına girilmesiyle de suç oluşur.

Bilişim sistemine girmek eyleminden bilişim sisteminin oluşturduğu elektronik ortama girilmesidir. Girmek eylemi ağ üzerinden veya fiziki olarak doğrudan da olabilir.

Ana sisteme bağlı olan o doğrultuda işlem yapabilen depolama aygıtı, CD veya DVD okuyucu aletleri veya ATM makineleri gibi donanım parçalarının girilmesi suretiyle de işlenebilir.[177]

Failin bilişim sistemine girmesi ve orada bir süre kalması sitemdeki gizli verilerin öğrenilmesi açısından tehlike oluşturmaktadır. Bu nedenle tehlike suçudur. Kanun koyucu burada verilerin öğrenilmesini, sisteme zarar verilmesini suçun oluşması açısından aramamıştır. Gizli verilerin öğrenilmesi ihtimali bile suç sayılmıştır.

Fail suç kastı olmadan bir bilişim sistemine girmiş olabilir. Ancak hata sonucu girdiği bilişim sisteminden çıkmayıp kalmaya devam etmesi halinde suçun oluştuğu kabul edilmelidir.[178]

---

[176] Murat Volkan Dülger, a.g.e, s..217
[177] Levent Kurt, a.g.e, s.156
[178] Mustafa Ekinci, Sinan Esen, a.g.e, s.353.

Bu suçun oluşmasında yetkisiz olarak sisteme girilmesinin yanında bir müddet sistemde kalınması arandığından mütemadi (Kesintisiz) bir suçtur. Süre şartı, tamlanmışsa suç oluşur.

c. Suçun Manevi Unsuru

Bu suçun oluşması için genel kast yeterlidir.

Failin hukuka aykırı olarak bilerek veya bilmeyerek rastlantı sonucu girdiği bilişim sisteminde durumun farkına vardıktan sonra bilerek ve isteyerek kalması ile suç oluşacaktır. Kanunla ya da ilgilinin rızasıyla izin verilen sürecin dışında sistemde kalmaya devam etmesi de suçu oluşturacaktır.[179]

Bu suç kasten işlenebilir. Taksirle işlenmesi mümkün değildir. Ancak yasa koyucu tarafından 243. maddenin 3. fıkrasında taksirle bilişim sistemindeki verilerin ortadan kaldırılmasını yaptırıma bağlanmıştır.

d. Suçun Faili

Suçun faili herkes olabilir. Madde metninde kimse dediği için suçun faili hukuka aykırı olarak bilişim sistemine giren ve orada kalmaya devam eden herhangi bir kimse olabilir.

Failin sıfat ve görevinin suçun nitelenmesi açısından bir önemi bulunmamaktadır.[180] Tüzel kişilerin fiil ehliyeti olmadığı için kusur ehliyeti de yoktur. Tüzel kişilerin cezai sorumluluğu yoktur. Suç tüzel kişi yararına bir gerçek kişi tarafından işlemişse tüzel kişi hakkında YTCK'nın 246 maddesi uyarınca tüzel kişilere özgü güvenlik tedbiri uygulanır, TCK'nın 60. maddesindeki tedbirler.

---

[179] Necati Meran, Yeni Türk Ceza Kanunun da Sahtecilik Malvarlığı Bilişim Suçları ile Ekonomi ve Ticaret Alanında Suçlar 2. Baskı,Seçkin Yayınevi, Ankara, 2008, s.567
[180] Necati Meran, a.g.e, s.563

e. Suçun Mağduru

Herkes suçun mağduru olabilir, gerçek veya tüzel kişiler olabilir. Bilişim sistemine hukuka aykırı olarak girilmesi ve orada kalınmasından dolayı zarara uğrayan kişi suçun mağdurudur.

f. Suçun Özel Görünüş Şekilleri

1. Teşebbüs

Bu suça teşebbüs mümkündür. Fail icrai hareketlere başlamış sisteme hukuka aykırı olarak girmiş ve sistemde bir süre kalamadan herhangi bir sebeple failin kendi isteği dışında eylemi tamamlayamaması durumunda suç teşebbüs aşamasında kalır. Failin cezası belirlenirken TCK'nın 35. maddesindeki teşebbüs hükümleri de somut olaya göre değerlendirilecektir.

Eğer fail kendi isteği ile icrai hareketleri tamamlayamamışsa faile TCK' nın 36. maddesi göz önünde bulundurularak ceza verilmez.

2. İştirak

Bu suçta iştirak açısında bir özellik yoktur. Suça iştirakin her hali mümkündür.[181] İştirak uygulanırken YTCK'nın genel hükümlerindeki 37,38,39, ve 40. maddeleri göz önünde bulundurulacaktır.

3. İçtima

Bu suçla ilgili özel bir içtima kuralı yoktur.

Bu suçun kısa aralıklarla aynı suç işleme kastıyla işlenmesi halinde zincirleme suç olur. TCK'nın 43. maddesi de ceza verilirken göz önünde bulundurulur, Suçu değişik zamanlarda bir kişiye karşı birden fazla işlemesi halinde zincirleme suça ilişkin YTCK'nın 43/1 maddesi uyarınca tek cezaya hükmedilir. Somut olayım durumuna göre bu ceza dörtte birinden dörtte

[181] Ali Parlar- Muzaffer Hatipoğlu, Türk Ceza Kanunu Yorumu 2. baskı cilt4, Seçkin Yayınevi, Ankara, 2008, s.3471

üçüne kadar arttırılır aynı suçun birden fazla kişiye karşı değişik zamanlarda işlenmesi durumunda zincirleme suç hükümlerinin uygulaması olanağı yoktur. Tek eylemle birden fazla kişiye karşı suçun işlenmesi olanaklı ise TCK'nın 43/2 maddesi delaletiyle TCK'nın 43/1 maddesindeki zincirleme suç hükümleri uygulanır.

Failin elde etmek istediği amaca yönelik eylemlerini gerçekleştirebilmesi için öncelikle hukuka aykırı, olarak bilişim sistemine girmesinin zorunlu olduğu durumlar da bu suç geçit suçu özelliği taşıdığından örneğin "sistemi engelleme, bozma verileri yok etme veya değiştirme suçu (244 md), banka veya kredi kartlarının kötüye kullanılması (245 md) veya bilişim sistemi aracılığıyla hırsızlık (142 md), dolandırıcılık (158. md) suçlarının fail tarafından öncelikle bir bilişim sistemine hukuka aykırı olarak gerçekleştirilmesi durumunda faile yalnızca gerçekleştirdiği ikinci eylemin cezası verilir. Ancak bu suçların bir bilişim sistemine hukuka uygun şekilde girildikten sonra gerçekleştirilmesi söz konusu ise bu durumda gerçek içtima kuralları, uyarınca fail her iki suçtan dolayı cezalandırılacaktır.[182]

TCK 243/1 ile getirilen hukuka aykırı olarak bilişim sistemine girme ve sistemden çıkmama eyleminin TCK 136 da ki kişisel verilerin hukuka aykırı olarak ele geçirilmesi suçu ile birlikte değerlendirilmesi gerekmektedir. TCK'nın 243/1'deki sisteme hukuka aykırı olarak girme fiili gerçekleşmeden TCK 136'da ki hukuka aykırı olarak verileri ele geçirme suçu oluşmayacaktır. TCK'nın 243'teki suçun oluşması için TCK'nın 136 maddesindeki suçtan geçmek gerekmektedir. Fail yalnızca TCK'nın 44. maddesi gereğince cezası daha ağır olan TCK 136'dan cezalandırılacaktır.

g. Suça Etki Eden Haller

1- Cezayı hafifletici neden

243. maddenin 2. fıkrasında bu suç açısından hafifletici bir neden öngörülmüştür. Buna göre, 1. fıkrada tanımlanan hukuka aykırı olarak bilişim

[182] Ali Parlar- Muzaffer Hatipoğlu, a.g.e, s.3471

sistemine girme ve orada kalmaya devam etme eylemlerinin “bedeli karşılığı yararlanılabilen sistemler hakkında işlenmesi halinde verilecek ceza yarı oranında indirilecektir.

Bedeli karşılığı yararlanılabilen sistemler kavramının tanımı madde gerekçesinde belirtilmemiştir.

Doktrindeki bir görüşe göre internet üzerinden hizmet veren web siteleri internet cafe gibi yerlerde ücret karşılığı bilişim sisteminin kiralanması bir kuruluş tarafından belli bir sistemin bedel karşılığı sunulması ve belli bir zaman ya da dönem sınırlamasıyla internet bağlantı servisinin sağlanmasıdır.[183]

Bu suçu TCK’nın 163. maddesindeki otomatlardan karşılıksız yaralanma suçu ile karıştırmamak gerekir. Otomatlar aracılığı ile sunulan bedeli ödediği taktir de yararlanılabilen hizmetten ödeme yapmadan yararlanma fiili TCK’nın 163. maddesindeki suça girer.

2- Cezayı Ağırlaştırıcı Nedenler

243. maddesi 3. fıkrasında bu suçun neticesi sebebiyle ağırlaşmış hali düzenlenmiştir. Birinci fıkrada tanımlanan suçun işlenmesi nedeniyle sistemin içerdiği bilgilerin yok olması veya değişmesi halinde fail suçun temel şekline 243/1 maddesine nazaran daha ağır ceza (altı aydan iki yıla kadar hapis) ile cezalandırılacaktır.[184] 243/3. fıkrasının uygulanabilmesi için sistemdeki verilerin yok olması veya verinin değişmesi gerekmektedir. Bunlardan birinin gerçekleşmesi halinde ağırlaştırıcı neden uygulanır.243/3 fıkradaki suçun oluşmasında ayrıca failin verileri yok etmek veya değiştirmek kastıyla hareket etmemiş olması gerekmektedir.[185]

[183] Murat Volkan Dülger, a.g.e, s.226, 227
[184] Ali Parlar- Muzaffer Hatipoğlu, a.g.e, s.3472
[185] Ali Karagülmez, a.g.e, s.174

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

1- Kovuşturma

Maddede belirtilen suçların kavuşturulması resen yapılır,

2- Görevli Mahkeme

5235 sayılı kanunun 10. maddesi uyarınca maddede tanımlanan suçlar dolayısıyla açılan davlara bakma görevi Sulh Ceza Mahkemesine aittir.

3- Suçun Yaptırımı

Maddenin 1. fıkrasındaki suçun yaptırımı bir aydan (TCK 49/1.md) bir yıla kadar hapis veya adli para cezasıdır. İkinci fıkra uyarınca bu fiilin bedeli karşılığı yararlanılabilen sistemler hakkında işlenmesi durumunda verilecek ceza yarı oranına kadar indirilecektir. Üçüncü fıkrada tanımlanan suçun neticesi sebebiyle ağırlamış halinde ise faile altı aydan iki yıla kadar hapis cezasına hükmolunacaktır. Bu suçların işlenmesinden tüzel kişilerin hukuka aykırı yarar sağlanması halinde bunlara YTCK'nın 60. maddesinde öngörülen güvenlik tedbirleri uygulanır. (TCK'nın 246m)

4- Dava Zaman Aşımı

Dava zaman aşım TCK'nın 66. maddesi uyarınca sekiz yıldır.

1.2.2. Sistemi Engelleme, Bozma Verileri Yok Etme Veya Değiştirme

Madde.244(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 fiille bir banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşun 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 halinde iki yıldan altı aya kadar hapis ve beşbin güne kadar adli para cezasına hükmolunur.

244. maddenin 1. ve 2. fıkraları 765 sayılı ETCK'nın 525/b-1 fıkrasının; 244/4 fıkra hükmü ise 765 sayılı TCK'nın 525/b-2 fıkrasının kısmen farklılaştırılarak karşılığı olarak düzenlenmiştir.

Bu suç tipiyle Avrupa Siber Suç Sözleşmesinin 4. maddesinde öngörülen "verilere müdahale" ve 5. maddesinde öngörülen "sistemlere müdahale" düzenlemelerine paralellik sağlanmaya çalışılmıştır.[186]

Maddenin gerekçesinde de anlaşıldığı üzere sistemlere zarar verme suç haline getirilmiştir.

Karşılaştırmalı hukukta bilişim sistemlerinde yer alan verilerin ya da programların kısmen veya tamamen tahrip edilmesi değiştirilmesi işlevlerinin üzerinde oynanması olağan işleyişinin engellenmesi erişimin kısıtlanması gibi eylemler genel olarak bilişim sistemlerine karşı mala zarar verme suçları olarak düzenlenmiştir.[187]

Fransa CK. M323-2, Alman CK. M. M.303, Avusturya CK' m.126/a1, Finlandiya CK.35. kısım m.1/2, Avustralya CK. M.76C, Danimarka

[186] R. Yılmaz Yazıcıoğlu, "Bilişim Suçları konusunda 2001 Türk Ceza Kanunu Tasarısının Değerlendirilmesi" Hukuk ve Adalet: Eleştirel Hukuk Dergisi, Y:1, S.1 Ocak-Mart 2004, İstanbul, s.179

[187] R. Yılmaz Yazıcıoğlu, (2001) a.g.e, s.468.

CK.m.279a, Norveç CK m.151b, İrlanda, Criminal Damage Act'te m.2/1 ve 2/a verilebilir.[188]

765 sayılı TCK 525/b. 1'de yer alan tahrip eden ifadesi yeni düzenlemede yer almamaktadır. Düzenlemenin 765 Sayılı TCK' dan farkı sistemin donanım öğesine zarar verilmesinin cezalandırılmamasıdır. Mala zarar verme suçu kapsamında değerlendirilir. Bilgisayarın donanım bölümüne zarar verilmesi TCK 244/1 kapsamında değerlendirilmeyecektir.

a. Suçla Korunan Hukuki Değer

244. maddenin 1. ve 2. fıkralarında tanımlanan bilişim sisteminin işleyişinin engellemesi bozulması verilerin yok edilmesi veya değiştirilmesi suçlarıyla korunmak istenilen hukuksal yarar, karma bir nitelik taşımaktadır.[189]

244. maddenin 1. fıkrasına paralel bir düzenleme olan Avrupa Siber suç sözleşmesinin "sistem Engellemeleri." Başlıklı 5. maddesinin dayanak raporuna göre bu suçlar korunan hukuksal yarar, bilgisayar verilerine veya programlarına zarar verilmesini, veri ve programların bozulmasını zarar görmesini engellemektir. Aynı sözleşmenin YTCK'nın 244/2. fıkrasının karşılığı olan "veriye müdahale" başlıklı 4. maddesinin dayanak raporuna göre bu suçla korunan hukuksal yarar ise temel olarak bilgisayar sabotajıyla ilgilidir ve bilişim sistemlerinin sağlıklı şekilde kullanımını sağlamak ve buna yönelecek haksız davranışlara engel olmaktır.[190]

1 numaralı fıkrada, bilişim sistemi sahibinin mülkiyet hakkı, zilyedinin ise; bilişim sisteminin dokunulmazlığı iletişim kurma, teknolojik gelişim özgürlüğü de korunmaktadır. (2). Numaralı fıkrada ise bazen mülkiyet hakkı

[188] Olgun Değirmenci, a.g.e, s.129-130.
[189] Murat Volkan Dülger, a.g.e, s.231.
[190] Ali Parlar- Muzaffer Hatipoğlu, a.g.e, s.3475

bazen de verilerin içeriğine göre fikri mülkiyet hakkı özel hayatın gizliliği ticari sırlar da korunmaktadır.[191]

244. maddenin 4. fıkrasında ise korunmak istenen hukuksal karar suçun işleniş biçimine göre zilyetlik üçüncü kişilerin iyi niyetleri ve maddi ya da manevi mülkiyeti haklarıdır.

b. Suçun Konusu

İşleyişi engellenen veya bozulan bilişim sistemi veya bilişim sisteminde bulunmasına karşılık bozulan yok edilen değiştirilen veya erişilmez kılınan ya da sisteme yerleştirilen başka bir yere gönderilen veriler suçun konusunu oluşturur.[192]

Maddenin düzenlenme amacı bilişim sisteminin işleyişinde ve verilerde meydana gelecek zarardır. Donanıma verilecek zararlar için YTCK'nın 151. maddesindeki mala zarar verme suçu oluşur.

c. Suçun Maddi Unsuru

Bilişim sisteminde sistemin engellenilmesi işleyişinin bozulması, verilerin yok edilmesi, verilerin değişilmesi ve erişilmez kılınması gibi eylemler suçun maddi unsurlarıdır. Bunlara ayrıntılı bakarsak;

1- Sistemin İşleyişini Engelleme:

Sistemin düzgün işlemesinden dolayı elde edilecek yararın engellenmesi veya sistemin olağan işlevini yerine getiremeyecek hale getirilmesidir.[193]

Sistemin işlemesinin engellenmesi sisteme her türlü müdahale şeklinde olabilir. Sistemin elektriğinin kesilmesi sistemleri birbirine bağlayan kabloların çıkarılması, bilişim donanımına it bir unsurun çıkarılması bilişim

[191] Levent Kurt, a.g.e, s:162.
[192] Necati Meran, a.g.e, s.571.
[193] Ümit Kardaş, "Bilişim Dünyası ve Hukuk", Karizma Dergisi Sayı:13, 01.03.2003 s.16

sisteminin genel olarak işleyişine ilişkin Somut unsurlarına yönelik eylemlerle gerçekleştirilebileceği gibi, zararlı virüsler başlatılarak sistemin yavaşlatılması ya da elektronik posta bombardımanı veya mantık bombası gibi yazılımlar yoluyla sistemin komutları algılamaz hale getirilmesi gibi soyut unsurlarına yönelik çok değişik işlenme şekilleriyle gerçekleştirilebilir.[194]

Engellemenin suçun oluşması bakımından geçici ya da sürekli olmasının bir önemi yoktur.

2- Bilişim sisteminin işleyişini bozmak.

Bozmak ifadesiyle bilişim sisteminin kendisinden beklenen işi yapamayacak duruma getirilmesi, bilişim sisteminin düzenin karıştırılması, bilişim sistemine zarar verilmesi kastedilmektedir.[195] Eylem sıradan verilere değil de örneğin işletim yazılımındaki sistem dosyalarının silinmesi biçimindeki sistemin işleyişini sağlayan dosyalara yönelik ise bu durumda 244. maddenin 2. fıkrasının değil 1. fıkrasının uygulanması gerekir.[196]

3- Sistemdeki verileri bozmak

Veriler üzerinde gerçekleştirilebilecek bir icra hareketidir. Bu icra hareketi ile verilerin bilinemeyecek hale gelmesi, bellek üzerinde bulunduğu noktaya ulaşılmasını sağlayan bağların koparılması ve ulaşımın engellenmesi kastedilmektedir.[197]

4- Verileri Değiştirmek

Bu eylem ve sistemdeki verilerin değiştirilerek yerine başka yeni görünüm kazanmış verinin konulmasıdır.

Değiştirilmenin kısmen veya tamamen olması suçun oluşumunu etkilemez.

---

[194] Murat Volkan Dülger, a.g.e, s.164.
[195] Murat Volkan Dülger, a.g.e, s.235
[196] Ali Parlar- Muzaffer Hatipoğlu, a.g.e, s.3477.
[197] İsmail Ergün, a.g.e, s.95

Fail verileri menfaat temin etmek için değiştirmiş ve kendisinin ya da başkasının yararına bir menfaat sağlamış ise eylem başka bir suçu oluşturmuyorsa, faile TCK' nun 244/4 maddesince ceza verilir.[198]

5- Sistemdeki Verileri Erişilmez Kılma

Maddi anlamda yok etmemekle birlikte verilere ulaşılması için gereken işlem bağının ortadan kaldırılmasıdır.

Verilerin erişilmez olmasından kasıt edilen verileri kullanan ya da bu verilerle malik olan kişinin dilediği zaman verilere ulaşmasının engellenmesidir. Burada önemli olan verilerin mutlaka malikine ait olması değil, verilere ulaşabilmenin engellemiş olmasıdır.[199]

6- Bilişim sistemine veri yerleştirilmesi.

Sistemi kullanmakla yetkili olan kimsenin izni alınmaksızın dışarıdan birinin sisteme girerek veri yerleştirmesidir. Bu İşlem kaydetme, ekleme veya yükleme şeklinde gerçekleştirilebilir.[200]

Veri yüklenen sisteme fail hukuka uygun olarak girmiş olsa dahi veri yerleştirme suçu gerçekleştirmiş olabilir. Örneğin bedeli ödenerek bir sisteme giren failin eğer o sisteme veri yerleştirme yetkisi yoksa suç gerçekleşmiş sayılacak ve fail cezalandırılacaktır.[201]

Burada failin veri yerleştirirken sisteme zarar verme kastı bulunmamakla hiçbir zarar oluşmazsa bile sadece sisteme girip verilerin değiştirilmesi bile başlı başına bir suçtur.

7- Bir sistemde var olan verilerin başka bir yere gönderilmesi.

---

[198] Ali Parlar- Muzaffer Hatipoğlu, a.g.e, s.3476
[199] Murat Volkan Dülger, a.g.e, s.169
[200] Şaban Cankat Taşkın, a.g.e, s.48
[201] Murat Volkan Dülger, a.g.e, S.237

8- Verilerin transferi, başka yere aktarılması, kaydedilmesi ya da kopyalanması anlamına gelmektedir. Verilerin gönderilmesi eylemi veri ileti ağları üzerinde Örneğin internette veya bilgisayara bağlanan veri taşıma aracı üzerine kaydedilerek gerçekleştirilebilir.[202]

d. Manevi Unsur

244/1. ve 2. fıkralardaki suçların manevi unsuru bakımından genel suç işleme kastı yeterlidir. 244/4. fıkradaki suç bakımından kişinin kendisine veya başkasına haksız bir çıkar sağlaması arandığından failde özel kast aranmaktadır.

TCK'nın 244/1 ve 2. fıkralarındaki suçun taksirle işlenmesi mümkün değildir.

e. Suçun Faili

Suçun faili herkes olabilir.

f. Suçun Mağduru

Mağdur bilişim sisteminin maliki zilyedi, bilişim sistemi üzerinde tasarruf yetkisi olan kişi olabilir.

g. Suçun Özel Görünüş Biçimleri

1- Teşebbüs

Maddede tanımlanan suçlara teşebbüs mümkündür.

Seçimlik hareketli bir suç olduğundan dolayı maddede tanımlanan eylemlerden birini failin tamamlaması ve zararın oluşması ile suç tamamlanır. Eğer fail elinde olmayan nedenlerle icrai hareketi tamamlayamıyorsa TCK' nun 35/1 maddesi uyarınca teşebbüsten dolayı sorumlu tutulur.

[202] Ali Parlar- Muzaffer Hatipoğlu, a.g.e, s.3478

2- İştirak

Bu suçlar iştirak açısından bir özellik göstermez. Bu suçlara somut olaya göre YTCK'nın 37, 38, 39 ve 40. maddeleri uygulanabilecektir.

3- İçtima

Bilişim sisteminin işleyişinin engellenmesi, bozulması, verilerin yok edilmesi veya değiştirilmesi suçu zincirleme suç şeklinde işlenebilecektir. Failin bir kişiye karşı aynı suçu birden fazla işlemesi durumunda YTCK'nın 43/1 maddesince ceza verilir. Failin her eyleminden ayrı ayrı değil bir ceza verilir ancak cezanın oranı arttırılır.

TCK'nın 243 maddesinde ki suç 244. maddesindeki suç için geçit suç özelliği taşıdığından (243. maddedeki hukuka aykırı olarak bilişim sistemine girme ve sistemde kalma suçu) faile sadece 244. maddedeki öngörülen ceza verilir.

Maddenin 4. fıkrasında tanımlanan suçtan (haksız çıkar sağlamanın başka bir suç oluşturmaması halinde) dolayı failin cezalandırılabilmesi için eylemin başka bir suçu oluşturmaması gerektiğinde, bu suçla benzer hukuksal değeri koruyan suç tipleri arasında bileşik suç (42.md) veya fikri içtima (44. md) durumları söz konusu olamaz.[203]

h. Suça Etki Eden Nedenler

244. maddenin 3. fıkrasında birinci ve ikinci fıkradaki suçların ağırlaştırıcı nedeni düzenlenmiştir. Bu fiillerin bir banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinde işlenmesi halinde faile verilecek ceza yarı oranında arttırılacaktır.

[203] Ali Parlar- Muzaffer Hatipoğlu, a.g.e, s.3480.

ı. Hukuka Aykırılık Unsuru

Bilişim sisteminin ve üzerinde bulunan verilerin maliki ya da ilgisinin hukuken geçerli bir rızasının bulunmaması gerekir. Hukuka uygun bir rızası olursa suç oluşmaz. Bilişim sistemine "fiilin hukuka aykırı olduğunu" bilerek girmek gerekmektedir.

i. Kovuşturma Görevli Mahkeme Suçun Yaptırımı Ve Dava Zamanaşımı

1- Kovuşturma

Bu suçların soruşturma ve kovuşturması resen, yapılır.

2- Görevli Mahkeme

5235 sayılı Kanunun 11. maddesi uyarınca bu suçlar dolayısıyla açılan davalara bakma görevi asliye ceza mahkemesine aittir.

3- Suçun Yaptırımı

1. Fıkrada bir yıldan 5 yıla kadar 2. fıkrada ise altı aydan üç yıla kadar hapis cezasıdır. 3. fıkradaki ağırlatıcı nedenin varlığı halinde bu cezalar yarı oranında arttırılır. Maddenin 4. fıkrasındaki suçun yaptırımı ise iki yıldan altı aya kadar hapis ve beş bin güne kadar adli para cezasıdır.

4- Dava Zamanaşımı

Maddenin 1. ve 2. fıkralarına uyan dava zamanaşımı süresi 66/1-e bendine göre sekiz yıldır, Birinci fıkradaki suçun üçüncü fıkradaki nitelikli halle birlikte uygulanması halle birlikte uygulanması halinde ve 4. fıkranın uygulandığı durumlarda bu süre 66/1-d bendi uyarınca on beş yıldır.

**** Bilişim Sistemi Aracılığıyla Hukuka Aykırı Yarar Sağlama Suçu,**

244. maddenin 4. fıkrası maddenin 1. ve 2. fıkralarına göndermede bulunmaktadır. Bu fıkraya göre cezaya hükmedilebilmesi için fiilin daha ağır cezayı gerektiren bir suç, oluşturmaması gerekir.

Fiilin dolandırıcılık, hırsızlık, güveni kötüye kullanma veya zimmet suçunu oluşturması halinde bu fıkra hükmüne istinaden cezaya hükmedilmeyecektir.[204]

Bu suç tipi 765 sayılı TCK'nın 525/b.2' deki suç tipinin karşılığıdır. Yeni düzenlemenin eski düzenlemeden temel farkı, yeni düzenlemede suçu oluşturan fiillerin açıkça gösterilmesi ve suçun sınırlarının iyi çizilmesidir.[205]

Yargıtay TEDAŞ da görevli olan Sanığın; kendisine ve 30 kişiye ait elektrik faturalarıyla ilgili bilgisayardaki kayıtları silmek veya ödemediği halde ödendi şeklinde değiştirmek suretiyle gerçekleşen eylemin fatura borcunu sildiği her kişi için ayrı ayrı TCK'nın 525/b-2, 80. maddeleri uyarınca cezalandırılması gerektiğine karar vermiştir.[206]

Avrupa Siber Suç Sözleşmesinde de bu madde yer almaktadır. Buna göre bilgisayarlarla ilgili sahtecilik fiilleri bir diğer kişinin malvarlığından doğrudan bir zarara yol açmış ve suçu işleyen kimse kasıtlı olarak kendisi veya bir başkası için yasadışı ekonomik yarar sağlamak amacıyla hareket etmişse suç oluşacaktır. Mal kaybı ifadesini geniş yorumlayarak para veya ekonomik değere sahip maddi ve manevi tüm varlıkları bu kapsamda değerlendirmek gerekecektir.[207]

Suçun korunan hukuksal değeri dolandırıcılık, hırsızlık, güveni kötüye kullanma veya zimmet suçlarının koruduğu hukuki yararlar, bu suçun da koruduğu hukuku yarardır.[208]

---

[204] Zekeriya Yılmaz, 2004 Notlu Gerekçeli Genel Açıklamalı Yeni Türk Ceza Kanunu, Seçkin Yayıncılık, Ankara, 2004,s.294
[205] Murat Volkan Dülger, a.g.e, s.243
[206] İsmail Ergün, a.g.e, s.99
[207] Aslı Deniz Helvacıoğlu, a.g.e, s.286-287.
[208] Levent Kurt, a.g.e, s.163

Bu suçun faili herkes olabilir ancak tüzel kişiler bu suçun faili olamaz. Suçun konusu failin sağladığı hukuka aykırı yarardır. Bu yarar manevi yararda olabilir illa bir mali kazanç elde etmesi gerekmiyor. Bu suçun mağduru herkes olabilir. Sistemin zilyedi ya da yararlananı olması bir şey değiştirmez. Tüzel kişiler bu suçun mağduru olamazlar.

Suçun maddi unsuru açısından 244. maddenin 1 ve 2. fıkralarında yapılan açıklamalar burada da geçerlidir. Suçun neticesi açısından failin amacı zarar vermek değil haksız bir çıkar sağlamaktır.

Bu suçun zarar mı tehlike mi suçu olduğu konusu doktrinde tartışmalıdır. Bu suç sonucunda bilişim sisteminde bir zarar oluşacağından dolayı zarar suçunu oluşturduğu görüşü doktrinde daha baskındır. Özel kasıtla işlenebilen bir suçtur ve kasten işlendiği için taksirle işlenmesi mümkün değildir.

Bu suçtan hukuka aykırılığı ortadan kaldıran sisteme girilirken verilen rızadır. Rızayı veren kişinin de rıza vermeye yetkili olup olmadığına bakmak gerekir. Teşebbüs ve iştirak bakımından bir özellik taşımayan bu suça YTCK'nın genel hükümleri uygulanır.

Bu suçun yaptırımı olarak iki yıldan altı aya kadar hapis cezası ve beş bin güne kadar adli para cezası öngörülmüştür. Tüzel kişilere de 5237 sayılı TCK'nın 60. maddesinde gösterilen kendilerine özgü güvenlik tedbirleri uygulanacaktır.

1.2.3. Banka Veya Kredi Kartlarının Kötüye Kullanılması

Madde. 245 (1) Değişik:29.06.2005-5377-27.md) Başkasına ait bir banka veya kredi kartını her ne suretle olursa olsun ele geçiren veya elinde bulunduran kimse kartı sahibinin veya kartın kendisine verilmesi gereken kişinin rızası olmaksızın bunu kullanarak veya kullandırtarak kendisine veya başkasına yarar sağlarsa, üç yıldan altı aya kadar hapis cezası ve beş bin güne kadar adli 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 on bin güne kadar adli 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 beş bin güne kadar adli para cezası ile cezalandırılır. (4) Birinci fıkrada yer alan suçun.

a- Haklarında ayrılık kararı verilmemiş eşlerden birisinin

b- Üstsoy veya altsoyunun veya bu derecede kayın hısımlarından birinin veya evlat edinen veya evlatlığın.

c- Aynı konutta beraber yaşayan kardeşlerden birinin zararına olarak işlenmesi halinde, ilgili akraba hakkında cezaya hükmolunmaz.

(5) (Ek Fırka: 06.12.2006-5560/11.md) Birinci Fıkra kapsamına giren fiillerle ilgili olarak bu kanunun malvarlığına karşı suçlara ilişkin etkin pişmanlık hükümleri uygulanır.[209]

245. madde de banka ve kredi kartlarının kötüye kullanılması eylemleri bağımsız bir suç tipi olarak düzenlenmiştir. 765 Sayılı TCK'nın 525/b.2 maddesindeki düzenlemenin karşılığıdır. 765 Sayılı TCK zamanında banka kartlarının ve kredi kantlarının kullanılmasıyla hukuka aykırı yarar elde edilmesi eylemlerini kapsayıp kapsamadığı tartışılıyordu. Bu nedenle YTCK'nın 245. maddesi düzenlenirken kredi kartı veya banka kartıyla gerçekleştirilen her türkü hukuka aykırı yarar sağlama eyleminin bu suç tipini oluşturduğu düzenlenmiştir.

[209] Türk Ceza Kanunu, Seçkin Yayınevi, Ankara, 2007, s.138

a. Suçla Korunan Hukuksal Değer

Madde gerekçesinde açıklandığı üzere banka veya kredi kartlarının hukuka aykırı olarak kullanılması suretiyle bankaların veya kredi sahiplerinin zarara sokulması, bu yolla çıkar sağlanmasının önlenmesidir.

Hırsızlık dolandırıcılık güveni kötüye kullanma ve sahtecilik suçlarının işlenme şekillerinin tümünü de içeren bu fiiller duraksamalar ve içtihat farklılıklarını önlemek amacıyla bağımsız suç haline getirilmişlerdir. Bu itibarla bu suçla aynı zamanda mağdurun mal varlığının korunması da amaçlanmıştır.[210]

b. Suçun Maddi Unsuru

1- 245. maddenin 1. fıkrasından başkasına ait banka veya Kredi Kartıyla Hukuka Aykırı yarar sağlama suçu (245/1. fıkra)

Başkasına ait bir banka veya kredi kartlarını her ne suretle olursa olsun ele geçirmesi ya da elinde bulunduran kimsenin kart sahibinin veya kartın kendisine verilmesi gereken kişinin rızası olmaksızın bunu kullanmak veya kullandırmak suretiyle kendisine veya başkasına yarar sağlanmasıdır.[211]

Banka kartı ve kredi kartının tanımlamalarını yapmamız suçun daha iyi anlaşılması açısından daha iyi olacaktır. Banka kartı 5464 sayılı Banka Kartları ve Kredi Kartları kanunu 3/d maddesinde banka kartı “mevduat hesabı veya özel cari hesapların kullanımı dahil bankacılık hizmetlerinden yararlanmayı sağlayan kart” olarak tanımlanmıştır.

5464 Sayılı Banka ve Kredi Kartları Kanununun 3/e maddesinde kredi kartı “Nakit kullanımı gerekmeksizin mal ve hizmet alımı veya nakit çekme olanağı sağlayan basılı kartı veya fiziki varlığı bulunmayan kart numarasını’’ ifade eder.

---

[210] Ali Parlar-Muzaffer Hatipoğlu, a.g.e, s.3493
[211] Ali Parlar-Muzaffer Hatipoğlu, a.g.e, s.3454

245/1. fıkradaki suçun oluşması için failin kartı nasıl ele geçirdiğinin bir önemi yoktur, kartın kullanılması bakımından da bir sınırlama yoktur. Bu suçta önemli olan failin eylemleri sonucunda hukuka aykırı olarak failin kendisine veya başkasına yarar sağlamasıdır.

2- Başkalarına ait banka hesapları ile ilişkilendirerek sahte Banka veya Kredi kartı üretme, satma, devretme, satın alma veya kabul etme suçu(245/2. fıkra)

245. maddenin 2. fıkrasındaki suçun maddi unsurunu oluşturan Seçimlik hareketler başkasına ait banka hesapları ile ilişkilendirerek sahte kartı üretmek, satmak devretmek, satın almak veya kabul etmektir.

Kredi kartı ya tamamen sahte olarak üretilebilir, ya da gerçek olarak üretilmesine rağmen üzerinde değişiklik yapılabilir. Tehlike suçu olarak görülmektedir. Bu suçun oluşumu için yarar elde etme şeklinde bir netice gerekmemektedir. Seçimlik hareketlerden birinin yapılması ile suç oluşur.

Yargıtay 6. C.D'si 31.01.2002-15823/883 sayılı kararı ile sanığın sahte olarak oluşturulan banka kredi kartlarına yabancı ülke banka kredi kartı sahibi kişilere ait bilgileri, bilişim sisteminde yer alan program ve verilerden yararlanarak zarar vermek ve haksız çıkar sağlamak için nakletme eylemini bir bütün olarak TCK'nın 525/a-2 ve 80. maddelerine uygun zincirleme tek suç oluşturduğuna karar vermiştir. YTCK'nın 245, maddesinin 2. fıkrasındaki suçu oluşturur.

Banka veya kredi kartı sahte olarak üretilmiş değil ancak kimlik bilgisindeki bilgilerin sahte olması durumunda ise banka yanıltılarak kredi kartı sağlanmıştır. Faili TCK'nın 245/3 maddesin den cezalandırmak mümkün olmayacak Failin TCK'nın 158/1-f deki nitelikli dolandırıcılıktan cezalandırılması gerekeceği söylenebilecektir.[212]

[212] Ayşe Nuhoğlu, Ceza Hukukunda Kredi Kartlarının Kötüye Kullanılması, Analiz Basım Yayınevi, İstanbul, 2002, s.92

Yargıtay 11. C.D. 01.04.2004-13869/2773 sayılı kararı ile Yapı Kredi bankasında bankanın yönetim ve denetim işlerinde bankanın tüm elektronik işlemleri ile ilgilenen BİLPA Bilgi işlem ve pazarlama şirketinde analist olarak çalışan sanığın bazı müşterilerin kredi kartı numara ve şifrelerini ele geçirerek bu bilgileri boş manyetik bantlı beyaz kartlara yüklemesi işleminde Sanık bu kartlar ile değişik zamanlarda para çekme makinaları olan ATM'ler den para çekmiştir. Sanığın buradaki eylemini Yargıtay Kredi kartı sahiplerine yönelen bir hile ve desise olmadığından dolayı dolandırıcılık olarak değerlendirmeyip ETCK'nın 525/b-2, 80. maddelerinde öngörülen zincirleme bilişim suçunu oluşturduğuna karar vermiştir.

3- Sahte oluşturulan veya üzerinde sahtecilik yapılan banka veya kredi kartıyla Hukuka aykırı yarar sağlama suçu (243/3. fıkra)

245. maddenin 3. fıkrasında tanımlanan bu suçun maddi unsuru sahte oluşturulan veya üzerinde sahtecilik yapılan bir banka veya kredi kartını kullanmak suretiyle kendisine veya başkasına yarar sağlamaktır.

Sahte kart oluşturmak gerçek kart üzerinde yapılanlar dışındaki sahtecilik fiillerini oluşturur.[213] 245/3. fıkra suçun neticesinin oluşması için failin sahte kart oluşturan veya kart üzerinde sahtecilik yapıp bunu kullanarak haksız bir yarar elde etmiş olması yeterlidir. Haksız yararı, kime sağlamış olması önemli değildir. Suç tamamlanır.

Bu konudaki çeşitli görüşlere bakarsak yanlış bilgilerle başvuru formunun doldurularak kredi kartı elde edilmesi durumunda failin sahte bir belge oluşturduğu kartın kullanılması durumunda ise belgede sahtecilik suçunu işlediğini belirtmektedir.[214]

Banka hesap cüzdanlarında yapılacak tahrifatın dolandırıcılık sayılacağına karar vermiştir. Kartın manyetik şeridinin değiştirilmesiyle sahte

[213] Ali Parlar- Muzaffer Hatipoğlu, a.g.e, s.3495.
[214] Ayşe Nuhoğlu, a.g.e, s.92.

kredi kartları ile yapılan alışverişler TCK'nın 245/3 maddesindeki suçu oluşturur.

Sahte olarak düzenlenen bir kart olmadan fail gerçeğe aykırı bir belge düzenleyerek ya da belgede tahrifat yaparak kendisine veya başkasına bir yarar sağlamışsa 5464 sayılı Banka ve kredi kartları kanunundaki 36. maddedeki suçu oluşturur, 5464 Sayılı Kanunun 36. maddesi sahte belge düzenlenmesi: Gerçeğe aykırı olarak harcama belgesi, nakit ödeme belgesi ya da alacak belgesi düzenlemek veya bu belgelerde ne suretle olursa olsun tahrifat yapmak suretiyle kendisine veya başkasına yarar sağlayanlar iki yıldan beş yıla kadar hapis ve beş bin güne kadar adli para cezası ile cezalandırılırlar.

Kredi kartı almak için yapılan sözleşmede sahtecilik yapanlar 5464 Sayılı Banka ve Kredi Kartları Kanunun 37/2 maddesine göre cezalandırılıp bu kişilere bir yıldan üç yıla kadar hapis cezası verilir.

Görüldüğü üzere banka ve kredi kartlarının kötüye kullanılması sonucunda suçun oluşabilmesi için fail tarafından yarar elde edilmesi gerekir.

c. Suçun Manevi Unsuru

Maddede tanımlanan suçlar genel kastla işlenebilir. Bu suçların taksirle işlenmesi mümkün değildir. 765 sayılı TCK zamanında YTCK' da ki 245. madenin karşılığı olan 525/b.2 maddelerinde suçun oluşması için özel kasıt aranmaktaydı.

d. Suçun Faili

Fail için özel bir özellik aranmamış, suçun faili herhangi bir kimse olabilir. Failin uzmanlık seviyesinde bir bilişim sistemi bilgisine sahip olması gerekmemektedir.

Bir görüşe göre ise suçun işlenmesi için gerekli olan banka veya kredi kartlarının kopyalanmasında kullanılan araçların yapılması teknik bilgiyi veya

uzmanlığı gerektirebileceğinden, bu durumda failde bu konulardaki uzmanlık koşulu aranacaktır. Dikkat edilmesi gereken diğer bir husus ise suçun çete oluşturularak işlenmesi durumunda çete üyelerinin hepsinde uzmanlığın aranmayacağıdır. Üyelerde birinin banka veya kredi kartlarını kopyalama konusunda uzman olması yeterli olacaktır.[215]

e. Suçun Mağduru

Bu suç tipinin mağdur açısından bir özellik göstermemektedir. Herkes mağdur olabilir.

Failin eylemi dolayısıyla mal varlığında azalma olan kişiler ile bilişim sistemlerinin ve kartlarının güvenilirliği ve genel olarak ticari itibarları zarar gören banka veya kredi kurumları bu suçun mağduru olabilirler. Hayali hesaplara bağlı olarak üretilen kartlarla işlem yapılarak doğrudan banka veya finans kurumunun mal varlığında zarara yol açılmışsa ilgili banka ya da finans kurumu doğrudan suçtan zarar gören konumunda olup suçun mağduru sayılır. [216]

f. Suçun Özel Görünüş Şekilleri

1- Teşebbüs

Maddenin her fıkrasında suç teşebbüse elverişlidir. Fail icrai hareketlere başlamış ancak suç elinde olmayan nedenlerle tamamlanamamışsa bu durumda suçun gerçekleşmemesi durumunda TCK'nın 35. maddesindeki teşebbüs hükümleri uygulanır.

Maddenin 1. ve 3. fıkralarında öngörülen suçlar haksız yararı sağlanması ile tamamlanır, Yarar elde edilemediği süre suç teşebbüs aşamasında kalır. Bu maddedeki suçlar seçimlik hareketli olduğundan icrai hareketlerden biri tamamlanmışsa tamamlanmış suça göre ceza verilir.

---

[215] Şaban Cankat, a.g.e, s.64.
[216] Murat Volkan Dülger, a.g.e, s.253.

2- İştirak

Bu suçlar iştirak bakımından herhangi bir özellik göstermediğinden dolayı YTCK'nın iştirake ilişkin genel hükümleri 37, 38, 39 ve 40. maddeleri uygulanır.

245. maddenin 2. fıkrasında sahte banka veya kredi kartı üreten, satan, devreden, satın alan veya kabul eden dediğinden kredi kartını üreten kişi başkası üreten kişiden alan kişi başkasıysa o zamanda çok failli suç olur. İkisinin de eylemi ayrı ayrıdır. Aynı eyleme iştirak etmemişlerdir.

3- İçtima

Özel bir içtima kuralı yoktur. Fail bir suç işleme kararının icrası kapsamında değişik zamanlarda başkasına ait bir banka veya kredi kartını kart sahibinin rızası dışında kullanıp kendisine veya başkasına yarar sağlarsa bu suçu aynı kişiye birden fazla işlerse TCK'nın 43/1 maddesindeki zincirleme suça ilişkin hükümler uygulanır. Eylemin farklı banka kartları ya da kredi kartları ile gerçekleşmesi durumunda aleyhine suç işlenen mağdur sayısınca suç oluşur. Faile hepsinden ayrı ayrı ceza verilir. Gerçek içtima kuralları uygulanır.

Maddenin 3. fıkrasında tanımlanan, suç açısından başka su tipleri fikri içtima bileşik suç durumları söz konusu değildir. Bu suçtan dolayı failin cezalandırılabilmesi için fiilin daha ağır cezayı gerektiren başka bir suç oluşturmaması gerekir.[217]

Fail mağdurun çantasını dolandırıcılık yoluyla ele geçirip içindeki kredi kartını alıp çantayı atmış ve kartı kullanıp kendine haksız yarar sağlamışsa fiille yalnızca 245/1 maddesinin uygulanabileceği söylenebilir.[218]

Harcama yapmadığı halde temin ettiği kredi kartı ile benzin istasyonundaki post kartını benzin alınmış gibi gösterip buna benzin alınmış

[217] Ali Parlar- Muzaffer Hatipoğlu, a.g.e, s.3497
[218] Ali Karagülmez, a.g.e, s.205

gibi gösterip buna ait bedelleri bankadan tahsil eden failin eylemi hem dolandırıcılık suçunu hem de banka veya kredi kartlarının kötüye kullanılması suçunu da oluşturmaktadır. Burada 44. madde uyarınca en ağır cezayı içeren TCK' nın 245/1 maddesinde hüküm kurulur.[219]

g. Hukuka Aykırılık Unsuru

Bu suçlar bakımından ilgilinin rızası ve zorunluluk hali gibi durumlarda hukuka uygunluk nedeni var kabul edilir.

h. Suça Etki Eden Nedenler (Cezasızlık Hali)

1- Cezasızlık Hali

245. maddenin 4. fıkrasında cezasızlık nedenleri öngörülmüştür. Buna göre birinci fıkrada yer alan suçun.

a- Haklarında ayrılık kararı verilmemiş eşlerden birinin.

b-Üstsoy veya alt soyunun veya bu derecede kadın hısımlarından birinin veya evlat edinenin veya evlatlığın.

c- Aynı konutta beraber yaşayan kardeşlerden birinin zararına işlenmesi halinde ilgili akraba hakkında ceza verilmez, CMK'nın 223/4-b bendi uyarınca faile ceza verilmesine yer olmadığı kararı verilir. TCK'nın 245/4 maddesindeki cezasızlık nedeni kişiseldir. İştirak halinde işlenen suçlarda maddede sayılanlar dışındaki kimselerin cezalandırılmasına engel değildir.[220]

2- 245/1 fıkrasındaki suç açısından Etkin pişmanlık (245/5. fıkra)

5560 sayılı Kanunla 2006 yılında getirilmiştir, 245/1 fıkra kapsamına giren fiillerle ilgili olarak YTCK'nın mal varlığına karşı suçlarına ilişkin hükümleri uygulanır.

---

[219] Levent Kurt, a.g.e, s.270.
[220] Sulhi Dönmezer, a.g.e, s.595.

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

1- Kovuşturma

Maddede tanımlanan soruşturma ve kovuşturma resen yapılır.

2-Görevli Mahkeme

5235 Sayılı Kanunun 11. maddesi uyarınca bu suçlar dolayısıyla açılan davalara bakma görevi Asliye Ceza Mahkemesine aittir.

3- Suçun Yaptırımı

Bu suçlar için öngörülen yaptırımlar şunlardır.

1- 1. fıkrada üç yıldan altı aya kadar hapis ve beş bin güne kadar adli para cezası

2- 2. fıkrada üç yıldan yedi yıla kadar hapis ve on bin güne kadar adli para cezası

3- 3. fıkrada ise dört yıldan sekiz yıla kadar hapis ve beş bin güne kadar adli para cezasıdır.

4- Dava Zamanaşımı

YTC'nın 66/1-d bendi uyarınca bu sulardan açılan davalar da dava zamanaşımı süresi on beş yıldır.

1.3. 5237 Sayılı 'TCK' da ki Diğer Bilişim Suçları

1.3.1. Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar Bölümünde Düzenlenen Suç Tipleri

1.3.1.1. Haberleşmenin Gizliliğini İhlal Suçu

TCK'nın 132. maddesinde düzenlenen bu suç tipiyle kişiler arasındaki haberleşmenin gizliliğini iptal eden kişi cezalandırılır denmektedir. 1. fıkrasında gizliliği ihlal eylemleri suç sayılırken gizliliği ihlal ederken bir

yandan da haberleşme içeriklerini kayda alırsa faile ceza arttırılarak uygulanır, kayıt her türlü aletle yapılabilir.

Bu suçun oluşmasında failde genel kast aranır.

Maddenin 2. fıkrasında ise haberleşme içeriklerinin hukuka aykırı olarak fail tarafından ifşa edilmesi suç sayılmıştır. İfşa edilme eylemi hukuka aykırı olmalıdır.

Maddenin üçüncü fıkrasında ise kendisiyle yapılan haberleşmenin içeriğini mağdurun rızası olmadan alenen ifşa eden fail cezalandırılır. 3. fıkrada aleniyet unsuru suçun özel şartıyken 2. fıkrada aleniyet unsuru yoktur.

Suç genel kastla işlenebilir ve takibi şikâyete bağlıdır ve aleniyet unsuru zorunludur.[221]

Maddenin dördüncü fıkrasında ise taraflar arasında geçen haberleşme içeriğinin basın ve yayın yoluyla yayınlanması da suç olarak kabul edilip faile verilecek ceza yarı oranın da arttırılır.

Kişiler arasında geçen haberleşme mektupla, telefonla, telgrafla, elektronik posta yoluyla yapılabilir. Bu suç için önemli olan haberleşmenin ne ile yapıldığı değil kişiler arasında yapılmasıdır.

Maddenin 2. fıkrası bu suçun nitelikli halidir. 2. fıkradaki ifşanın açıkça hukuka aykırı olması gerekir. Hukuka uygunluk sebebinin olmaması gerekir. İfşa haberleşme içeriklerinin yetkisiz üçüncü kişilerce öğrenilmesidir. Soruşturma ve kovuşturma aşamasında kişileri arasında geçen haberleşme içeriklerinin bir suçla ilgili kayda alınması ile mahkemede duruşma sırasında okunması sırasında suç oluşmaz.

[221] Durmuş Tezcan ,Mustafa Ruhan Erdem, Murat Önok, Teorik ve Pratik Ceza Özel Hukuku 5560 Sayılı Kanuna Göre Güncellenmiş 5. Baskı, Seçkin Yayıncılık, Ankara, 2007 s.460

Maddenin üçüncü fıkrasında ise suçun oluşması için alenen haberleşme içeriğinin ifşa edilmesi gerekiyor. Dördüncü fıkrada da kişiler arasında geçen haberleşme içeriğinin basın ve yayın yolu ile yayınlanması halinde ikinci ve üçüncü fıkraya göre verilecek ceza da artırım öngörülmüştür.[222]

Suçun faili herkes olabilir. Burada fail haberleşmenin tarafları dışındaki birisidir.[223]

Suçun mağduru herkes olabilir. Suç tehlike suçudur. Bir zararın doğması aranmaz, suçla korunan hukuki yarar ise kişilerin özel hayatı ve hayatın gizli alanıdır.

Suça teşebbüs ve iştirak bakımından ise 5237 sayılı TCK'nın genel hüküm maddeleri uygulanır.

765 Sayılı TCK'nın 195 ve 197 maddelerine göre elektronik sohbet ve elektronik posta yoluyla suçun işlenip işlenmeyeceği uygulamada tartışmalı iken YTCK, 132. maddesi ile bu suçun her türlü yayınla işlenebileceğini düzenleyerek tartışmalara son noktayı koymuştur. Ayrıca ETCK zamanında bu suç zarar suçuydu. Suçun oluşması için zararın meydana gelmesi gerekirken YTCK da tehlike suçudur.

1.3.1.2. Özel Hayatın Gizliliğini İhlal Suçu

134. maddede birinci fıkrada özel hayatın ihlali suç olarak tanımlanmaktadır. Özel yaşam alanına girilerek başkaları tarafından görülmesi mümkün olmayan bir özel olayın kaydedilmesi cezalandırılmaktadır.

İkinci fıkrada ise elde edilen saptama ve kayıtlardan herhangi bir suretle karar sağlanması veya bunların başkalarına verilmesi başka kişilerin

[222] 5237 sayılı YTCK'nun 132. madde gerekçesi
[223] Doğan Soyaslan, Ceza Hukuku Özel Hükümler Gözden Geçirilmiş 6. baskı, Yetkin Yayınevi, Ankara, 2006, s.268

bilgi edinmesi, basın ve yayın yoluyla açıklanması suçun ağırlaşmış şeklini oluşturmaktadır. İkinci fıkrada kişinin özel hayatına ilişkin görüntü ve seslerin hukuka aykırı olarak ifşa edilmesi ayrı bir suçtur. Bu görüntü ve sesler kayda alınırken hukuka uygunluk sebebinin olmaması gerekir.

Suçun faili ve mağduru herkes olabilir. Tüzel kişiler mağdur olamaz.

Suç iştirak ve içtima bakımından bir özellik taşımamaktadır. YTCK'nn genel hükümleri uygulanır. Takibi şikâyete bağlıdır. Genel kastla işlenebilen bir suçtur.

İlgilinin rızası karar hükmünün icrası hukuka uygunluk nedenidir.[224] TCK'nın 137 maddesinde bu suçun nitelikli hali sayılmış. Bu suçu görevinin verdiği yetkiyi kötüye kullanarak failin işlemesi ağırlatıcı sebep sayılmıştır.

1.3.1.3 Kişisel Verilerin Kaydedilmesi Suçu

5237 Sayılı TCK'nın 135. maddesinde düzenlenmiştir. (1). Hukuka aykırı olarak kişisel verileri kaydeden kimse altı aydan üç yıla kadar hapis cezası verilir. (2) Kişilerin siyasi felsefi veya dini görüşlerine ırki kökenlerine hukuka aykırı olarak ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin bilgileri kişisel veri olarak kaydeden kimse yukarıdaki fıkra hükmüne göre cezalandırılır. [225] ETCK' da bu maddenin karşılığı yoktur.

Maddenin. 2. fıkrasındaki düzenleme ile mevzuatımız AB'nin "Kişisel verilerin Korunması Yönergesine" uyumlu hale getirilmiştir. .Bu yönergenin 25. maddesi bilgi korunmasına sahip olmayan ülkelere bilgi akışını yasaklamaktadır.[226]

Avrupa Birliği tarafından 1995 yılında 95/46/EC sayılı "Kişisel verilerin işlenmesi ve serbest dolaşımı bakımından bireylerin korunması" konulu

[224] Şaban Cankat Taşkın, a.g.e, s.96
[225] Türk Ceza Kanunu, Seçkin Yayınevi, Ankara, 2007, s.92
[226] Doç. Dr. Mustafa Topaloğlu, Bilişim Hukuku, Karahan Kitabevi, Adana, 2005, s.167

direktifte vatandaşlıkları söz konusu olsun olmasın bütün üye ülkelerdeki kişilerin kişisel verilerinin korunması ve bu verilerin Avrupa Birliği sınırları içerisinde serbest dolaşımını sağlayacak kapsamda güvenli bir düzenleme yapılması amaçlanmıştır. 2002 yılında ise "Elektronik İletişim sektöründe kişisel verilerin işlenmesi ve Mahremiyetin korunmasına'' ilişkin 2002/581/ EC Sayılı direktif kabul edilmiştir. TCK'nın 135. maddesindeki düzenleme 1999 yılında kabul edilen İnternette özel hayatın korunmasına ilişkin R (99) 5 sayılı Tavsiye kararındaki "İnternet kullanımı her eylem bakımından bir sorumluluğu gerektirir, özel hayat açısından riskler içerir. İnsanın kendi kendisini koruyacak şekilde hareket etmesi önemlidir. Hak ve yükümlülükler saklı kalmak üzere özel hayatın korunmasına ilişkin bazı pratik çözümler önerilebilir. Özel hayata saygı gösterilmesi her fert için temel bir hak olup verilerin korunmasına ilişkin yasalarla da korunabilir açıklamasıyla paralellik gösterir.[227]

Çağımızda kişilerle ilgili kayıtlar bazı kamu ve özel kuruluşlar tarafından bilgisayar ortamına aktarılarak muhafaza edilmektedir. Bu bilgiler başkalarının 3. kişilerin eline geçtiğinde de hakkında bilgi toplanan kişiler zarara uğramaktadır. Kişilerle ilgili bilgilerin hukuka aykırı olarak kayda alınması suç olarak tanımlanmıştır.

a. Korunan Hukuksal Yarar

Korunan hukuksal değer genel olarak kişilerin özel hayatıdır.

Bir görüşe göre ise madde gerekçesinden yola çıkarak maddede gerçek kişiyle ilgili her türlü bilgi veya kişisel verinin korunduğunu belirterek korunan hukuki yararı "kişilerin özel hayatı ve buna ilişkin veriler" olarak belirlemektedir.[228]

---

[227] Durmuş Tezcan, İnternet Karşısında Özel Hayatın Korunması ve Adli Yardımlaşma Uluslar arası İnternet Hukuku Sempozyomu 21-22 Mayıs 2001 DEÜ yayımı, İzmir, 2002, s.634-635

[228] Ali Karagülmez, a.g.e, s.268

b. Suçun Konusu

Maddenin gerekçesinde suçun konusunun kişisel veriler olduğu belirtilmiştir. Maddenin ikinci fıkrasında kişisel veriler sınırlı olarak sayılmıştır. Kişilerin Siyasi, felsefi ve dini görüşleri, ırkları, sendikal bağlantıları, cinsel yaşamları ve sağlık durumları kişisel veri olarak sayılmıştır. Bunların dışında veriler kaydedilirse TCK'nın 135/1 fıkrasına göre ceza verilir.

c. Suçun maddi unsurları: Kişisel verilerin hukuka aykırı olarak her türlü kayıt altına alınması fiili ile suç oluşur. Bu suçun işlenme şekli ve alanı sınırlandırılmamıştır. Suçta netice önemli değildir, kayıt edilme olayı ile su oluşur. Suçun oluşumunda bir zararın oluşması gerekmez.

d. Suçun Manevi Unsurları

TCK'nın 135/1 maddesindeki suçun oluşması için failin özellikle kişisel verileri hukuka aykırı olarak kaydetme kastı vardır. Birinci fıkra bakımından özel kast aranır TCK'nın 135/2 fıkrasında ise genel kast aranır.[229]

Fail hukuka aykırı olarak bilerek ve isteyerek hareket ettiği için bu suçun taksirle işlenmesi mümkün değildir.

e. Suçun faili ve mağduru: Suçun faili herkes olabilir. YTCK'nın 137 maddesinde 1. fıkranın a bendine göre bu suçların kamu görevlisinin görevinin verdiği yetkiyi kötüye kullanmasıyla işlemesi ve YTCK'nın 137. maddenin 1. fıkrası b. Bendine göre ise belli bir meslek ve sanatın sağladığı kolaylıktan yararlanmak suretiyle işlenmesi haline de ceza yarı oranında arttırılır demektedir.

Bu suçun mağduru herkes olabilir. Mağdur olabilmek için yasanın öngördüğü tek zorunlu koşul verilerin maliki veya zilyedi olmaktır.[230]

[229] Ali Karagülmez, a.g.e, s.232
[230] Murat Volkan Dülger, a.g.e, s.269.

f. Suçun Özel Görünüş Şekilleri

1- Teşebbüs.

Kişisel verilerin kaydedilmesi suçunun teşebbüs halinde kalması mümkündür. Fail eylemi gerçekleştirmek için harekete başlayıp ta elinde olmayan sebeplerle kendi isteği dışında fiili tamamlayamazsa fiil teşebbüs aşamasında kalacaktır.

2- İştirak

İştirak bakımından TCK'nın genel hüküm maddeleri TCK 37,38,39,40. maddeleri uygulanır. Suça iştirak eden kamu görevlisi veya bu konu ile ilgili belli bir meslek veya sanat sahibi ise bu kişilere TCK'nın 137. maddesi uyarınca ceza arttırılarak verilir.

3- İçtima

TCK'nın 135 maddesindeki suçun işlenmesi için TCK'nın 243/1 maddesindeki hukuka aykırı bilişim sistemine girme ve bir müddet kalma suçu geçit özelliği taşıyabilir. Bu durumda TCK'nın 44. maddesi gereğince fikri içtima uygulanarak ağır ceza alan TCK'nın 135. maddesinden ceza verilir.

g. Suça Etki Eden Sebepler.

TCK 135. maddesinde suça etki eden neden TCK'nin 137. maddesinde düzenlenen failin kamu görevlisi olması veya belli bir meslek ve sanatın sağladığı kolaylıktan yararlanmak suretiyle bu suçu gerçekleştirilmesi halinde faile ceza arttırılarak verilir.

h. Hukuka Aykırılık Unsuru

Kişisel verilerin kaydedilmesi suçunda mağdurun rızası eylemi hukuka uygun hale getirecektir.

TCK'nın 135/1 deki eylem bakımından, failin eylemin hukuka aykırı olduğunu ayrıca bilmesi gerekmektedir. İlk fıkradaki kişisel verilerin kaydedilmesi bakımından aranan hukuka aykırılık türü "hukuka özel aykırılıktır.[231]

Kanunun verdiği yetkiye dayanılarak kişisel verilerin kaydedilmesi bir hukuka uygunluk sebebidir.

CMK'nun 135 maddesindeki iletişimin tespiti ve kayda alınması ile CMK'nun 134. maddesinin 3. fıkrasındaki bilgisayarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma işlemi sırasında sistemdeki bütün verilerin yedeklemesi yapılır ve verilerin içine girilir, TCK'nun 135 maddesinin 2. fıkrasında verilerin kaydedilmesinde failin yaptığı eylemin hukuka aykırı olduğunu bilmesine gerek yoktur. Kanununu bilmemek mazeret sayılmaz ilkesi burada uygulanıyor.

ı. Yaptırım

TCK 135. maddedeki suçu işleyenler hakkında suçun cezası olarak altı aydan üç yıla kadar hapis cezası görülmüştür.

TCK'nın 140. maddesinde kişisel verilerin hukuka aykırı olarak kaydedilmesi suçunun tüzel kişiler tarafından işlemesi hali yaptırıma bağlanmıştır. TCK'nın 60. maddesindeki güvenlik tedbirleri uygulanır.

1.3.1.4. Kişisel Verileri Hukuka Aykırı Olarak Verme Veya Ele Geçirme Suçu

TCK'nın 136. maddesinde düzenlenmiştir. "Kişisel verileri hukuka aykırı olarak bir başkasına veren, yayan veya ele geçiren kişi bir yıldan dört yıla kadar hapis cezası ile cezalandırılır hükmüne yer verilmiştir.[232]

---

[231] Doğan Soyaslan, a.g.e, s.273.
[232] Nevzat Toroslu-Metin Feyzioğlu, Türk Ceza Kanunu –Ceza muhakemesi Kanunu ve ilgili kanunlar, Savaş Yayınevi, Ankara, 2009, s. 133.

Hukuka uygun olarak kaydedilmiş kişisel verilerin hukuka aykırı olarak başkasına verilmesi, yayılması veya değiştirilmesi eylemleri suç olarak düzenlenmiştir.

Bu suça kimlik hırsızlığı suçu da denir. Hemen hemen tüm kişisel bilgiler ve kimlik bilgileri internette bulunmaktadır. Bu bilgileri kişiler kendi rızaları ile sitelere verirler. Bu verilerin hukuka aykırı olarak ele geçirilmesi maddede tanımlanan suçu oluşturur.[233]

765 Sayılı TCK'nın 525/a.1 maddesi YTCK'nın 136. maddesindeki suçun karşılığıdır. 765 sayılı TCK'nin 525/a-1 maddesindeki düzenleme gerçek ve tüzel kişiler hakkında uygulanırken YTCK'nın 136. maddesi gerçek kişiler bakımından uygulanıyor. Tüzel kişiler ve kamuya ait bilişim sistemlerindeki veriler bu kapsamda kalmaz.

a- Korunan Hukuksal Değer

TCK'nın 135. maddesindeki kişisel verilerin kaydedilmesi suçu ile TCK'nin 136. maddesindeki korunan hukuksal değer aynıdır. Bu suçla kişilerin özel yaşamı özel kişisel verileri korunur.

b- Suçun Konusu

Suçun konusunu kişisel veriler oluşturur.

c- Suçun Maddi Unsuru

Bu suç seçimlik hareketli bir suçtur. Verilerin verilmesi yayılması veya ele geçirilmesi fiillerinden herhangi birinin gerçekleşmesiyle suç tamamlanmış olur.

1- Kişisel Verilerin Başkasına Verilmesi Eylemi

Kişisel veriler kağıda yazdırılarak elden verilebileceği gibi posta ile de gönderilebilir. Elektronik posta ile de gönderilebilir. Sanal ortamda bulunan

[233] Murat Volkan Dülger, a.g.e, s. 276.

kişisel veriler bir CD-Rom veya mobil disk üzerine kaydedilerek gönderilmesi yoluyla verilmesi gösterilebilir.[234]

2- Kişisel Verilerin Yayılması Eylemi

Kişisel verilerin birçok kişiye verilmesi eylemidir. Yazılı görsel/sanal yayın yoluyla yapılabilir.

İnternet üzerinde kişilerin kişisel verilerini herkesin ulaşabileceği şekilde yayınlamak suretiyle gerçekleşebilir.

3- Kişisel Verilerin Ele Geçirilmesi Eylemi

Kişisel verilerin kayıtlı olduğu yerden hukuka aykırı olarak yetkisiz erişimle, sistemi müdahale etmeksizin özel programlarla ele geçirilmesidir.

d- Manevi Unsur

Failin genel kastla hareket etmesi suçun oluşması için yeterlidir. Taksirle bu suç işlenemez.

e- Fail

Suçun faili herkes olabilir.

f- Mağdur

Suçun mağduru herkes olabilir.

g- Netice

Suçun oluşması için zararın oluşmasına gerek yoktur. Seçimlik hareketlerden birinin gerçekleşmesiyle suç tamamlanır.

[234] Şaban Cankat Taşkın, a.g.e, s. 101.

h- Hukuka Aykırılık Unsuru

Failin eylemin hukuka aykırı olduğunu bilmesi ve buna rağmen eylemini gerçekleştirmesi gerekir.

İlgilinin rızası veya yasa ile verilen yetki nedeniyle verilerin verilmesi yayılması ele geçirilmesi hukuka uygunluk sebebidir.

ı- Suçun Özel Görünüş Şekilleri

1. Teşebbüs

Bu suça teşebbüs mümkündür. Fail tarafından icra hareketlerine başlandıktan sonra dışarıdan gelen bir sebeple hareketlerin eylemin tamamlanamaması sebebiyle eylem yarıda kalır. Teşebbüs hükümleri uygulanır. Bu suçta zarar meydana gelmesi aranmadığından tehlike suçu olması nedeniyle madde metninde belirtilen eylemleri gerçekleştirmesi ile suç tamamlanır.

2. İştirak

TCK'nin 37-40. maddeleri arasındaki genel hükümleri uygulanır. Suça iştirak edenlerden biri kamu görevlisi ise TCK'nin 137. maddesindeki ağırlatıcı neden uygulanır.

3. İçtima

Kişisel verileri hukuka aykırı olarak fail verme veya ele geçirme suçunu aynı kişiye karşı değişik zamanlarda birden fazla işlerse YTCK'nın 43. maddesinde düzenlenen zincirleme suç hükümleri uygulanıp failin cezasının oranı arttırılır. Her suç bağımsız bir suç ise o zaman gerçek içtima kuralları uygulanıp ayrı ayrı her suçta ceza verilir.

YTCK'nın 135'teki verilerin kaydedilmesi suçuyla YTCK 136 maddesindeki kişisel verilerin hukuka aykırı olarak bir başkasına verilmesi yayılması ele geçirilmesi için failin öncelikle TCK'nın 135. maddedeki kişisel

verileri kaydedip ondan sonra TCK'nin 136. maddesindeki suçu işler. TCK'nın 135. maddesindeki suç TCK'nın 136. maddesinde ki suç için geçit suçudur. YTCK'nın 44. madde gereğince fail ağır olan eylemi TCK'nın 136. maddesinden ceza alır.

i. Suça Etki eden Sebepler

TCK'nin 136. maddesindeki suça etki eden sebepler TCK'nın 137. maddesinde öngörülmüş olup failin sıfatından kaynaklanan bir ağırlatıcı sebep vardır. 137. maddede bu suç kamu görevlisinin görevinin verdiği yetkiyi kötüye kullanarak veya belli bir meslek ve sanat icra eden failin mesleğinin sağladığı kolaylıktan yararlanarak suçun gerçekleştirilmesidir.

j. Yaptırım

Kişisel verileri hukuka aykırı olarak verme veya ele geçirme suçunu işleyenler hakkında suçun cezası bir yıldan dört yıl kadar hapis cezasıdır. TCK'nın 140. maddesi gereğince suçun işlenmesinden tüzel kişinin hukuka aykırı yarar sağlaması durumunun da 5237 Sayılı TCK'nin 60. maddesindeki güvenlik tedbirleri uygulanır.

1.3.1.5. Kişisel Verilerin Yok Edilmemesi Suçu

TCK'nın 138. maddesinde düzenlenmiştir. Kanunların belirlediği sürelerin geçmiş olmasına karşın verileri sistem içinde yok etmekle yükümlü olanlara görevlerini yerine getirmediklerinden dolayı altı aydan bir yıla kadar hapis cezası verilir.

765 Sayılı TCK'de bu suçun karşılığı bulunmamaktadır. Yasal süresi dolmasına rağmen sistem içindeki kişisel verileri yok etmekle görevli olan kişilerin bu görevlerini yerine getirmemesi nedeniyle suç oluşur.

a. Korunan Hukuksal Değer

Bu suç tipiyle korunan hukuksal değer kamu idaresinin güvenirliği ve işleyişi ile kişisel verilerin güvenliğidir.[235] Bu suçla korunan ikinci hukuki yarar ise hem kişisel verilerin kendisi hem de kişisel veriler için oluşturulmak istenen güvenliktir.[236] Bu suçu incelerken TCK'nın 257. maddesindeki görevi kötüye kullanma suçuna da bakmak gerekiyor. Failin eylemi TCK'nın 138. maddesindeki suça giriyorsa 138. madde uygulanır. Çünkü TCK 257. madde genel bir maddedir. Öncelikle özel hükümler uygulanır. Özel hüküm yoksa genel hükümler uygulanır. Ayrıca 138. maddedeki suçun oluşması için failin kamu görevlisi olması gerekmiyor. Kamu görevlisi olmayan kişilere de görev verilir. TCK'nın 257. maddesinde ise verileri yok etmekle görevli olan kişi bunu kamu görevi olarak yapmaktadır.

b. Suçun Konusu

Verileri yok etmeme suçunun konusu da kişisel verilerdir

c. Suçun Maddi Unsurları

Suçun oluşması için biri fail diğeri yasadan olmak üzere iki temel önkoşulun gerçekleşmesi gerekir. Failden kaynaklanan önkoşul failini yasa ile verileri yok etmekle görevlendirilmiş olmasıdır.

İkinci ön koşul ise yasadan kaynaklanır. Ve verilerin yok edilmesi gereken yasal süre içerisinde yok edilmemiş olması durumunda suç oluşur.[237]

Bu suç neticesi harekete bitişik bir suçtur, kanunen faile verileri yok etmesi için verilen süre sonunda suçun sonucu belli olacağı için süre sonunda verileri yok etmemişse suç oluşur.

---

[235] Murat Volkan Dülger, a.g.e, s. 282
[236] Murat Volkan Dülger, a.g.e, s. 282.
[237] Ali Karagülmez, a.g.e, s 238

d. Suçun Manevi Unsurları

Bilerek ve isteyerek fail suçu işler taksirle işlenebilmesi mümkün değildir.

e. Suçun Faili ve Mağduru

Suçun faili verileri yok etmekle görevli olan kişidir. Fail kamu görevlisi sıfatını taşımak zorundadır. Bu suç yine de özgü bir suçtur. Bu suç kendine özgü bir görevi ihmal suçudur.

Yasa ile verilerin yok edilmesi görevi verilen herhangi bir kimse bu suçun faili olur.

Suçun mağduru kamu ve toplumdur. Kişisel verileri yok edilmeyen kişide mahkeme aşamasında davaya katılabilir.

f. Hukuka Aykırılık Unsuru

Bu suç açısından mağdurun rızası hukuka uygunluk nedeni sayılamayacaktır. Bu suçta mağdur birey değil kamudur. Mücbir sebep nedeniyle hukuka uygunluk nedeni olarak kabul edilebilir.

g. Suçun Özel Görünüş Şekilleri

1. Teşebbüs

Bu suç ihmal suretiyle işlenebildiğinden bu suça teşebbüs söz konusu olmaz.

2. İştirak

YTCK'nın 37, 38, 39, 40. maddelerindeki genel düzenlemeler uygulanır. Sadece TCK'nın 39/2.b ve c bendinde yazılı olan iştirak türünün oluşması zordur.

3. İçtima

Fail aynı suçu işleme kastıyla aynı mağdura karşı değişik zamanlarda birden fazla işlerse TCK'nın 43. maddesindeki zincirleme suça ilişkin hükümler uygulanır. Her eylem için ayrı ceza verilmez. Tek ceza verilip belli oranda cezası arttırılır.

h. Yaptırım

Kişisel verileri yok etmeme suçunu işleyen failler için yasada yalnızca hürriyeti bağlayıcı ceza öngörülmüştür. Suçun cezası da ise 6 aydan 1 yıla kadar hapistir.

5237 Sayılı TCK'nın 140. maddesi gereğince bu suçun işlenmesinden dolayı tüzel kişilerin hukuka aykırı yarar sağlaması halinde bunlara 5237 Sayılı TCK'nın 60. maddesinde gösterilen kendilerine özgü güvenlik tedbirleri uygulanacaktır.

1.3.1.6. 5237 Sayılı TCK'nin 124. Maddesi "Haberleşmenin Engellenmesi Suçu"

TCK'nın 124. maddesi Yeni TCK'nın kişilere karşı suçlar başlıklı ikinci kısmının Hürriyete Karşı Suçlar başlıklı yedinci bölümünde düzenlenmiştir.

Haberleşmenin engellenmesi suçunun bilişim suçları aracılığıyla işlenmesi mümkündür.[238] Günümüzde haberleşme internet aracılığıyla, elektronik posta, telefon görüşmeleri telgraf gibi iletişim araçlarıyla sağlanmaktadır.

Bu suçun madde gerekçesinde haberleşme araçları sayılmamıştır. Ancak haberleşmenin bilişim sistemleri aracılığıyla engellenmesi TCK'nın 124. maddesindeki suçu oluşturur. Bu suç 765 Sayılı TCK'nın 391. maddesinin karşılığıdır. 765 sayılı TCK yalnızca telefon, telgraf veya telsiz iletişiminin engellenmesi suç olarak düzenlenmiş ancak internet iletişiminin

[238] Murat Volkan Dülger, a.g.e,s. 288.

engellenmesini suç olarak düzenlememiştir. YTCK ile internet iletişiminin engellenmesi de suç sayılmıştır.[239]

Kişiye veya herhangi bir kamu kurumunun elektronik hesabına gelen iletilerin muhatabı tarafından ulaşılmasından önce ulaşımının engellenmesi maddede yazılı suçu oluşturur. Bu engellemenin hukuka aykırı yapılması gerekir.[240]

Maddenin birinci fıkrası kişiler arasındaki haberleşmeyi kapsarken bu suçun oluşması için belirli kişiler arasındaki haberleşmenin engellenmesi hukuka aykırı bir şekilde olmalıdır. Haberleşmenin yapıldığı araç önemli değildir. Telefon hatlarının kesilmesi, elektromanyetik alan oluşturarak görüşmenin karıştırılması araya girerek görüşmeleri engelleme, e-mail metinlerinin değiştirme şeklinde olabilir. Maddenin ikinci fıkrasında kamu kuruluşları arasındaki haberleşmenin hukuka aykırı olarak her türlü engellemesini düzenleyen YTCK ceza miktarını da arttırmıştır. Üçüncü fıkrada ise basın yayın organının yayınının hukuka aykırı bir şekilde engellenmesini düzenleyip bu suçu işleyenlerinde maddenin ikinci fıkrasına göre cezalandırılmasına yer vermiştir.

Haberleşme hürriyetine bir kamu görevinin gereği olarak engelleme getirilmişse bu durumda hukuka aykırılık olmadığı için suçta oluşmaz. Haberleşme hürriyeti anayasa ile de güvence altına alınıp yine anayasada yer alan savaş olağanüstü hal durumları da duruma göre engellenebilir.

1.3.1.7. 5237 Sayılı TCK'nin 125. maddesinde düzenlenen Hakaret Suçunun Bilişim Sisteminin Kullanılması Yoluyla İşlenmesi

5237 Sayılı TCK'nın "şerefe karşı suçlar" başlıklı sekizinci bölümde düzenlenmiştir. 765 Sayılı TCK dönemindeki hakaret ve sövme ayrımı kaldırılıp yerine tek bir düzenleme ile hem hakaret hem de sövme suçu düzenlenmiştir.

---

[239] Şaban Cankat Taşkın, a.g.e, s. 114.
[240] Levent Kurt, a.g.e, s. 282.

Maddenin ikinci fıkrasında eylem sesli, yazılı ve görüntülü bir iletiyle işlenirse suç olarak kabul edilmiştir.

Hakaret suçunun bilişim sistemleri aracılığıyla e-mail yoluyla hakaret içeren yazı, resim veya karikatür gönderilmesi, cep telefonunda mesaj çekilmesi suretiyle işlenmesi de cezalandırılacaktır.[241] Bu suçla korunan hukuksal yarar şereftir.

Maddenin dördüncü fıkrasında da hakaretin alenen işlenmesi ağırlaştırıcı neden olarak öngörülmüştür. Aleniyet unsuru iletiyi mağdur dışında üçüncü kişilerinde görmesi demektir. Sanal ortamda işlenen hakaret suç örneğin internette bir kişiyle ilgili hakaret cümleleri ve yorumları bu iletileri başkaları da gördüğü zaman aleniyet unsuru gerçekleşmiş olacağından faile ceza arttırılarak verilir.

Yine dördüncü fıkrada hakaret suçunun basın ve yayın yoluyla işlenmesini de artırım nedeni olarak kabul etmiştir.

1.3.1.8. 5237 Sayılı TCK'nin 142. Maddesinde Bilişim Sistemi Yoluyla İşlenen Hırsızlık Suçu

TCK'nın 142. maddesinin ikinci fıkrasının "e" bendinde düzenlenmiştir. Hırsızlığın bilişim sistemi aracılığıyla işlenmesi "nitelikli" hırsızlık sayılmıştır.[242]

141. maddede hırsızlık zilyedin rızası dışında başkasına ait taşınır mali failin kendisine veya başkasına yarar sağlamak için bulunduğu yerden almasıdır. Bu suçun bilişim sistemleri yoluyla işlenmesi nitelikli hırsızlık sayılmış örneğin failin mağdura ait banka hesaplarından kendisinin veya başkalarının hebasına mağdurun rızası dışında para aktarması TCK'nın 142/2.e maddesinde cezalandırılabilmesine olanak tanımaktadır.

---

[241] Murat Volkan Dülger, a.g.e, s. 289.
[242] Erdal Noyan, Hırsızlık ve Yağma Suçları, Bilge Yayınevi, Ankara 2005, s. 246.

Doktrinde bazıları verinin somut nesne veya elektrik enerjisi gibi olmadığını bu nedenle kanun koyucunun 142/2e maddesine yer vermesini çelişki olarak değerlendirirken[243] bazıları da bilişim yoluyla işlenen suçun konusunun veri olduğunu klasik anlamdaki hırsızlık suçu gibi işlenemeyeceğini bu nedenle bilişim yoluyla hırsızlığın ayrı işlenmesini kanun koyucunun ayrı düzenlediğini ileri sürmüştür.[244]

Bu suçun konusu kişinin malvarlığı değerleridir.

1.3.1.9. 5237 Sayılı TCK'nin 158. Maddesinde Düzenlenen Bilişim Yoluyla Dolandırıcılık Suçu

5237 Sayılı TCK'nın malvarlığına karşı suçlar başlıklı onuncu bölümünün 158. maddesinin 1. fıkrasının f bendinde düzenlenmiştir. 158. madde dolandırıcılık suçunun nitelikli hallerini düzenlemiştir.

Dolandırıcılık suçunda failin sorumlu tutulabilmesi için gerçek bir kişiye karşı hileli davranışlarda bulunulması gerekir. 158. maddenin 1. fıkrasının f bendinde birden fazla nitelikli hal belirtilerek bilişim sistemlerinin, banka veya kredi kurumlarının araç olarak kullanılması suretiyle işlenmesi halinde iki yıldan yedi yıla kadar hapis ve beş bin güne kadar adli para cezasına hüküm olunur denmektedir.

Günümüzde bilişim yoluyla dolandırıcılığına en çok görüldüğü yer internet üzerinde gerçekleştirilen elektronik ticaret dolandırıcılıkları ve internetteki müzayede sitelerinde yaşanan olayları örnek verebiliriz. Örneğin kişi sahte ticari bir web sitesi oluşturup mağdurların güveninin kazanıp onlara satacağını vaat edip para havale etmelerini sağlayarak dolandırıcılık suçu işlenebilir yine para çekme cihazlarında önceden hazırladıkları tertibatla bankamatik kartının sıkışmasını sağlayıp banka görevlisi ile telefonda görüşüyormuş gibi yapıp mağdurdan kartın şifresini öğrenip bankadan para çekilmesi eylemi de TCK'nin 158/1-f maddesi kapsamında kalır.

---

[243] Murat Volkan Dülger, a.g.e, s. 289, 290.
[244] Levent Kurt, a.g.e, s. 282

1.3.1.10. 5237 Sayılı TCK Müstehcenlik Suçu

5237 Sayılı TCK'nın topluma karşı suçlar başlıklı üçüncü kısmının genel ahlaka karşı suçlar başlıklı yedinci bölümünün 226. maddesinde düzenlenmiştir.

Maddenin metninde müstehcenlik ve çocukların bu tür zararlı yayınlara karşı korunmasına yönelik düzenlemeler yer almaktadır.

Veri iletim ağları ile zararlı yayınların yayılması ve paylaşılması eylemlerine uygulanan bir maddedir. Son zamanlarda çocuk pornografisi giderek artmakta ve Türkiye'de de bu suçlarla mücadele devam etmektedir.

Benzeri düzenlemeler karşılaştırmalı hukukta da yer almaktadır.

ABD'de çocukların Online yayınlardan korunması yasası[245] yine Amerika'da çocuk pornografisinin önlenmesi yasası[246] Fransa'da Ceza Kanununda, İngiltere'de Müstehcen Yayınlar yasasında ve Telekomünikasyon Yasasında yapılan değişikliklerle sanal âlemde yapılan pornografik içerikli yayınlar engellenmiştir.[247]

Avrupa Konseyi Siber suç sözleşmesinde çocuk pornografisine ilişkin materyalin elektronik olarak üretimi dağıtımı ve bu materyale sahip olunması fiilleri cezalandırılmaktadır. Burada dikkati çeken sözleşme ile yalnızca çocuk pornografisi ile küçüklerle ilgili müstehcen görüntülerin yasaklanmış olduğudur. Siber suç sözleşmesinde 9. Maddenin kapsamına çocuk erotizmi dahil edilmediğinden birçok ülkede bu konudaki yasal boşluktan yararlanılarak bu materyalin satılması suç sayılmamıştır.[248]

---

[245] Yaman Akdeniz, "Controlling illegal and harmful content on the internet", Crime and The internet, Edited by David S Wall, First Published 2001, by Routledge, London s. 113-141, bkz Şaban Cankat Taşkın, Bilişim Suçları, Beta Yayınevi, Bursa, 2008, s. 118-119.
[246] Russel Smith/ Peter Grobasky/ Gregor Urbas, Cyber Criminals on Trial First Published by Cambridge University Pres, Cambridge, 2004.
[247] Şaban Cankat Taşkın, a.g.e, s. 119.
[248] Murat Volkan Dülger "Avrupa Konseyi ve Avrupa Birliği Düzenlemelerinde Çocuk pornografisinin internet aracılığıyla yayılmasına karşı yapılan düzenlemeler, İBD, Cilt 78,

TCK'nin 226. maddesinin ikinci fıkrasında müstehcen görüntü yazı veya sözlerin basın ve yayın yoluyla yayınlanması ve 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 durumunda müstehcenlik suçu işlenir.

Tarafı olduğumuz 182 no'lu İLO sözleşmesinde ve 54/263 Sayılı Birleşmiş Milletler Kararıyla onaylanan çocukların satılması, Çocuk Fahişeliği ve Çocuk pornografisi hakkında seçmeli protokolüne göre ticari cinsel sömürü bağlamında çocuk fuhşu, çocuk pornografisi eylemlerinin taraf devletlerin iç hukuklarında yaptırıma bağlanması gerektiği belirtilmektedir.[249]

TCK'nın 226. maddesinde çocuklara ve yetişkinlere ilişkin müstehcenlik arasında bir ayrım yapılmadığından bizde de yasal bir boşluk bulunmaktadır. Bu da uygulamada sorunlara sebep olabilir.

TCK'de hangi eylemlerin pornografik hangi eylemlerin müstehcen sayıldığının sınırları çizilmemiştir. Maddenin ikinci fıkrasındaki müstehcenlik ifadesinin neyi kastettiği belirtilmemiş. Hâkime yasa koyucu burada takdir yetkisi vermiştir.

Yine 226. maddenin 4. fıkrasında doğal olmayan yoldan yapılan cinsel ilişki ifadesinde net somut bir açıklama yoktur. Her türlü yazı, görüntü ve ses olabilir yasa koyucu geniş yoruma açık bir alan bırakmıştır.

Yine dördüncü fıkrada suç teşkil eden görüntü, ses ve yazıların bulundurulması suç olarak düzenlenmiş. Devlet eliyle kişinin özel bilgisayarında bulundurduğu bu verilere müdahale edilebilecektir. Bu da

---

Sayı 2004/4, S. 1488-1493, Ayşe Aslıhan Erbaşı, Çocuk Pornografisi İBD, Cilt 81, Sayı 2007/4, S. 1623 vd.

[249] Şaban Cankat Taşkın, a.g.e, s. 121.

anayasanın 20. maddesine (özel yaşama müdahale) ve Anayasanın 13. maddesine (hakkın özüne aykırılık) teşkil edebilecektir.

Bu suçun mağduru çocuktur. Kasten işlenen bir suçtur. İçtima bakımından özellik göstermez. TCK'nin genel hükümleri uygulanır. Teşebbüs mümkündür. İştirak bakımından da TCK'nin genel hükümleri uygulanır.

YTCK'nun 226. maddesinde 2.3.4 fıkralarında suçun alenen işlenmesine ilişkin bir düzenleme yer almamıştır.

1.4. Türkiye'de Özel Kanunlarda Bilişim Suçları

1.4.1. 5846 Sayılı Fikir ve Sanat Eserleri Kanunu

5846 Sayılı Fikir ve Sanat Eserleri Kanunun 2. maddesinde 07.06.1995 tarih ve 4110 sayılı kanun ile değişiklik yapılmış, eser kavramının tanımı yapılırken bilgisayar programları da koruma kapsamına alınmıştır.

FSEK' in 2 md. İlim ve Edebiyat Eserleri şunlardır[250]. Herhangi bir şekilde dil ve yazı ile ifade olunan eserler ve her biçim altında ifade edilen bilgisayar programları ve bir sonraki aşamada program sonucu doğurması koşuluyla bunların hazırlık tasarımları"dır.

5846 sayılı FSEK' in 6. maddesine 4110 sayılı kanun ile eklenen (10) numaralı bend ile "Bir bilgisayar programının uyarlanması, düzenlenmesi veya her hangi bir değişim yapılması da fikir ve sanat eseri sayılmaktadır."

FSEK de ki bu değişiklikle 14.05.1995 tarihli Avrupa Konseyi direktifiyle FSEK arasında uyum sağlanmıştır.

FSEK'nin 71, 72 ve 73. maddelerinde yapılan değişiklikle fikri mülkiyet kapsamında olan eser kavramının içeriğine bilişim yazılımları ve bunarı oluşturan veriler dahil edilmiş böylece eser olarak kabul edilen bilişim

[250] Ali Karagülmez, a.g.e, s. 154.

yazılımları üzerindeki manevi ve mali hakların kasten ihlali halinde failin cezalandırılması öngörülmüştür[251].

FSEK'in 71. maddesinde manevi haklara tecavüz, 72. maddesinde mali haklara tecavüz, 73. maddesinde ise diğer suçlar başlıklı suç tipleri düzenlenmiştir.

A. Manevi, Mali ve Bağlantılı Haklara Tecavüz

FSEK'in 71. maddesinde eser sahibinin mali, manevi ve bağlantılı haklarına tecavüz fiilleri yaptırıma bağlanmıştır. Yaptırıma bağlanan eylemler şunlardır,

a) Alenileşmiş olsun veya olmasın, eser sahibi veya halefinin yazılı izni olmadan bir eseri umuma arz etmek veya yayınlamak

b) Sahip veya halefinin yazılı izni olmadan, bir esere veya çoğaltılmış nüshalarına ad koymak.

c) Başkasının eserini kendi eseri veya kendisinin eserini başkasının eseri olarak göstermek veya aynı kanunun 15. maddesinin ikinci fıkrasına aykırı hareket etmek.

d) 32,33,34,35,36,37,39 ve 40. maddelere göre alıntı (iktibas) yapılması, halinde kaynak göstermemek, yanlış yahut yetersiz veya aldatıcı kaynak göstermek.

e) Eser sahibinin yazılı izni olmaksızın bir eseri değiştirmektir.

23.01.2008 tarih ve 5278 sayılı kanunla (8 Şubat 2008 tarih ve 26871 sayılı Resmi Gazete ile) FSEK'in 71. maddesinde değişiklik yapılmadan önce eser sahibinin manevi haklarına tecavüz, maddi haklarına tecavüz 72. maddede düzenlenmekte ve eser sahibinin haklarına yönelik diğer suçlar hakkında ise 73. maddede uygulanmaktaydı. Yapılan değişiklikle her üç

[251] Murat Volkan Dülger, a.g.e, s. 112

maddede tanımlanan fiiller tek madde altında toplanmış 72. madde yeniden yazılmış ve 73. madde yürürlükten kaldırılmıştır[252].

Bu maddede korunan hukuki yarar, suç eser sahibinin malvarlığına yöneldiği için kişinin malvarlığı değerleridir[253]. Eser sahibinin manevi haklarına yönelik olan hukuka aykırı eylemler cezalandırılır. Bu suçta herkes fail olabilir. Suçun konusu ise her türlü eser çalışması ile ilgili bilgisayar yazılımlarındır. Takibi şikâyete bağlı bir suçtur.

FSEK md. 71'de manevi haklar devredilemez; eser sahibi hayatta olduğu sürece eserin sahibi mağdur sayılacak ancak eser sahibi ölürse mirasçıları manevi hakka sahip olamaz. FSEK'in 19. maddesi uyarınca yasadan kaynaklanan haklara sahip olurlar. Bu haklar saldırıya uğrarsa FSEK 71/1, 2 ve 6. fıkralarda ki suçlar oluşur. Bu nedenle eser sahibi ölmüş dahi olsa yetmiş yıllık bir koruma süresi vardır. Bu süre içinde eserin manevi haklarına herhangi bir saldırı olursa yasada belirtilen mirasçılar mağdur sayılır[254].

Doktrinde web sitelerinin eser olup olmadığı tartışmalıdır. Web siteleri başka bir ad altında çalınırsa web sitesinin eser özeliği taşıyıp taşımamasına ve sahibinin özelliklerini taşıyıp taşımamasına kanun maddesindeki hükümlere girip girmediğine bakmak gerekir.

FSEK'in 71. maddesinde suçun maddi unsurlarından birincisi yazılım sahibinin veya halefinin yazılı izni olmadan bir yazılımı işlemek çoğaltmak, değiştirmek, her türlü görüntü ileten araçla yazılımı umuma arz etmek yayımlamak hukuka aykırı olarak işlenen ya da çoğaltılan bir yazılımı satışa arz etmek satmak kiralamak değişik şekillerde yaymak ithal veya ihraç etmek kişisel kullanım dışında elde bulundurmak suçtur.

---

[252] Şaban Cankat Taşkın, a.g.e, s. 133.
[253] Murat Volkan Dülger, a.g.e, s. 294.
[254] Şaban Cankat Taşkın, a.g.e, s. 134.

Suçun diğer maddi unsuru ise başkasına ait eseri kendisine aitmiş gibi göstermek ve bu şekilde adlandırmaktır.

Diğer ihlal türlerine bakarsak bir eserin içeriğini hak sahibinin izni olmadan kamuya açıklamak, bir eserle ilgili yetersiz aldatıcı kaynak göstermek verilebilir.

Bu suçlar bilişim yoluyla işlenebilir. Bu maddede belirtilen eylemlerin gerçekleşmesi ile suç oluşur. Zararın oluşması gerekmez. Neticesi harekete bitişik bir suçtur. Bu suç açısından teşebbüs mümkün görünmemektedir. Tehlike suçudur.

FSEK md. 71'deki suçlarda "rıza" hukuka uygunluk nedeni olarak kabul edilecektir. FSEK md. 71/4 fıkrasına göre rızanın yazılı olması ve filin işlenmesinden önce verilmesi gerekir[255].

FSEK'in 38. maddesinin 2. fıkrasına göre yazılımı hukuka uygun olarak iktisap eden kimsenin bu yazılımı çoğaltma işleme ve yazılımdaki hataları düzeltme hakkı bulunmaktadır[256].

8 Şubat 2008 tarihinde 5728 sayılı yasa ile FSEK'in 74. maddesi kaldırılmıştır. Eskiden FSEK'in 71, 72 ve 73. maddelerindeki suçu işleyen tüzel kişinin temsilcisi bu suçu işletmeye ilişkin faaliyetleri yerine getirirken işlerse tüzel kişinin sahibi suçun işlenmesine engel olabilecek engel olmamışsa o da suçu işleyen gibi sorumluydu. Bu durum cezaların şahsiliği ilkesiyle bağdaşmamaktadır.

Bu suçlara iştirakte 5237 sayılı TCK'nın iştirake ilişkin genel hükümleri uygulanır. Fail aynı suçu işleme kastıyla değişik zamanlarda yazılımı birden çok kez çoğaltırsa zincirleme suç hükümleri uygulanır.

FSEK'in ikinci bendindeki başkasına ait bir esere kendi eseri olarak ad koymak fiillinin eseri dağıtmak ya da yayımlamak suretiyle işlenmesi

[255] Ali Karagülmez, a.g.e, s. 155.
[256] Murat Volkan Dülger, a.g.e, s. 303.

durumunda artık fail hakkında seçenek yaptırımı uygulanmaz. Faile 6 aydan 5 yıla kadar hapis cezası verilir. 71. maddedeki diğer suçlar bakımından da 71/1-b.4, b.5 deki suçlar bakımından da seçenek yatırımı öngörülmemiş hürriyeti bağlayıcı ceza verilir, 71. maddedeki 71/1-b.1, b.2, b.3, b.6 maddelerindeki suçlar bakımından ise hürriyeti bağlayıcı ceza öngörülmüştür[257].

FSEK 71/son'da etkin pişmanlık öngörülmüş, hukuka aykırı olarak çoğaltılmış, dağıtılmış, yayınlanmış bir eseri satan veya satın alan kişi kovuşturma aşaması başlamadan eserleri kimden temin ettiğini belirtirse faile ceza verilmeyebilir. Ya da cezada belli oranda indirim yapılır.

B. Koruyucu Programları Etkisiz Kılma

23.01.2008 tarihinde 5728 sayılı yasa ile FSEK de yapılan değişiklikle FSEK md. 72'deki koruyucu programları etkisiz kılmak amacıyla işlenen fiiller yaptırıma bağlanmıştır.

72. maddede de yazılımların güvenliği korunur. Bu maddedeki suç özel kastla işlenir. Failin bilgisayar programlarını hukuka aykırı olarak kullanmak veya çoğaltmak amacıyla program ya da teknik donanım üretme yönün de özel bir kastı bulunur.

Fail herkes olabilir, mağduru da eser sahibidir. Tehlike suçudur.

72. maddede Hak sahibinin izni olmaksızın bir eserin herhangi bir şekilde işlenmesi, çoğaltılması, yayılması bir eserin nüshalarının yasal veya yasal olmayan yollardan ülkeye sokulması ve her ne şekilde olursa olsun ticaret konusu yapılması veya bir eserin topluma açık yerlerde gösterilmesi veya temsil edilmesi bu gösterimin düzenlenmesi veya dijital ortamda dahil olmak üzere her nevi işaret, ses veya görüntü iletimine yarayan araçlarla yayılması veya yayımına aracılık edilmesini yaptırıma bağlanmıştır.

[257] Şaban Cankat Taşkın, a.g.e, s. 138.

Bu suç seçimlik hareketli bir suçtur. Maddi unsurda belirtilen hareketlerin herhangi birinin gerçekleşmesiyle suç oluşur. İcrai hareketle işlendiğinden teşebbüs mümkündür. Bu suçu işleyenler altı aydan iki yıla kadar hapis cezası ile cezalandırılır.

1.4.2. 5070 sayılı Elektronik İmza Kanununda Düzenlenen Bilişim Suçları

5070 sayılı elektronik İmza Kanunu TBMM tarafından 15.01.2004 tarihinde kabul edilip yayınlandıktan 6 ay sonra yürürlüğe girmiştir.

EİK'nu Avrupa Birliğinin direktifi doğrultusunda hazırlanıp güvenli elektronik imza, güvenli elektronik imza doğrulama araçları, bu imzanın hukuk alanında doğurduğu sonuçlar elektronik sertifika hizmet sağlayıcıları gibi elektronik imzayla ilgili araçlar ve hizmet sağlayıcılarının hukuki yetki ve sorumlulukları düzenlenmiştir[258].

Avrupa Birliği tarafından elektronik ticaretin işlevselliğini arttırmak ve elektronik imzanın güvenirliği konusundaki standartları belirlemek bakımından 30 Kasım 1999 tarih 1999/93/EC sayılı "Elektronik İmza Yönergesi" kabul edilmiştir[259].

EİK'nun 16. maddesinde "elektronik imza oluşturma verilerin izinsiz kullanımı suçu 17. maddesinde de "elektronik sertifikalarda sahtekârlık suçu" düzenlenmiştir.

Yasanın 3. maddesinde elektronik imza, başka bir elektronik veriye eklenen veya elektronik veriyle mantıksal bağlantısı bulunan ve kimlik doğrulama amacıyla kullanılan elektronik veri olarak tanımlanmıştır.

Elektronik veri ise, 3. maddesinde de "elektronik, optik veya benzeri yollarla üretilen taşınan veya saklanan kayıtlar şeklinde tanımlanmıştır.

---

[258] İsmail Ergün, a.g.e, s. 77.
[259] İpek Sağlam, Elektronik Sözleşmeler, Legal Yayınevi, İstanbul, 2007, s. 54.

EİK'nun 5. maddesinde klasik imzanın yararlandığı hukuki güvenceden sayısal imzanın yararlanması amaçlanmaktadır.

Yasanın 16. maddesinde "imza oluşturma verilerinin izinsiz kullanımı suçu" tanımlanmıştır. 16. maddede de korunan hukuki değer elektronik imzanın doğruluğu ve buna duyulması gereken güven duygusu idi. Kanunda öngörülen seçimlik hareketlerden birinin yapılması ile suç tamamlanır.

5728 sayılı kanunla yapılan değişiklikten önce maddenin üçüncü fıkrasında bu maddedeki suçlar nedeniyle oluşan zarar ayrıca tazmin ettirilirdi. Değişiklikle zararla ilgili kısım kaldırılmıştır.

Suçun oluşumu için failde elektronik imzayı oluşturmaya yönelik kasıt bulunmalıdır. Suç işlemeden önce verilen ilgilinin rızası hukuka uygunluk nedenidir.

Bu suçta korunan kamu güveni ve elektronik belgelerin doğruluğuna olan inançtır.

Fail ve mağdur herkes olabilir. Ancak 16. maddenin 2. fıkrasına göre suçun elektronik sertifika hizmet sağlayıcısı tarafından işlenmesi durumunda cezada yarı oranında artırıma gitmek gerekecektir[260].

Neticesi harekete bitişik suçtur. Bu suça teşebbüs mümkün değildir. EİK'nu md. 16'daki suçun TCK 243/1'deki bilişim sisteminin bütününe veya bir kısmına girme suçuyla içtima durumunda bulunursa o zaman EİK'nun dan ceza verilir. Çünkü TCK'ya göre daha özeldir.

Bu suçta fail hakkında hem hürriyeti bağlayıcı ceza hem de adli para cezası öngörülmüştür.

EİK'nun 17. maddesinin tamamen veya kısmen sahte elektronik imzalar oluşturanlar veya geçerli olarak oluşturulan elektronik sertifikalar, taklit veya tahrif edenler ile yetkisi olmadan elektronik sertifikaları, bilerek

[260] Ali Karagülmez, a.g.e, s. 161

kullananlar, fiilleri başka bir suç oluştursa bile ayrıca iki yıldan beş yıla kadar hapis veya bir milyar liradan aşağı olmamak üzere ağır para cezasıyla cezalandırılır.

Elektronik sertifika suçu hizmet sağlayıcısı tarafından işlenirse bu cezalar yarısına kadar arttırılır.

Hizmet sağlayıcısı EİK'nun 8. maddesinde elektronik sertifika zaman dalgası ve elektronik imzalarla ilgili hizmetleri sağlayan kamu kurum ve kuruluşları ile gerçek veya özel hukuk tüzel kişileridir, şeklinde tanımlanmıştır.

EİK'nun 3. maddesinin 1. bendinde imza doğrulama verisini ve kimlik bilgilerini birbirine bağlayan elektronik kayıt olarak tanımlanmıştır. Suçta korunan hukuki yarar elektronik sertifikadaki sahtekârlığın önlenmesidir.

5728 sayılı yasa ile değişiklik yapılmadan önce bu maddenin üçüncü fıkrasında da zarar ödettiriliyordu. Değişiklikten sonra kalktı. Bu suçun faili ve mağduru herkes olabilir. Suçun oluşumu için genel kast yeterlidir. Neticesi harekete bitişik bir suçtur.

İçtima bakımından elektronik sertifikada sahtecilik suçunun diğer suçlarla içtiması durumunda EİK'nun da ki 17 md. Uygulanır. Özel yasadır. TCK'ya göre, faile hem para hem hürriyeti bağlayıcı ceza verilir. Hürriyeti bağlayıcı cezanın alt sınırı iki, üst sınırı ise beş yıldır. Adli para cezasının alt sınırı da 100 gündür.

SONUÇ

Günümüzde bilişim sistemleri insan hayatını bir yandan kolaylaştırırken bir yandan da sorunları beraberinde getirmektedir. Hayatın her alanında olduğu gibi hukuk alanında da bilişim suçları ciddi sorunlar doğurmaktadır. Dünyada birçok devlet gibi ülkemizde bilişim suçlarına mevzuatın da yer verip karşılaşılan sorunlara göre bir takım düzenlemelere gitmiştir. Ceza Hukuku başta olmak üzere çeşitli hukuk mevzuatında düzenleme yapılmıştır.

Ülkemiz bilişim suçlarındaki düzenleme bakımından birçok ülkeden öndedir, YTCK da ki düzenlemeler Avrupa Konseyi Siber Suç sözleşmesinin hükümlerini büyük oranda karşılamaktadır.

Bilişim suçları ile ilgili ülkemizde ilk ayrıntılı yapılan düzenleme de Türkiye Avrupa Topluluğu tavsiye kararlarını dikkate alarak 06.06.1991 tarihinde 3756 sayılı kanunla Türk Ceza Yasasına 525/b-2 maddesinde bilgileri otomatik işleme tutmuş bir sistemin kullanılarak menfaat temin etmeyle ilgili her türlü eylem suç olarak kabul edilmiştir. Madde metninde geçen “her türlü eylem” deyimi geniş bir düzenleme olduğu için TCK’nın kıyas yasağı ilkesine aykırıdır.

Türk yasa koyucu 5237 sayılı Yeni TCK’da Bilişim Alanında Suçlar Başlığı altında 243, 244 ve 245. maddeleri düzenlemiştir. Bu maddelerde 765 sayılı TCK da eleştirilen kısımlar bir şeklide giderilmeye çalışılmış suçun maddi unsurları tek tek tanımlanmıştır.

TCK’nın 244. maddesinin 1 ve 2. fıkrasında düzenlenen sisteme ve veriye müdahale suçu klasik mala zarar verme suçunun bilişim sistemine uygulanabilir olup olmadığının tartışılmasının bir sonucu olarak düzenlenmiştir. Mala zara verme suçları şikâyete tabi suçlardır. Ancak 244. maddedeki suç şikâyete tabi değildir. Resen kovuşturulmaktadır.

Kanun koyucu 244. maddeyi mala zarar verme suçunun özel hali olarak düzenleyerek ağırlaştırıcı sebep saymıştır.

Yine 244. maddenin son fıkrasında bir kişiye karşı hileli hareket düzenlemeden haksız yarar sağlanması düzenlenmiş maddede sadece haksız yarar sağlanmasının düzenlenmesi bu suçun dolandırıcılık suçuyla da karıştırılmasına sebebiyet verebilir. Burada fail sistemi bozuyor işleyişe ve verilere müdahale ediyor. Dolandırıcılık suçundaki gibi hileli hareketle suçun oluşmasına sebebiyet vermiyor.

YTCK'yla 245. maddenin düzenlenmesiyle beraber banka ve kredi kartlarının ele geçirilmesi usulüne kanun koyucu son noktayı koymuştur. 3756 sayılı kanunla değişik 765 sayılı TCK zamanında kanun koyucu banka ve kredi kartlarının ele geçirilmesi konusunda bir düzenleme yapmadığından Yargıtay'ın 6. ve 11. Hukuk Daireleri de bu konuda farklı kararlar vermekteydi. 5237 sayılı kanunla kanun koyucu her ne suretle olursa olsun ibaresini kanun metnine koyarak kredi kartlarının ele geçiriliş tarzının suçun vasfını etkilemeyeceğine dair düzenleme yapmıştır. 245. maddede önemli olan banka ve kredi kartının haksız olarak kişilerin eline geçmesidir.

TCK 244/4 maddesinde failin yapmış olduğu hukuka aykırı eylem TCK 244. maddenin 1, 2, 3 fıkralarına girmiyorsa TCK 244/4 maddesinden ceza verilir denmektedir. TCK 244. 1, 2, 3 fıkralarında sayılan eylemler yoluyla kişinin kendisinin veya bir başkasına haksız çıkar sağlamasının başka bir suç oluşturmaması halinde TCK 244/son maddesinin uygulanacağını kanun koyucu açıkça düzenlemiştir.

TCK 243/3 maddesinde birinci fıkradaki eylemin taksirle işlenmesini yaptırıma bağlamıştır. Bura da bilişim sistemine hukuka aykırı olarak girmek ve orada kalmak gerekir. Bir kişinin taksirli eylemden sorumlu tutulabilmesi için suç işlediği konuda en azından biraz bilgi sahibi olması; kendisinden beklenen dikkat ve özeni göstermemesi yaptığı eylemin önündeki sonucunu ön görebilmesi gerekir.

TCK'nın 132. maddesinde haberleşmenin gizliliğini ihlal, TCK 134'de de özel hayatın gizliliğinin ihlal edilmesi cezayi yaptırıma bağlanmıştır.

TCK 135'te hukuka aykırı olarak kişisel bilgilerin kaydedilmesi suçu düzenlenmiş, ancak TCK'da kişisel bilginin tanımı yapılmamıştır. Kişisel bilginin yok edilmesi de ilk defa TCK'da suç sayılmıştır. Kişisel veriler hakkında ülkemizde şu an bir kanun tasarısı hazırlanmış, henüz yürürlüğe girmemiştir.

Bilişim güvenliğinin artırılabilmesi ve yaygınlaştırılabilmesi için Bilişim suçları ile mücadele edecek, özel eğitimden geçecek personelin yetiştirilmesi ve teknik personel eksikliğinin de giderilmesi gerekir.

KAYNAKÇA

Akbulut, Berrin (1999), Türk Ceza Hukukunda Bilişim Suçları Yayımlanmamış Doktora Tezi, Selçuk Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı Ceza ve Ceza Usul Hukuku Bilim Dalı, Konya, 1999.

Akbulut, Berrin (2000), ‘’Bilişim Suçları’’, Selçuk Üniversitesi Hukuk Fakültesi Dergisi, Milenyum Armağanı, Sayı: 1-2, Cilt: 8

Akdeniz Yaman “Controlling illegal and harmful content on the internet”, Crime and The internet, Edited by David S Wall, First Published 2001, by Routledge, London S. 113-114.

Akıncı, Hatice/ Alıç A Emre/ Er, Cüneyd, (2004), “Türk Ceza Kanunu ve Bilişim Suçları” İnternet ve Hukuk, İstanbul Bilgi Üniversitesi Yayınları, İstanbul.2004

Altaylı Behçet (1988) ‘’Bilgisayarlar ve Basic ile Programlama’’, Filiz Kitabevi, İstanbul, 1988.

Aydın Emin (1992) ‘’Bilişim Suçları ve Hukukuna Giriş ‘’ Doruk Yayınevi, Ankara, 1992.

Beceni Yasin/ Uçkan Özgür, (2004), “Bilişim iletişim Teknolojileri ve Ceza Hukuku” İnternet ve Hukuk, İstanbul Bilgi Üniversitesi Yayınları. İstanbul 2004.

Bilgisayar Ansiklopedisi, (1991) Milliyet Yayınları, İstanbul.

Bozkurt, Mazlum (2003) ‘’Şifreli Yayınlar ve Bilişim Sistemleri, Türkiye Ortadoğu Amme İdaresi Enstitüsü Adalet Yönetimi Yüksek Lisans Programı, Ankara, 2003.

Çeken, Hüseyin (2008) ‘’Amerika Birleşik Devletlerinde Siber Suçlar’’ http://www. jura.unisb.de/turkish/HÇeken html.

Değirmenci, Olgun (2002) “Bilişim Suçları Yayımlanmamış Yüksek Lisans Tezi” , Marmara Üniversite Sosyal Bilimler Enstitüsü, İstanbul, 2002.

Dijital Platform İletişim Hizmetleri A.Ş’nin Sunduğu Rapor, İletişim Şurası Notları, Ankara, 20-21 Şubat 2003.

Doğan, Aydın Emin (1992) ‘’ Bilişim suçları ve Hukukuna Giriş’’ Doruk Yayınevi, Ankara 1992.

Doğan, Koray (2008) ‘’Bilişim Suçları ve Yeni Türk Ceza Kanunu, http// adlibilisim.iyte.edu.tr./AdliBilisim 2005 web/file/koraydogan.pdf.

Dönmezer, Sulhi (2001) ‘’Ceza Hukuku Özel Kısım-Kişilere ve Mala Karşı Cürümler’’ Beta Yayınevi 16. Baskı, İstanbul, 2001.

Dülger, Murat Volkan (2004) ‘’ Bilişim Suçları’’ Seçkin Yayınevi, Ankara, 2004.

Dülger, Murat Volkan (2004) “Avrupa Konseyi ve Avrupa Birliği Düzenlemelerinde Çocuk Pornografisinin İnternet Aracılığıyla Yayılmasına Karşı Yapılan Düzenlemeler ‘’ İBD, Cilt 78, Sayı 2004/4.

Erbaşı, Ayşe Aslıhan (2007) ‘’ Çocuk Pornografisi ‘’ İBD, Cilt 81, Sayı 2007/4,

Emniyet Genel Müdürlüğü Bilişim Suçları Çalışma Güvenliği Raporu, http://www.bilisimsurasi.org.tr/dosyalar/10.doc,

Ekinci, Mustafa/ Esen Sinan (2005) ‘’ Anlatımlı ve Gerekçeli Yeni Türk Ceza Kanununda Yer Alan Hırsızlık, Yağma, Güveni Kötüye Kullanma, Dolandırıcılık, Hileli ve Taksirli iflas, Karşılıksız Yararlanma, Belgelerde Sahtecilik ve Bilişim Alanında Suçlar’’ Adalet Yayınevi, Ankara, 2005.

Eralp, Özgür (2005) ‘’ Bilişim Suçlamasına Giden Yol –IP ‘’ IP’’,http://www.turkhukuksitesi.com.

Erdağ, Ali İhsan (2005) “5237 Sayılı Yeni Türk Ceza Kanununda Bilişim Suçları” www.adalet.gov.tr.

Ergün, İsmail (2008) ‘’Siber Suçların Cezalandırılması ve Türkiye de Durum ‘’ Adalet Yayınevi, Ankara, 2008.

Erman, R. Barış (2001) ‘’Alman Hukukunda İnternetten Kaynaklanan Ceza Sorumluluğu ‘’ İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, Sayı: 1-2 ,Cilt: 59, İstanbul, 2001.

Ersoy, Yüksel (1994) “Genel Hukuki Koruma Çerçevesinde Bilişim Suçları” Ankara Üniversitesi Siyasal Bilimler Fakültesi Dergisi, Cilt: 49, Sayı: 3-4, 1994.

Helvacıoğlu Aslı Deniz (2004) “Avrupa Konseyi Siber Suç Sözleşmesi Temel Hükümlerin İncelenmesi ’’ İnternet ve Hukuk İstanbul Bilgi Üniversitesi Yayınları, İstanbul, 2004.

İçel, Kayıhan (2001) “Avrupa Konseyi Siber Suç Sözleşmesi Bağlamında Avrupa Siber Suç politikasının Ana İlkeleri ” İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, C. LIX, S. 1-2, İstanbul, 2001.

İçel, Kayıhan (2001) ‘’Kitle Haberleşme Hukuku’’ Basın, Radyo- Televizyon, Sinema, İnternet, Beta Yayınevi, İstanbul, 2001.

İnternet ve Hukuk Platformu, Ankara Barosu, Avrupa Konseyi Siber Suçlar Sözleşmesi Taslağı, Ankara, 2007.

Kangal, Zeynel T. “Fransa’da İnternet Yoluyla İşlenen Suçlardan Doğan Ceza Sorumluluğu” İstanbul Üniversitesi Hukuk Fakültesi Mecmuası C LIX, S. 1-2, 2001.

Karagülmez, Dr. Ali (2005) ‘’Bilişim Suçları ve Soruşturma - Kavuşturma Evreleri’’ Seçkin Yayınevi, Ankara, 2005

Kardaş, Ümit (2003) “Bilişim Dünyası ve Hukuk”, Karizma Dergisi Sayı:13.

Ketizmen, Muammer (2008) ‘’Türk Ceza Hukukunda Bilişim Suçları’’ Adalet Yayınevi, Ankara, 2008

Kurt, Levent (2005) ‘’ Açıklamalı- İçtihatlı Tüm Yönleriyle Bilişim Suçlamaları ve Türk Ceza Kanundaki Uygulaması ‘’ Seçkin Yayınevi, Ankara 2005.

Mahmutoğlu, Fatih Selami, (2001) ‘’ Karşılaştırmalı Hukuk Bakımından İnternet Sujelerinin Ceza Sorumluluğu’’ İ.Ü.H.F.M , cilt LIX, Sayı:1-2, İstanbul 2001.

Mahmutoğlu, Fatih Selami, (2002) “Bankacılık Suçları Bağlamında Çıkar Amaçlı Suç Örgütü”, Avrupa Birliğine Uyum Süreci Bağlamında Organize Suçlulukla Mücadele, Panel, 5 Ekim 2001, Bildiriler ve Tartışmalar, Yönetici Kayıhan İçel, İstanbul, 2002

Malkoç, İsmail/ Üler, Mahmut (tarih belirtilmemiştir) ‘’Uygulamada Türk Ceza Kanunu Özel Hükümler –IV ‘’, Adil Yayınevi, Ankara.

Memiş, Tekin (2008) ‘’Hukuki Açıdan Kitlere E-posta Gönderilmesi’’ http://bilisimsurasi.org/dosyalar/14.doc.

Meran, Necati (2008) ‘’ Yeni Türk Ceza Kanunun da Sahtecilik Malvarlığı, Bilişim Suçlarıyla Ekonomi ve Ticaret Alanın da Suçlar ‘’2. Baskı Seçkin Yayınevi, Ankara, 2008.

Noyan, Erdal (2005) ‘’Hırsızlık ve Yağma Suçları ‘’ Bilge Yayınevi, Ankara 2005.

Nuhoğlu, Ayşe (2002) ‘’ Ceza Hukukunda Kredi Kartlarının Kötüye Kullanılması ‘’ Analiz Basım Yayınevi, İstanbul 2002.

Önder, Ayhan (1994) ‘’ Şahıslara ve Mala Karşı Cürümler ve Bilişim Alanındaki Suçlar ” Filiz Kitabevi, İstanbul, 1994.

Özel, Cevat (2001) ‘’ Bilişim Suçları İle İletişim Faaliyetleri Yönünden Türk Ceza Kanunu Tasarısı ‘’ İ.B.D, Yıl: 2001, Sayı: 7-8-9.

Özel, Cevat (2004) '' Bilişim-İnternet Suçları Üzerine Bir İnceleme İnternet Hukuku '' www.law.ankara.edu.tr/yazı.

Parlar Ali/ Muzaffer Hatipoğlu (2008) '' Türk Ceza Kanunu Yorumu'' 2. baskı Cilt: 4, Seçkin Yayınevi, Ankara 2008.

Peşkirin, Hülya ve diğerleri '' Türkiye Bilişim Şurası Hukuk Çalışma Grubu Raporu '' Türkiye Bilişim Şurası, Ankara, 10-12 Mayıs 2002.

Sağlam, İpek (2007) '' Elektronik Sözleşmeler '' Legal Yayınevi, İstanbul, 2007.

SchJolberg, Stein "The Legal Framework-Unauthorized Access To Computer Systems, penal Legislation in 44 Countries", (Updated April 7, 2003), http://www.mosstingrett.no/info/legal.html.

Schreibaver, Marcus, (2002), Strafrechtliche Verantwortliclikeit für Delikte im. İnternet, Handbucuh Zum internetrecht 2. Auflage, Düsseldorf.

Smith, Russel/Grobasky, Peter/Urbas, Gregor; Cyber Criminals on Trial First Published by Cambridge University Pres, Cambridge, 2004.

Sınar, Hasan (2001) '' İnternet ve Ceza Hukuku '' Beta Yayınevi, İstanbul, 2001.

Sokullu-Akıncı, Füsun (2001) "Avrupa Konseyi Siber Suç Sözleşmesinde Yer Alan Maddi Ceza Hukukuna İlişkin Düzenlemeler ve Özellikle İnternette Çocuk Pornografisi" İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, C LIX, S: 1-2. İstanbul, 2001.

Soyaslan, Doğan (2005) ''Ceza Hukuku Genel Hükümler Güncelleştirilmiş 3. Baskı '' Yetkin Yayınevi, Ankara, 2005.

Şehitoğlu, Yzb. Onur (2005) '' Bilgisayar ve Ağ Üzerinde İşlenen Siber Suçlarla Müdahalenin Hukuksal ve Güvenlik Boyutu İsimli Yayınlanmamış Yüksel Lisans Tezi '' Kara Harp Okulu Savunma Bilimleri Enstitüsü Güvenlik Bilimleri Ana Bilim Dalı, Ankara 2005.

Taşkın, Şaban Cankat (2008) '' Bilişim Suçları '' Beta Yayınevi, Bursa, 2008.

Tavukçuoğlu, Cengiz (2004) ''Bilişim Terimleri Sözlüğü '' Asil Yayın Dağıtım, Ankara 2004.

Tezcan, Durmuş (2002) '' İnternet Karşısında Özel Hayatın Korunması ve Adli Yardımlaşma Uluslararası İnternet Hukuku Sempozyomu 21-22 Mayıs 2001, Dokuz Eylül Üniversitesi Yayını, İzmir, 2002.

Tezcan, Durmuş/ Erdem Mustafa Ruhan/ Önok, Murat (2007) '' Teorik ve Pratik Ceza Özel Hukuku 5560 Sayılı Kanuna Göre Güncellenmiş 5. Baskı '' Seçkin Yayınevi, Ankara, 2007.

Topaloğlu, Mustafa (2005) '' Bilişim Hukuku ''Karahan Yayınevi, Adana, 2005.

Türk Dil Kurumu "Güncel Türkçe Sözlük" www. tdk.gov.tr

Toroslu, Nevzat/ Metin Feyzioğlu (2009) ''Türk Ceza Kanunu –Ceza Muhakemesi Kanunu ve İlgili Kanunlar '' Savaş Yayınevi, Ankara, 2009

''Türk Ceza Kanunu ''Seçkin Yayınevi, Ankara, 2005.

Türkçe sözlük, http://www.tdk.gov.tr

Ünver, Yener (2001) '' Türk Ceza Kanununun ve Ceza Kanunu Tasarısının İnternet Açısından Değerlendirilmesi "İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, Sayı; 1-2, İstanbul,2001.

Yazıcıoğlu , R.Yılmaz (1997) ‘’ Bilgisayar Suçlar Kriminolojik Sosyolojik ve Hukuki Boyutları ile ‘’ Alfa yayınevi, İstanbul, 1997.

Yazıcıoğlu R. Yılmaz (2004) “Bilişim Suçları Konusunda 2001 Türk Ceza Kanunu Tasarısının Değerlendirilmesi” Hukuk ve Adalet: Eleştirel Hukuk Dergisi, Y:1, S.1, İstanbul 2004.

TCK 243. Madde İle İlgili Yargıtay Kararları

Sanık Dilek Topbaşlı'nın bir süre çalışıp ayrıldığı, katılan Aktif Bilgisayar Hizmetleri ve Danışmanlık Ltd. Şti. tarafından hazırlanan ve patenti alınan POLDY isimli programı ele geçirerek QSOFT ismi altında diğer sanık Kemal Çatmakaş ile pazarlamaya çalıştığı ileri sürülerek. Bursa 6. Asliye Hukuk Mahkemesince 27.6.2002 günü yapılan tespit sırasında POLDY isimli programın PBL ve PBD isimli uzantılarının sanık Kemal'e ait şirketin terminallerinde bulunduğu belirlenmiş olması karşısında katılan şirkete ait POLDY isimli program ile sanıkların pazarlamaya çalıştıkları iddia edilen QSOFT isimli programın uzman bilirkişilere karşılaştırmaları yapılarak, QSOFT isimli programın, katılanın şirketine ait programın taklidi olup olmadığı, PBL ve PBD isimli uzantıların kullanılıp kullanılmadığı, her iki programın ne kadar sürede geliştirilebileceği belirlenmeden ve taklit edildiği iddia edilen programın internetten herkes tarafından indirilmesinin olanaklı olup olmadığı araştırılıp saptanmadan, eksik soruşturma ile hüküm kurulması, **(6. CD., 20.04.2006,7493-4024)**

---•---

Yakınana ait internet hattına 18.6.2000-5.12.2000 tarihleri arasında dışarıdan başkaları tarafından toplam 329 defa bağlantı yapılarak girilip görüşme yapıldığı, bunlardan sadece 48 adetinin sanıkların babası Muharrem İşçi adına kayıtlı ev telefonundan 18.6.2000-30.9.2000 tarihleri arasında gerçekleştirildiği, sanıklardan Türker İşçi'nin 29.7.2000-16.12.2000 tarihleri arasında yurtdışında olduğu, sanık Mustafa Alper İşçi'nin de Aralık 1999-Nisan 2001 tarihleri arasında askerde olduğu 3 veya 4 haftada bir hafta sonları babasının evine geldiği. her iki sanığın evde olmadıkları günlerde de babaları üzerine kayıtlı telefon ile yakınanın internet hattına bağlantı yapıldığının anlaşılması ve bilirkişi Özgür Tamer tarafından düzenlenen 12.3.2003 tarihli raporda **da** "bağlanılan telefonun başka bir numara olarak gösterilmesinin mümkün olduğunun" belirtilmesi karşısında; sanıkların yüklenen suçu işlediklerine ilişkin her türlü kuşkudan uzak, hukuken elverişli,

yeterli, kesin ve inandırıcı kanıt bulunmadığı gözetilmeden, yazılı şekilde mahkumiyetlerine karar verilmesi, **(6. CD., 16.03.2006, 5464-2574)**

16.7.2002 havale tarihli bilirkişi raporunda, sanığın kullandığı abone şifresi ile yakınana ait web sitesine zarar veren olarak görünen IP'nın 212.253.230.172 olup Superonline firmasına ait bulunduğu, bu IP'nın kurumsal müşterisi olan bilgisayar şirketine verildiği. IP'nın statik, telefon numarası bilgisinin bulunmadığı belirtilmiş, sanık savunmanın temyiz dilekçesine ekli sunduğu 7.11.2002 tarihli şişli cumhuriyet başsavcılığına hitaben Superonline firması tarafından yazılan yazıda fastcam şirketinin internete dial-up yöntemi ile bağlandığı ve telefon numarasının bildirilmesi karşısında: bu çelişkinin giderilmesi için bilirkişiden bağlantının statik olduğuna ilişkin saptamanın gerekçelerinin açıklattırılması için ek rapor aldırıp, Superonline firmasına yazı yazılarak katılan kuruma ait web şirketine zarar veren İP bağlantısının statik mi, dinamik mi **(dial-up telefon bağlantısı)** olup olmadığını, dinamik ise bağlantı sırasında kullanılan telefon numarası ile abonelik bilgilerinin belirlenmesinden sonra, telefon numarasının kime ait olduğu ve adresi Türk Telekom kurumundan sorularak, sanıktan başka kişi olması halinde, bu kişi dinlenerek sanıkla bağlantısı araştırılıp, sonucuna göre sanığın hukuki durumunun takdiri gerektiren eksik kovuşturma ile yazılı şekilde hüküm kurulması, **(6. CD., 13.09.2005,16070-7439)**

TCK 244. Madde İle İlgili Yargıtay Kararları

I- Sanıkların, yakalanamadıkları için sorguları yapılamayan ve bu nedenle haklarındaki kamu davalarının tefrikine karar verilen diğer sanıklar İlkay Gobi ve Musa Hayta ile önceden bir araya gelerek haksız yarar sağlamak için sayısı belirsiz suçları işlemek amacıyla tam bir işbirliği ve eylemli paylaşım anlayışı içinde süreklilik taşıyan biçimde örgütlenip faaliyette bulunduklarına ilişkin delillerin nelerden ibaret olduğu karar yerinde açıklanıp gösterilmeden, suç işlemek amacıyla kurulmuş Örgüte üye olmak suçundan yazılı şekilde mahkûmiyetlerine hükmolunması.

II- Bilişim ve dolandırıcılık suçlarından kurulan hükümlere yönelik temyiz itirazlarına gelince:

1- Dolandırıcılık suçunda unsur olan hilenin gerçek kişiye yönelmesi ve hataya düşürülerek kendi veya bir başkasının mal varlığı aleyhine, sanık veya bir başkasının lehine bir işlemde bulunmaya yöneltilmesi ve bu işlem sonucunda sanığın kendine veya başkalarının yararına haksız bir menfaat sağlanması gerekir. Somut olayda ise; katılan İshak Kutluay adına Akbank Van Şubesinde açılan hesaba internet üzerinden girilerek, mevduatında bulunan paraların, fikir ve eylem birliği içerisinde hareket eden sanıklar tarafından aynı tarihte Aydın ilinde sahte isimlerle açtırılmış üç ayrı banka hesabına havale edilerek, yine aynı tarihte bankalardan çekilmesinden ibaret eylemlerinin bir bütün halinde hüküm tarihinde yürürlükte bulunan 765 sayılı TCK'nın 525/b-2. (5237 Sayılı Yasanın 244/4.) maddesinde öngörülen ve teselsül eden bilgileri otomatik İşleme tabi tutmuş bir sistemi kullanarak kendisi veya başkası lehine hukuka aykırı yarar sağlamak suçunu oluşturduğu gözetilmeden suçun nitelendirilmesinde yanılgıya düşülerek dolandırıcılık suçundan yazılı şekilde hüküm kurulması yasaya aykırı.

2- Kabul ve uygulamaya göre de;

Hükümden sonra. 01.05.2005 tarihinde yürürlüğe giren, 5335 Sayılı Yasanın 22. maddesi ile 5083 Sayılı Yasanın 2. maddesine eklenen son fıkra uyarınca, bir Yeni Türk Lirasının altında kalan tutarların atılmasında ve 01.06.2005 tarihinde yürürlüğe giren 5237 Sayılı Türk Ceza Kanununun 7 ve 5349 Sayılı Kanunla değişik 5252 Sayılı Türk Ceza Kanununun Yürürlük ve Uygulama Şekli Hakkında Kanunun 9. maddeleri uyarınca; anılan Kanunlar değerlendirilerek sonucuna göre sanıkların hukuki durumlarının takdir ve tayininde zorunluluk bulunması. **(11. CD., 01.11.2007, 10806-7429)**

Sanığın, şikayetçilere ait hesaplardan internet aracılığı ile kendi hesabına para aktarmaktan ibaret eyleminde gerçek kişiye yönelik hile ve desise bulunmadığı gözetilmeden 5237 Sayılı TCK'nın 244/4. maddesi yerine suç vasfında hataya düşülerek dolandırıcılık suçundan hüküm kurulması.

Kabule göre de:

Bilişim sistemindeki verileri değiştirmek suretiyle haksız menfaat elde edilmesi suçunun sanık tarafından havalenin şikayetçilerin hesaplarından kendi hesabına intikali anında tamamlandığı gözetilmeyerek eylemin teşebbüs aşamasında kaldığından bahisle eksik ceza tayini, (11. CD., **18.09.2007,6963-5533)**

1- Dolandırıcılık suçunun oluşabilmesi için 765 Sayılı TCK'daki hile ve desise ile 5237 Sayılı TCK'daki hilenin gerçek kişiye yöneltilerek aldatılması ve bu işlemler sonucunda onun veya başkasının zararına olarak sanığın veya bir başkasının lehine haksız yarar sağlanması gerekli olup, somut olayda; sanığın şikayetçiye ait kredi kartı bilgilerini ele geçirip kendisine ait cep telefonu faturasını Turkcell İletişim Hizmetleri A.Ş'nin Web sayfasına girerek interaktif ortamda ödediğinin iddia ve kabul olunması karşısında, gerçek kişiye yöneltilen hile ve desise bulunmadığından yüklenen fiilinin suç tarihinde yürürlükte bulunan 765 Sayılı TCK'ıım 525/b-2 (5237 sayılı Yasanın 244/4) maddesinde öngörülen bilişim suçunu oluşturduğu gözetilmeden vasıfta hataya düşülerek banka vasi kılınarak nitelikli dolandırıcılık suçunu oluşturduğunun kabulü ile yazılı şekilde hüküm kurulması.

2- Kabule göre de;

5252 Sayılı Türk Ceza Kanununun Yürürlük ve Uygulama Şekli Hakkındaki Kanunun 9/3. maddesi uyarınca suç tarihinde yürürlükte olan 765 sayılı TCK. ile 01.06.2005 tarihinde yürürlüğe giren 5237 Sayılı Kanunun ilgili bütün hükümleri olaya uygulanarak ortaya çıkan sonuçların birbirleriyle karşılaştırılması suretiyle lehe olan hükmün belirlenmesi gerektiği gözetilmeden denetime olanak vermeyecek şekilde 765 Sayılı Yasanın lehe 5237 Sayılı Yasanın aleyhe olduğundan bahisle yazılı şekilde karar verilmesi, **(11. CD., 23.01.2007,8412-87)**

Sanıkların oluşa uygun olarak sübutu kabul edilen önceden hazırladıkları tertibatla şikayetçilere ait bankamatik kartlarını ATM makinesine sıkışmasını sağlayıp yine atm kabinine monte ettikleri, içinde cep telefonu

bulunan duvar tipi telefonu arayıp kendisini banka görevlisi olarak tanıtıp kartı iptal edeceği bahanesiyle bankamatik kartının şifresini de öğrenip ATM makinesinden ayrılmalarını müteakip hile ve desiselerle ele geçirip şifresini öğrendikleri bankamatik kartlarıyla para çekmekten ibaret eylemlerinin 765 sayılı TCK'nın 504/3 (5237 sayılı TCK'nın 244/1.) maddesinde yazılı suçu oluşturduğu gözetilmeden bilişim suçu kabul edilerek yazılı şekilde hüküm kurulması, **(11. CD., 20.09.2006, 2696-7334)**

Sanıkların olay günü başkasına ait manyetik kart bilgileri ile birlikte kart şifrelerini ele geçirip bu şekilde ele geçirilen manyetik bilgileri beyaz kart denilen boş kartlara yazarak kartların ikizini üretmek suretiyle bu kartlarla alışveriş yapmak ya da nakit para çekmek için Denizbank'a ait ATM makinesinin güvenlik kamerasını bantla kapatarak yanlarında getirdikleri 60 cm uzunluğunda içinde çeşitli elektronik bağlantılar bulunan kamera düzeneğini ve kart kopyalama cihazını ATM makinesine monte ederek araçlarında beklemeye başladıkları sırada henüz kopyalama yapamadan yakalandıkları sanıkların eylemlerinin suç tarihi olan 26.6.2005 tarihi itibariyle yürürlükte bulunan 5237 sayılı TCK'nın 244/2-3 maddesinde tanımlanan suçu oluşturmadığı gibi 5237 sayılı TCK'nın 5377 sayılı yasa ile değişik 245/2. maddesinin de suç tarihinden sonra yürürlüğe girdiğinin anlaşılması karşısında yüklenen eylemlerin yürürlükte bulunan 5237 sayılı TCK'nın 158/f maddesinde tanımlanan suçu oluşturup oluşturmayacağına ilişkin delillerin tartışılması gerekli olup bu suça bakmak görevinin de üst dereceli ağır ceza mahkemesine ait olduğu, **(11. CD., 26.04.2006,1856-3468)**

Yakınana ait internet hattına 18.6.2000-5.12.2000 tarihleri arasında dışarıdan başkaları tarafından toplam 329 defa bağlantı yapılarak girilip görüşme yapıldığı, bunlardan sadece 48 adedinin sanıkların babası M. adına kayıtlı ev telefonundan 18.6.2000-30.9.2000 tarihleri arasında gerçekleştirildiği, sanıklardan T'nin 29.7.2000-16.12.2000 tarihleri arasında yurtdışında olduğu, sanık M'nin de Aralık 1999-Nisan2001 tarihleri arasında askerde olduğu 3 veya 4 haftada bir hafta sonlar babasının evine geldiği, her iki sanığın evde olmadıklar günlerde de babaları üzerine kayıtlı telefon ile

yakınanın internet hattına bağlantı yapıldığının anlaşılması ve bilirkişi Ö. tarafından düzenlenen 12.3.2003 tarihli raporda da "bağlanılan telefonun başka bir numara olarak gösterilmesinin mümkün olduğunun" belirtilmesi karşısında; sanıkların yüklenen suçu işlediklerine ilişkin her türlü kuşkudan uzak, hukuken elverişli, yeterli, kesin ve inandırıcı kanıt bulunmadığı gözetilmeden, yazılı şekilde mahkumiyetlerine karar verilmesi, **(6. CD., 16.03.2006,5464-2574)**

Sanıkların, haksız olarak ele geçirdikleri katılan şifresiyle internete girmek suretiyle hukuka aykırı yarar sağladıklarının iddia olunmasına göre; eylemin 765 Sayılı TCK'nın 525/b-2. maddesinde öngörülen suçu oluşturup oluşturmayacağına ilişkin delilleri takdir ve tartışmanın üst dereceli Asliye Ceza Mahkemesine ait olduğu gözetilerek görevsizlik kararı verilmesi gerekirken duruşmaya devamla yazılı şekilde hüküm kurulması. (11. CD., 08.02.2006,15451-698)

765 sayılı TCK'nın 525/b-2. (5237 sayılı TCK'nın 244) maddesine uyan suçlara ilişkin davaya bakmak, kanıtları değerlendirmek ve karar vermek görevi Asliye Ceza Mahkemesine ait bulunduğu halde, görevsizlik yerine yargılama sürdürülerek yazılı şekilde karar verilmesi. **(6. CD., 10.11.2005,18552-9931)**

1- Mağdura ait kredi kartını ele geçirerek bununla alışveriş yapan sanığın eyleminin 765 sayılı TCY'nin 504/3. maddesine uyan suçu oluşturduğu gözetilmeden, yazılı biçimde uygulama yapılması.

2- Sanığın çaldığı kredi kartı ile yaptığı alışverişlerin tarihlerini gösteren liste ilgili Bankadan getirtilerek sonucuna göre, 765 sayılı TCY'nin 80. maddesinin uygulama koşullarının tartışılması gerekirken, eksik inceleme ile hüküm kurulması.

3- Kabule göre de: uygulama yeri bulunmayan 765 sayılı Yasanın 522/1. maddesiyle cezanın arttırılması. **(6. CD., 07.11.2005,15800-9750)**

TCK 245. Madde İle İlgili Yargıtay Kararları

Yargıtay Ceza Genel Kurulu'nun 28.12,2004 gün ve 173/228 sayılı kararında da açıklandığı üzere; sanıkların, bankanın maddi varlıklarından olan şikayetçinin çalınan kredi kartını, post cihazından geçirerek haksız menfaat temin ettiklerinin iddia olunması karşısında; eylemin, suç ve karar tarihinde yürürlükte bulunan 765 sayılı TCK'nın 504/3. maddesinde öngörülen bankayı vasıta kılmak suretiyle dolandırıcılık suçunu oluşturup oluşturmayacağına ilişkin delillerin takdirinin üst dereceli Ağır Ceza Mahkemesine ait olduğu gözetilip görevsizlik kararı verilmesi gerekirken, yargılamaya devamla yazılı şekilde hüküm kurulması, **(11. CD., 08.10.2007,11162-6425)**

Sanık ile annesi diğer sanığın aşamalarda; hak sahibi ölü olan murisleri Kemal'in vefatından önce anılanın yatalak hasta olması ve sanık Bahar'in da okuma yazma bilmemesi nedeniyle maaşının oğlu sanık Cavit tarafından bankamatikten çekildiğini savunmalarına, maaşın yatırıldığı Vakıfbank İstanbul Gaziosmanpaşa Şubesinin 18.7.2002 tarihli yazısında da ölü Kemal'in maaşlarının bankomattaıV çekildiğinin bildirilmesi, şifresi bilinmeden kartın kullanılarak maaş hesabına ulaşılmasının mümkün bulunmayıp hak sahibinin maaşının ö-lümden öncede şifresi sanık tarafından bilinen kartın kullanıldığının ve sanığın 18.4.2001 günü ölen babasına ait banka kartını tahsis eden katılan kuruma iade etmeyerek haksız surette elinde bulundurup ölü babası Kemal'in hesabına yatırılan 19.4.2001-18.8.2001 dönemini kapsayan 4 aylık maaşını çekmeye devam ettiğinin anlaşılmasına göre suç tarihinde yürürlükte bulunan 765 sayılı TCK'nın 525/b-2, 80. (5237 sayılı yasanın 245/1.43) maddeleri de tartışılarak mahkumiyetine karar verilmesi gerektiği gözetilmeden, dosya kapsamındaki delillere, bankamatik kartının ancak bir şifre girilmek suretiyle bankoınatta kullanılmasının olanaklı bulunmasına sanığın, aile ilişkileri ve hayatın olağan deneyimlerine uygun düşmeyen savunmasına itibarla yazılı şekilde delil yetersizliğinden beraatine karar verilmesi, **(11. CD., 25.09.2007,10881-5846)**

Sanık Hüseyin Cinoğlu'nun, Danış adlı bir kişiden, dışı Ahmet Durak adına, içi, Mr. Olaf Fichtner isimli kişinin Allegemeine Deutsche Direklbank AĞ Frankfurt AM Main Germany (Almanya) isimli yabancı bankadaki gerçek hesabı ile ilişkilendirilmek suretimle tamamen sahte olarak üretilmiş Vakıfbank'a ait kredi kartı ve hayali bir kişi olan Ahmet Durak adına düzenlenmiş sahte nüfus cüzdanıyla cep telefonu satan mağdur Süleyman Savcı'nın işyerine diğer sanık Musa Yaman ile birlikte gelip, bir telefon ile 20 adet Türkcell ve Telsim firmalarına ait telefon kartlarım almak istedikleri, ödeme için sanık Hüseyin Cinoğlu'nun sahte kartı ve kimliği uzatması ile durumdan kuşkulanan şikayetçinin polis çağıracağını demesi üzerine sanıkların kaçtıkları ve polis tarafından 5-10 dakika sonra yolda yakalandıklarının iddia olunması karşısında; aynı kartla daha önce yapılan alış verişlerle ilgili olarak sanıklar hakkında açılmış bir dava olmadığı gözetilerek, dava konusu olmayan bu eylemlerde sanıkların birlikte veya tek başlarına hareket ettiklerinin ve suça konu sahte nüfus cüzdanının daha önce yapılan alış verişlerde kullanıldığının tespiti halinde sanık ya de sanıklar hakkında 5237 sayılı Yasanın 245/3. 43 ve 204/1. maddelerinde öngörülen zincirleme suretiyle "başkasına ait banka hesabıyla ilişkilendirilen sahte kredi kart kullanmak ve resmi evrakta sahtecilik" suçlarından davalar açılması sağlanıp, bu dava ile birleştirildikten sonra tüm deliller birlikte değerlendirilerek; sonucuna göre hüküm kurulması gerekirken, söz konusu kartla daha önce yapılan alış verişlerden dolayı dava açıldığı kabul edilmek suretiyle yazılı şekilde sanık Hüseyin Cinoğlu hakkında "zincirleme suretiyle başkasına ait banka hesabıyla ilişkilendirilen sahte kredi kartı kullanmak" ve "resmi evraktı sahtecilik" suçlarından, sanık Musa Yaman hakkında ise başkasına ait banka hesabıyla ilişkilendirilen sahte kredi kartı kullanmaya teşebbüs" suçuna yardım etmekten mahkumiyet hükümleri kurulması. (Y.CD., 11.06.2007,2956-4014)

Sanık üzerinde ele geçirilen sahte kredi kartlarını kabul etmek suçundan zamanaşımı içinde 5237 sayılı TCK'nın 245/2. maddesi uyarınca kamu davası açılması mümkün görülmüş ve anılan kanunun 61. maddesine

göre yasal ve yeterli gerekçe gösterilmeden cezanın alt sınırdan tayini aleyhe temyiz olmadığından bozma nedeni yapılmamıştır.

1- Yapılan duruşmaya, toplanıp karar yerinde gösterilen delillere, mahkemenin soruşturma neticelerine uygun şekilde inanç ve takdirine, incelenen dosya içeriğine göre sanık müdafiinin sair temyiz itirazlarının reddine; ancak:

TCK'nın 245/3. maddesinin "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 adli para cezası ile cezalandırılır" hükmü gereğince sanığın sahte kredi kartını pos cihazından geçirerek şikayetçi Feridun Razi Şahinbaz'ın dükkanından altın alma eyleminin daha ağır cezayı gerektiren kredi kartını kötüye kullanmak suçunu oluşturacağı gözetilmeden ayrıca dolandırıcılık suçundan da mahkumiyetine karar verilmesi,

2- Kabule göre de;

Dolandırıcılık suçunda, elde edilen menfaat olan altınların, alıp kaçan sanığın yakalanarak cebinden şikayetçi tarafından istirdat edildiğinin (geri alındığının) anlaşılması karşısında rızaya dayalı bir iade olmadığından etkin pişmanlık nedeniyle indirim yapılmayacağının gözetilmemesi, **(11. CD., 14.03.2007,480-1683)**

Sanık Abdullah Ekinci'nin. annesinin ölümünden sonra onun adına Bağ-Kur Genel Müdürlüğü tarafından Türkiye Halk Bankası Nevşehir Şubesi'ndeki hesabına yatırılan 65.000.000 lira maaşını bankamatik karlı ile bankomattan çektiğinin anlaşılması karşısında; eyleminin suç ve karar tarihinde yürürlükte bulunan 765 sayılı TCK'nın 525/b-2. (5237 sayılı Yasanın 245/1.) maddesinde öngörülen bilişim suçunu oluşturduğu gözetilmeden yazılı şekilde hüküm kurulması. **(11. CD., 12.03.2007,8843-1582)**

ÖZET

NACAR, Fatma Burcu, Information Crimes Practices in Criminal Law of European Union and Turkey, Master's Thesis, Ankara, 2010.

Yirminci yüzyılda bilişim ve sanayi devrimiyle beraber bilgisayarın hayatımıza girmesiyle bilişim sistemleri günlük hayatımızda geniş yer tutmuştur. İnsanlığa bir çok yarar ve iyilik sağlamakla beraber insanlığın zararına da kullanılmasıyla takip edilmesi ve önlenmesi zor sonuçlara sebebiyet vermektedir.

Çalışmamızın amacı bilişim suçlarıyla ilgili mücadelede devletlerin yapmış olduğu mevzuatın irdelenmesidir. Çalışmamızın ilk başında genel olarak bilişim ile ilgili temel bilgiler, bilişim suçlarının tarihi gelişimi, bilişim suçlarının tasnifi ve bilişim suçlarının yapısı incelenmiştir.

Çalışmamızda uluslararası alanda ve karşılaştırmalı hukukta bilişim suçları konusu ele alınmış, Avrupa Siber Suç Sözleşmesi işlenmiş, Türk Ceza Kanununu, Fikir ve Sanat Eserleri Kanunu ile Elektronik İmza Kanununda düzenlenen kanun hükümleri ele alınmış, karşılaştırılıp tartışılmıştır.

Anahtar Kelimeler: Bilişim, Veri, Program, Siber Suç Kavramı, Bilişim Suçu

ABSTRACT

NACAR, Fatma Burcu, Avrupa Birliği Ülkeleri ve Türkiye'de Bilişim Suçlarının Ceza Hukukundaki Uygulamaları, Yüksek Lisans Tezi, Ankara, 2010.

Computers having become a part of our lives further to industrial revolution, Information Technologies systems have become an important aspect of our lives. Although they provide many benefits and to humanity, they also cause many problems, which are hard to prevent, due to malevolent use by humans.

Purpose of this study is to scrutinize the legislation created by states in order to cope with information technologies crimes. Basic information on information technologies, historical development of information technologies crimes, classification of information technologies crimes, and structure of information technologies crimes are addressed at the beginning of our study.

We discussed information technologies in international field and in comparative law in our study, European Cyber Crimes Treaty was discussed, and Turkish Criminal Code, Intellectual and Industrial Properties Code, and Electronic Signature Code were discussed and compared.

Keywords: Information Technologies, Data, Program, Cyber Crime Concept, Information Technologies Crime