**ÇANKAYA ÜNİVERSİTESİ**
**SOSYAL BİLİMLER ENSTİTÜSÜ**
**KAMU HUKUKU ANABİLİM DALI**

**YÜKSEK LİSANS TEZİ**

# 5237 SAYILI TÜRK CEZA KANUNUNDA BİLİŞİM SİSTEMİNİ ENGELLEME, BOZMA, VERİLERİ YOK ETME VEYA DEĞİŞTİRME SUÇU

**BARIŞ EMRE ALP**

**EYLÜL 2018**

**ÇANKAYA ÜNİVERSİTESİ**
**SOSYAL BİLİMLER ENSTİTÜSÜ**
**KAMU HUKUKU ANABİLİM DALI**

**YÜKSEK LİSANS TEZİ**

# 5237 SAYILI TÜRK CEZA KANUNUNDA BİLİŞİM SİSTEMİNİ ENGELLEME, BOZMA, VERİLERİ YOK ETME VEYA DEĞİŞTİRME SUÇU

**BARIŞ EMRE ALP**

**EYLÜL 2018**

Tez Başlığı: **5237 Sayılı Türk Ceza Kanununda Bilişim Sistemini Engelleme, Bozma, Verileri Yok Etme Veya Değiştirme Suçu**

Tezi Hazırlayan: **Barış Emre ALP**

Sosyal Bilimler Enstitüsü Onayı

**Prof. Dr. Mehmet YAZICI**
**Enstitü Müdürü**

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

**Prof. Dr. Feriha Bilge TANRIBİLİR**
**Kamu Hukuku ABD Başkanı (Uhde)**

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

**Prof. Dr. Doğan SOYASLAN**
**Tez Danışmanı**

**Tez Jüri Tarihi: 04/09/2018**

**Tez Jüri Üyeleri:**

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

Doç. Dr. Güneş Okuyucu ERGÜN (Ankara Üniv.) :

Dr. Öğr. Üyesi A. Uğur ERİŞ (Çankaya Üniv.) :

**ÇANKAYA ÜNİVERSİTESİ**
**SOSYAL BİLİMLER ENSTİTÜSÜ MÜDÜRLÜĞÜ'NE**

Bu belge ile bu tezdeki bütün bilgilerin akademik kurallara ve etik davranış ilkelerine uygun olarak toplanıp sunulduğunu beyan ederim. Bu kural ve ilkelerin gereği olarak, tez çalışmamda bana ait olmayan tüm veri, düşünce ve sonuçları bilimsel etik kurallar gözeterek ifade ettiğimi ve kaynağını gösterdiğimi ayrıca beyan ederim. **06.09.2018**

Adı Soyadı : Barış Emre ALP

İmza :

# ÖZET

## 5237 SAYILI TÜRK CEZA KANUNUNDA BİLİŞİM SİSTEMİNİ ENGELLEME, BOZMA, VERİLERİ YOK ETME VEYA DEĞİŞTİRME SUÇU

**Barış Emre ALP**
**Yüksek Lisans Tezi**

Sosyal Bilimler Enstitüsü
Kamu Hukuku

Tez Danışmanı: Prof. Dr. Doğan SOYASLAN

Eylül 2018, 109 sayfa

Bilişim sistemleri ekonomi, sağlık, eğitim, bilimsel araştırmalar, savunma, idare gibi hayatımızın birçok alanında etkin bir rol oynamaktadır. Günümüzde hemen hemen tüm devlet kurumları, bankalar ve ticari işletmeler bütün iş ve işlemlerini bilişim sistemlerini kullanmak suretiyle gerçekleştirmektedir.

Vazgeçilemez hale gelen bilişim sistemlerinin, geçici süreyle de olsa çalışamaması büyük zararlara neden olabilmektedir. Özellikle çok iyi bir şekilde üretilmiş olan zarar verici yazılımlar ile pek çok kamu kurumunun işleyemez hale getirilebilmesi mümkün olduğu gibi şirketlerin ticaret yapması da engellenebilmektedir.

Yasa koyucu bu gibi yıkıcı etkileri olan eylemleri düzenleme altına alarak, bir nebze de olsa ortaya çıkabilecek zararların önüne geçmek istemiştir. Atfedilen bu önem dolayısıyla çalışmamızda, Bilişim Sistemini Engelleme, Bozma, Verileri Yok Etme veya Değiştirme Suçu incelenmiştir.

Çalışmamızda yapılan geniş kapsamlı kaynak araştırması neticesinde, incelenen tüm kaynaklar dikkate alınarak, özellikle çalışmamıza katkıda bulunacağı düşünülen doktrindeki tartışmalara mümkün olduğunca yer verilmiştir. Ayrıca, konumuzla ilgili Yargıtay kararlarına, çalışmamızı zenginleştirmesi, uygulamadaki

durumu ortaya koyması ve örnek oluşturması için atıfta bulunulmaya gayret edilmiştir.

**Anahtar Kelimeler:** Bilişim, Bilgisayar, Veri, Bilişim Suçu.

## ABSTRACT

## TURKISH CRIMINAL LAW CODE N. 5237 INFORMATION SYSTEMS TO PREVENT, DİSRUPT, DESTROY OR MODİFY DATA CRİME

**ALP, Barış Emre**
**Master Thesis**

Graduate School of Social Sciences
The Division of Public Law

Thesis Supervisor: Prof. Dr. Doğan SOYASLAN

September 2018, 109 pages

IT systems, economy, health, education, scientific research, defense, plays an active role in many areas of our lives such as administration. Nowadays, almost all government institutions, banks and commercial enterprises carries out all the work and operations through the use of information systems.

The inability to work indispensable informatics systems, even temporarily, can cause great losses. Particularly damaging software with many companies as possible to make the public institutions can not handle is also prevented from doing business.

The legislator regulated by the devastating effects of such actions, he wanted to prevent any damage that may occur to some extent. Because of the importance of attribution, we have studied "Blocking the Information System", "Destruction, Destroying Data" or "Modification Crimes".

As a result of the extensive resource survey conducted in our work, the discussions in the doctrine, which is thought to contribute particularly to our work, are given as much as possible, taking into account all the resources examined. Moreover, the Supreme Court decision regarding our issues, our enrichment activities, create a situation that demonstrate exemplary practice and every effort was made to be referred to.



**Keywords:** Informatics, Computer, Data, Cyber Crime.

## İÇİNDEKİLER

**İKİNCİ BÖLÜM**

**BİLİŞİM SUÇLARININ İŞLENME ŞEKİLLERİ**

**ÜÇÜNCÜ BÖLÜM**

**5237 SAYILI TÜRK CEZA KANUNUNDA BİLİŞİM SİSTEMİNİ ENGELLEME, BOZMA, VERİLERİ YOK ETME VEYA DEĞİŞTİRME SUÇU İLE HAKSIZ ÇIKAR SAĞLAMA SUÇU**

## KISALTMALAR LİSTESİ

| | |
|---|---|
| age. | : Adı geçen eser |
| ASSS | : Avrupa Konseyi Siber Suç Sözleşmesi |
| BAM | : Bölge Adliye Mahkemesi |
| bkz. | : Bakınız |
| C | : Cilt |
| CD | : Ceza Dairesi |
| CGK | : Ceza Genel Kurulu |
| CMK | : Ceza Muhakemesi Kanunu |
| Çev. | : Çeviren |
| E. | : Esas |
| FSEK | : Fikir ve Sanat Eserleri Kanunu |
| HAGB | : Hükmün Açıklanmasının Geri Bırakılması |
| HMK | : Hukuk Muhakemeleri Kanunu |
| K. | : Karar |
| m. | : Madde |
| Mat | : Matbaa |
| M.Ö. | : Milattan önce |
| ODTÜ | : Orta Doğu Teknik Üniversitesi |
| RG | : Resmi Gazete |
| RTÜK | : Radyo ve Televizyon Üst Kurumu |
| S. | : Sayı |
| s. | : Sayfa |
| SSÇ | : Suça Sürüklenen Çocuk |
| SÜHFD | : Selçuk Üniversitesi Hukuk Fakültesi Dergisi |
| T. | : Tarih |
| TAAD | : Türkiye Adalet Akademisi Dergisi |
| TBB | : Türkiye Barolar Birliği |
| TBK | : Türk Borçlar Kanunu |

| | |
|---|---|
| TBMM | : Türkiye Büyük Millet Meclisi |
| TCK | : Türk Ceza Kanunu |
| YCGK | : Yargıtay Ceza Genel Kurulu |
| TDK | : Türk Dil Kurumu |
| TMK | : Terörle Mücadele Kanunu |
| TTK | : Türk Ticaret Kanunu |
| TÜBİTAK | : Türkiye Bilimsel ve Teknolojik Araştırma Kurumu |
| UYAP | : Ulusal Yargı Ağı Bilişim Sistemi |
| Y | : Yıl |
| Yay. | : Yayın |

# GİRİŞ

İnsanlık tarihinin en önemli buluşlarından birisi olan bilgisayar, günümüzde insan hayatının ayrılmaz bir parçası haline gelmiştir. Bilgisayarın bulunmasıyla bu alanda hızlı bir ilerleme gösterilmiş, gelişen teknoloji akıl almaz boyutlara ulaşmıştır. Bilgisayara ilaveten internetin de kişisel kullanıma açılmasıyla bu alan daha da ilerleme göstermiş, internet de tıpkı bilgisayar gibi hayatımıza kalıcı bir şekilde yer edinmiştir.

Günümüzde hemen hemen herkesin üzerinde, akıllı telefonlarla bir bilişim sistemi ve bir internet bağlantısı mevcut hale gelmiştir. Önceleri görüntülü konuşmanın hayali bile kurulamazken şimdilerde kıtalar arası görüşmeler her an yapılabilmektedir. Hatta bu teknoloji küçük çocukların dahi rahatlıkla ulaşabileceği ve kullanabileceği seviyeye gelmiştir.

Bu bilişim teknolojisi ekonomi, sağlık, eğitim, bilimsel araştırmalar, savunma, idare gibi hayatımızın birçok alanında etkin bir rol oynamaktadır. Günümüzde hemen hemen tüm devlet kurumları, ticari işletmeler, bankalar bütün iş ve işlemlerini bilişim sistemlerini kullanarak gerçekleştirmektedir. Bu bilişim sistemlerinde para dahil her türlü bilgi ve değer zahmetsizce ve kolaylıkla saklanabilir hale gelmiştir. Aynı doğrultuda saklanan bu bilgi ve değerler yine tek tuşla hazır edilebilir hale gelmiştir.

Bu denli ilerleyen teknoloji yeni suç tiplerini de beraberinde getirmiştir. Yüzyıllar boyunca işlenen hırsızlık, yaralama vb. klasik suç tiplerine teknoloji ile beraber bilişim suçları da eklenmiştir.

Diğer suç tiplerine nazaran bu suç tipinde faillerin yakalanma ihtimali çok az olup coğrafi alan sınırlaması da yoktur. Fail eylemlerini istediği yerde istediği ülkede gerçekleştirebilme imkanına sahiptir. Aynı doğrultuda uğranılan zarar da bu suç tipinde bir hayli yüksektir. Bir kamu kurumuna ait bilişim sisteminin geçici süreyle de olsa çalışamaması büyük zararlara neden olabilmektedir. Hatta bu zarar bazen bütün toplum aleyhine olabilmektedir. Özellikle çok iyi bir şekilde üretilmiş olan

zarar verici yazılımlar ya da bir web sitesini çökertmek için kullanılan DDoS saldırıları ile pek çok kamu kurumunun işleyemez hale getirilebilmesi mümkün olduğu gibi şirketlerin ticaret yapması da engellenebilmektedir.

Yasa koyucu bu gibi yıkıcı etkileri olan eylemleri düzenleme altına alarak bir nebze de olsa ortaya çıkabilecek zararların önüne geçmek istemiştir. Atfedilen bu önem dolayısıyla çalışmamızda, Bilişim Sistemini Engelleme, Bozma, Verileri Yok Etme veya Değiştirme Suçu incelenmiştir.

Çalışmamızda, yapılan geniş kapsamlı kaynak araştırması neticesinde incelenen kaynakların tamamı dikkate alınmakla birlikte özellikle çalışmamıza katkıda bulunacağı göz önünde tutularak doktrindeki tartışmalara da mümkün olduğunca yer verilmiştir. Ayrıca çalışmamızı zenginleştireceği ve uygulamadaki durumu ortaya koyacağı, örnek oluşturucağı düşüncesiyle, konumuzla ilgili Yargıtay kararlarına atıf yapılmaya gayret edilmiştir.

Çalışmamız üç ana bölümden oluşmaktadır.

İlk bölümde bilgisayar, veri, internet, bilişim, bilişim sistemi ve bilişim suçunun tanımı yapılarak özellikleri ve tarihsel gelişimlerinden bahsedilmiştir.

İkinci bölümde, bilişim suçlarının işlenme şekilleri incelenmiştir. Bu kapsamda, truva atı, çöpe dalma, gizlice dinleme, bilgi ve veri aldatmacası, gizli kapı, sosyal mühendislik, salam tekniği, mantık bombası vb. pek çok yöntem ele alınarak bilgi verilmiştir.

Çalışmamızın üçüncü ve son bölümünde ise 5237 sayılı Türk Ceza Kanununda düzenlenen Bilişim Sistemini Engelleme, Bozma, Verileri Yok Etme veya Değiştirme Suçu ile Bilişim Sistemini Kullanarak Haksız Çıkar Sağlama Suçu üzerinde durularak bu suçlar açısından korunan hukuki yarar, unsurları, suçun özel görünüş şekillleri, nitelikli halleri, yaptırımı ile soruşturma ve kovuşturma hususları incelenmiştir. Çalışmamızın sonuç bölümünde ise incelememiz neticesinde elde etmiş olduğumuz tespitler ile değerlendirmelere yer verilmiştir.

# BİRİNCİ BÖLÜM
# BİLİŞİM SİSTEMİ

## 1. BİLGİSAYAR

### 1.1. Genel Olarak

İngilizcede "compute" kelimesinden türeyen "computer", türkçede bilgisayar kelimesine karşılık gelmektedir. Computer, sayma, toplama, hesaplayarak sonuca ulaşma, hesap etme anlamlarına sahip olmakla birlikte aslında daha da geniş bir kavramı ifade etmektedir[1].

1970'li yıllarda ülkemize giren bilgisayar, bilimsel ve iş alanlarında kullanılmaya başlanmasıyla yabancı dillerin de etkisinde kalınarak "ordinatör", "kompütür" ve "elektronik beyin" gibi kelimeler ile anılmaktaydı. Fakat günümüzde bütün bu kelimeler terk edilmiş ve bilgisayar kelimesi üzerinde tam bir uzlaşı sağlanmış ve sözcük kullanımdaki yerini tam manasıyla almıştır[2].

Bilgisayar kelimesi devşirme bir kelime olmayıp öz Türkçe bir kelimedir. İngilizcedeki computer kelimesinin aksine yalnızca hesaplayıcı anlamına gelmez. Computer kelimesinden daha geniş bir kavramı içerir. Bilgi işleme kökünden türetilerek bilgi vermek, bilgi saymak anlamlarını içerir[3].

### 1.2. Tanımı

Önceleri büyük bir monitör ve kasa olarak üretilen bilgisayar, günümüzde teknolojinin de hızla ilerlemesi sonucunda diz üstü bilgisayar (lap top), tablet, cep telefonu gibi bir çok türde ve hatta dokunarak çalışır şekilde üretilmeye başlanmış, bunların bir çoğu dokunarak çalışır hale gelmiştir. Yakın bir gelecekte bu teknolojinin de ilerisine gidilerek sesle çalışabilir hale hatta katlanabilir, cebe konulabilir şekilde bilgisayar yapılmasına yönelik çalışmalar bulunmaktadır. Bu çerçevede teknolojinin hızla ilerliyor olması sebebiyle bilgisayarın tanımını yapmak her geçen gün zorlaşmaktadır. Ceza hukukunda tipe uygunluk, kıyas yasağı ve

---

[1] Dülger, M. V. (2015). *Bilişim Suçları ve İnternet İletişim Hukuku*. Ankara: Seçkin Yay., s. 62; Pallı, H. (2008). *Türk Hukukunda ve Mukayeseli Hukukta Bilişim Suçları*. (Yayımlanmamış Yüksek Lisans Tezi). Erciyes Üniversitesi/Sosyal Bilimler Enstitüsü, Kayseri. s. 4.

[2] Dülger, age. s. 63

[3] Dülger, age. s. 63

kanunilik ilkeleri çerçevesinde konuya bakıldığında ve aynı zamanda bizim ceza kanunlarımızın bu ve benzeri kavramlara genel olarak yer vermiş olması da göz önünde bulundurularak, tanımların açık ve net olarak herkesce bilinmesi gerekmektedir[4].

Doktrinde kabul edilmiş genel bir bilgisayar tanımı mevcut olmayıp, farklı şekillerde tanımlamalar yapılmıştır. Buna göre bilgisayarı, Yenidünya-Değirmeci "*dış ortamdan çeşitli yöntemlerle aldığı verileri, içeriğinde bulundurduğu programlar doğrultusunda depolayan, işleyen, bu verilerden yeni sonuçlar üreten, ürettiği sonuçları kullanıcıya sunan, bu suretle veri iletişimi sağlayan bir makine*" şeklinde tanımlamıştır[5]. Akbulut, "*insanlar tarafından hazırlanıp yüklenen programlar yardımıyla bilgileri belirli bir düzende saklamak, işleyerek yeni sonuçlar üretmek, üretilen bilgileri başka bir yerlere iletmek, başka yerlerdeki bilgilere ulaşmak gibi amaçlarla kullanılan makineler*" şeklinde tanımlamıştır[6]. Yazıcıoğlu, "*yeterince kavramsallaştırılmış ve iyi tanımlanabilmiş her türlü problem üzerinde çalışabilen bir aygıttır"* şeklinde ifade etmiştir[7]. Kurt, "*programlara ve verilen komutlara göre işlem yapan, otomatik olarak çalışan, sıralı işlem yapan, verileri depolama, işleme tabi tutma, tasnif ve terkip etme, iletme özelliklerine sahip olan, elektronik ya da manyetik akımlarla çalışan, mantıklı sonuçlar üreten, programlanabilen, genel amaçlı kullanılabilme özelliklerine sahip elektronik cihazlar"* olarak belirtmiştir[8].

Bilişim Ağı Hizmetlerinin Düzenlenmesi ve Bilişim Suçları Hakkında Kanun Tasarısı taslağının 2. maddesinin 1. fıkrasının b bendinde bilgisayar, "*belleğindeki programa uygun olarak aritmetik ve mantıksal işlemleri yapabilen, karar verebilen, yürüteceği programı ve işleyeceği verileri ezberinde tutabilen, çevresiyle etkileşimde bulunabilen araçlardır*" şeklinde tanımlanmış, fakat bu tasarı yerine yürürlüğe giren 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar

---

4 Pallı, age. s. 6-7; Dülger, age. s. 64.

5 Yenidünya, A. C., Değirmenci O., (2003). *Mukayeseli Hukukta ve Türk Hukukunda Bilişim Suçları*. 1. Baskı, İstanbul: Legal Yayıncılık. s. 19.

6 Akbulut, B. B., (2000). Bilişim Suçları. Selçuk Üniversitesi Hukuk Fakültesi Dergisi. Milenyum Armağanı, C. VIII, S.1-2. s. 546.

7 Yazıcıoğlu, R. Y. (1997). *Bilgisayar Suçları: Kriminolojik, Sosyolojik ve Hukuki Boyutları İle*. İstanbul: Alfa Yay. s. 27.

8 Kurt, L. (2005). Bilişim *Suçları ve Türk Ceza Kanunundaki Uygulaması.* Ankara: Seçkin Yay. s. 31; Benzer tanım için bkz. Özmestik, F. Ü., (2015). Bilişim Sistemleri Üzerine Arama ve El Koyma Tedbirine İlişkin Mevzuat ve Uygulamada Yaşanan Sorunlar. (Yayımlanmamış Yüksek Lisans Tezi). İstanbul Bilgi Üniversitesi/Sosyal Bilimler Enstitüsü. İstanbul. s. 4.

Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkındaki Kanun'da bilgisayarın tanımına dair herhangi bir düzenleme mevcut değildir[9].

TDK ise bilgisayarı, "*çok sayıda aritmetiksel veya mantıksal işlemlerden oluşan bir işi, önceden verilmiş bir programa göre yapıp sonuçlandıran elektronik araç, elektronik beyin"* olarak tanımlamıştır[10].

Bilgisayar terimi gerçekten de çok geniş bir kavramdır. Sadece bilgi işleyen ya da hesaplama yapabilen araçlar değildir. Bilgisayarlar sadece bilgi işleyen bir araç olarak kabul edilseydi, hesap makinelerinden bir farkı olmayacaktı. Bilgisayarların programlanabilir olmasının, onları hesap makinesinden ayırarak çamaşır makinesi ya da televizyon gibi cihazlara yaklaştırdığı düşünülmektedir. Gerçekten de çamaşır makineleri de programlanabilir makinelerdir. Ancak tabiki bilgisayarların bilişim özelliğinin, yani genel amaçlı kullanılabilme özelliğinin bulunması en önemli ayırıcı unsurdur. Bir bilgisayar ile bilgiler depolanabilmekte, istenilen bilgilere ulaşılabilmekte, hesap yapılabilmekte, müzik dinlenebilmekte, ses ve görüntü kaydı yapabilmektedir[11].

Bu çerçevede genel ve kısa bir bilgisayar tanımı yapmak gerekirse bilgisayar, çok sayıda aritmetiksel ve mantıksal işlemler yapabilen, verileri, bilgileri saklayan, depolayan, işleyen, gerektiğinde çok hızlı bir şekilde sonuçları ileten bir elektronik alettir. Bilişim suçları bakımından önemli olan kıstas ise, verileri saklaması, alması ve göndermesidir. Yukarıda bir çok tanımda bilgisayar için depolamadan bahsedilmemiştir. Bilgisayarlar, veri depolama işlevine sahip olup bir nevi sanal arşiv hizmeti vermektedir. Bu sanal arşivler bir çok bilişim suçunun özellikle konumuz olan TCK'nın 244. maddesinin işlenme yeri olacaktır.

Konunun başında da bahsedildiği üzere, teknolojik gelişmeler yüzünden bilgisayara ilişkin genel ve yeterli nitelikte bir tanımlama yapılması çok zordur. Bilişim alanındaki yeni gelişmeler nedeniyle bugün yapılan tanımlamalar yarın için yeterli olmayabilir. Bu yüzden teknoloji karşısında yapılan her tanımlama yetersiz kalacak, sürekli yeni bir tanımlama yapılması ihtiyacı doğacaktır. Bakıldığı zaman akıllı ev projesi kapsamında, ikamette bulunan buzdolapları, içerisinde barındırdığı

---

9 Erdoğan, Y. (2013). *Türk Ceza Kanunu'nda Bilişim Suçları (Avrupa Konseyi Siber Suç Sözleşmesi ve Yargıtay Kararları İle)*. İstanbul: Legal Yay. s. 22.

10 http://www.tdk.gov.tr/index.php?option=com_gts&arama=gts&guid=TDK.GTS.5ab88d03dc32b2.99174495 (Erişim tarihi: 02/01/2018)

11 Pallı, age. s. 6.

bir takım besinlerin bitmesi ya da azaldığını tespit etmesi halinde marketlerden otomatik olarak sipariş vermekte, bu özellikleri sayesinde de adları bilgisayar olmasa bile bilgileri otomatik olarak işleme tabi tutuyor olması sebebiyle bilgisayar kavramı içerisinde değerlendirilebilmektedir. Aynı doğrultuda, parmak izi, göz retinası taraması ve yüz tanıma aracılığıyla aktif hale gelen sistemler de bu çerçevede bilgisayar sayılabilecektir[12]. Gelecekte, hem ev içerisinde hem de evler arasında ağ vasıtalarıyla bağlantı kurulabilecek, bu bağlantı, ev işlerinin yapılmasına yönelik olacaktır. Bu şekilde birbirine bağlanan evlere yönelik büyük tehlikelerin de ortaya çıkması söz konusu olabilecektir. Şöyle ki, yetkisiz erişim ve siber saldırılarla bir evin içerisine girilmesi, ev halkı hakkında bilgiler temin edilebilmesi gibi tehlikeler ortaya çıkabilecektir.

### 1.3. Tarihsel Gelişimi

Bilgisayar tek bir hamle ile ya da tek bir mucitin sadece kendi çabalarıyla meydana getirebileceği kadar basit bir buluş değildir. Eski tarihlere kadar giden birçok farklı buluşun çakışması, birçok bilgi aktarılması ve düşünme etkinliklerinin üst üste gelmesi sonucu bilgisayar ortaya çıkmıştır[13].

Bilgisayar, adından da anlaşılacağı üzere, hesap işlerinde yardımcı olmaya yarayan bir alet olarak düşünülmüştür. İlk mekanik hesaplama aleti, M.Ö. 3500'lü yıllarda abaküs olarak adlandırılan bir sayı aletidir. Abaküslerden esinlenilerek, aynı zamanda kağıt ve kalemin kullanımının yaygınlaşmasıyla ilk toplama aleti, 1642'li yıllarda bir vergi toplayıcısının oğlu olan Blaise PASCAL tarafından geliştirilmiştir. Daha 18 yaşındayken babasına yardım etmek amacıyla bulduğu ve sayısal hesaplama çarkı adını verdiği bu alet, 8 hareketli kadranlardan oluşarak 8 basamaklı sayıları toplayabilmekteydi. PASCAL'dan esinlenen Alman matematikçi Gottfried Wilhem Von Leibniz 1694'lü yıllarında çarpma işlemi yapabilen bir makineyi; 1820'li yıllarda da Fransız Charles Xavier Thomas de Colmar dört işlemi yapabilen bir makineyi icat etmişti. Colmar'ın bu icadı birinci dünya savaşına kadar yaygın bir şekilde kullanılmıştı[14].

---

12 Yenidünya C. Değirmenci O. age. s. 19; Dülger, age. s. 65.

13 Dülger, age. s. 104-105.

14 Güngör N. M., (2007). *Yeni Türk Ceza Kanunu Kapsamında Bilişim Suçları ve Emniyet Genel Müdürlüğü Uygulamaları.* (Yayımlanmamış Yüksek Lisans Tezi). İstanbul Üniversitesi/Sosyal Bilimler Enstitüsü. İstanbul. s. 23.

Günümüzde kullanılan bilgisayar, 1856 yıllarda icat edilen bir alet ile başlamaktadır. Charles BABBAGE tarafından analitik motor adı verilen bu alet belli bir programlama içerisinde hesapları otomatik olarak yapabilmekteydi[15].

Günümüzdeki bilgisayarlara gerçek anlamda en yakın teknoloji 1940'lı yıllarda ortaya çıkmıştır. İki büyük dünya savaşının 1900'lü yılların yaşanması, aynı zamanda ikinci dünya savaşında havacılık ve uzay teknolojisinin hızla ilerlemesi, bu savaşlar sebebiyle iki büyük gücün ortaya çıkması bu ülkelerin silahlanma, nükleer ve uzay çalışmalarında büyük yol almasına neden olmuş, bu gelişmelere paralel olarak bilgisayar teknolojisi de büyük gelişim göstermiştir[16].

Bu tarihlerden sonra birçok mucit bilgisayarın ortaya çıkması konusunda önemli ilerlemeler kaydetmiştir. İkinci dünya savaşı ile birlikte ülkeler, stratejik bilgiler için bu alanda çalışmaya başlamış, bu alanlara önemli miktarlarda fon aktarılmış, bu gelişmeler de bilgisayarın gerçek anlamda ortaya çıkmasına ve geliştirilmesine büyük katkı sağlamıştır[17].

1940'lı yıllarda ABD hükümeti Pennslyvania Üniversitesi ile birlikte geliştirdiği ENIAC (Elektronik Numerical Integrator and Computer) adlı bilgisayar, 30 ton ağırlığında 18.000 vakum tüp, 5 milyon lehim noktası, 70.000 resistor ve 180 metrekarelik alandan oluşmaktaydı[18].

Alman mühendis Konrad Zuse 1941 yılında uçaklar ve mermiler için Z3 adında bir bilgisayar geliştirdi. Bu bilgisayar ile müttefik kuvvetler önemli başarılar elde etmişti. Almanların bu denli başarılarını gören İngilizler, gizli kodları kıran Colossus adını verdikleri bir bilgisayar geliştirerek Alman mesajlarını deşifre etmişlerdi. Bu Colossus adındaki bilgisayar fazla gelişim gösteremedi. Fazla gelişim gösterememesindeki başlıca sebeplerden birisi, bu makinenin varlığının savaştan sonra on yıl boyunca gizli tutulması, bir diğer sebep de genel amaçlı bir bilgisayar olmayıp sadece gizli bilgileri deşifre etmesi için tasarlanan bir bilgisayar olmasıydı[19].

1944 yılında IBM ile çalışan mühendis Howard H. Aiken, ABD Deniz Kuvvetleri için balistik bir deniz haritası oluşturabilmek için tamamıyla elektronik bir hesap makinesi üretmeyi başardı. Makine içerisindeki kablolar 500 mil uzunluğunda ve bir futbol sahasının yarısı kadar büyüklükteydi. 1951'li yıllarda bir

---

15 http://www.bilgiler.gen.tr/ilk-bilgisayar-nasil-ortaya-cikti.html (Erişim tarihi: 02/01/2018)
16 Dülger, age. s. 106.
17 Güngör, age. s.24-25.
18 Yenidünya C. Değirmenci O. age. s. 13-14; Güngör, age. s. 26.
19 Güngör, age. s. 24-25.

şirketin ticari amaçları doğrultusunda üretilen bilgisayar Amerikan Nüfus bürosunda kurularak çalıştırılmıştı. 1958 ile 1964'lü yıllarda bilgisayarın donanım unsuru yerine yazılım unsuruna önem verilmiş, uzmanlar tarafından yazılım üretilmeye başlanılmıştır. Transistörlerin (mikroçipler) küçük boyutlara indirgenmeleri Amerikalı mucitin silisyum olan transistörlü işlemciyi bulmasıyla mümkün hale gelmişti. 1965 ile 1971'li yıllarda transistörlerin yerini tümleşik devreler almış, bilgisayarlar artık ulaşılamaz makineler olmaktan çıkarak gündelik işlerde kullanılan makine halini almıştır[20].

Bu doğrultuda 18 Ekim 1966 tarihinde yeni bir suç türü, Minneapolis Trıbune gazetesinden yayımlanan "bilgisayar uzmanı banka hesabında tahrifat yapmakla suçlanıyor" başlıklı haber ile kamuoyuna yansımış, bu olay yeni bir suç işleme şeklini yani alanımız olan bilişim suçunu ortaya çıkarmıştır[21].

1971'li yıllardan sonra uygulama yazılımları geliştirilmiş, her türlü iş bilgisayarlarda yapılır hale gelmiştir. 1978 yılında Apple isimli bilgisayar şirketi ve devamında diğer şirketlerin de devreye girmesiyle işlemci ve tümleşik devlerin geliştirilip küçültülmesiyle çok sayıda işyerinde bilgisayarlar aktif halde kullanılmaya başlanmıştır. 1990'lı yıllarda internetin kişisel kullanıma açılmasıyla bilgisayar başka bir boyutlara ulaşmış ve bilgisayar alanında şimdilik en son değişiklik bu olmuştur[22].

### 1.4. Unsurları

Bilgisayar soyut ve somut unsurlarıyla bir bütündür. Bilgisayarın somut unsurları onun donanım kısmını oluşturur. Bir bilgisayarın klavyesi, faresi, yazıcısı, belleği, mikro işlemcisi gibi fiziksel kısımları somut kısımlarına yani donanım kısımlarına örnek olarak gösterilebilir. Bilgisayarın somut unsurlarının yanı sıra fiziki varlığı olmayan soyut unsurları da vardır. Bunlar yazılım kısmıdır. Elle tutulamayan veri veya programlar bilgisayarın yazılımını oluşturur.

#### 1.4.1. Donanım Unsuru (Hardware)

Bilgisayarı oluşturan elle tutulabilen fiziki bileşenler, bilgisayarın donanım kısmını oluşturur. Bunlar ana işlemci, salt okunur bellek (ROM), rasgele erişilebilen bellek (RAM), klavye, fare, yazıcı, tarayıcı, ekran, cd-room, ekran ve ses kartı,

---

20 Aydın, E. D., (1992). *Bilişim Suçları ve Hukukuna Giriş.* Ankara: Doruk Yayınevi. s. 13.

21 Aydın, age. s. 13.

22 Dülger, age. s. 108.

bilgisayar giriş çıkış birimleri gibi parçaları ifade eder. Bu parçaların en önemlilerinden kısaca bahsetmek gerekirse;

#### 1.4.1.1. Ana İşlemci (Mikro İşlemci - Merkezi İşlem Birimi)

İngilizce Central Processor Unit (CPU)'dan çevrilen merkezi işlem birimi veya kısaca mikro işlemci olarak da çevrilen ana işlemci, içerisinde on binlerce küçük devre barındıran tümleşik yapıdaki bir yongadır. Bilgisayarın bütün birimleri ana işlemcinin komutlarıyla devreye girerek işlem yapar. Bilgisayarın yönetim birimi ve beynidir[23].

Ana işlemci giriş biriminden gelen veriler üzerinde mantıki işlemler yapar, yapılan işlemleri denetler ve işlem sonuçlarını geçici olarak saklar[24].

Bu birim, gerçek komutları işleten denetim birimi, komut biriminin doğrudan bağlandığı yazmaç adı verilen bellek birimi, trigonometrik ve logaritmik fonksiyonlar gibi hesaplamaların yapılmasında rol oynayan matematiksel yardımcı işlemci, komutları sıraya sokarak komut birimine gönderen komut besleme birimi, sık kullanılan komutların tutulduğu dahili ön bellek, dış dünya ile bağlantısını sağlayan adres yolu ile veri yolu denetçilerinden oluşur[25].

#### 1.4.1.2. Salt Okunur Bellek (ROM)

Salt okunur bellek, ingilizce Read Only Memory (REM) ibaresinden dilimize çevrilmiştir. Bilgisayarın temel işlevlerini yerine getirmesi ve açılması için gerekli olan verilerin bulunduğu bellektir. Buradaki veriler bilgisayarın yapım aşamasında bilgisayarı yapan kişiler tarafından yerleştirilen verilerdir. Bu veriler salt okunur özelliklerinin bulunması sebebiyle, silinmeleri, değiştirilmeleri, zarara uğratılmaları mümkün değildir. Ana işlemci tarafından sadece okunmak için kendisine ulaşılır[26].

Salt okunur bellek üzerinde, bilgisayarın en temel işlevlerini yerine getirmesine yarayan programlar bulunur. Bu programlar topluluğuna Bios (Basic Input / Output System) yani temel giriş çıkış sistemi adı verilir. Bu programların temel amacı, kullanıcı ile bilgisayar arasında bilgi alış verişi sağlamaktır. Örneğin,

---

[23] Pallı, age. s. 10-11; Dülger, age. s.66; Yenidünya, Değirmenci, age.s. 22-23.

[24] Kızıltan M. B., (2007). *5237 sayılı Türk Ceza Kanununda Bilişim Sistemine Girme, Sistemi Engelleme ve Bozma Suçları.* (Yayımlanmamış Yüksek Lisans Tezi). İstanbul Üniversitesi/Sosyal Bilimler Enstitüsü. İstanbul. s. 9.

[25] Yenidünya, Değirmenci, age. s. 23.

[26] Dülger, age. s. 67; Kızıltan, age.s.10; Pallı, age. s.12.

bilgisayar kullanıcısının klavyede bastığı "A" tuşu ile salt okunur bellekte saklanan programlar sayesinde ekranda "A" harfi görülür ve bu hiç bir zaman değiştirilemez[27].

#### 1.4.1.3. Rasgele Erişimli Bellek (RAM)

İngilizce "Random Access Memory-RAM" kelimesi, Türkçede "Rasgele Okunur Bellek" şeklinde çevrilmiştir. Rasgele Erişimli Bellek, bir tür veri deposudur. Bilgisayara girilen verilerin üzerine yazıldığı, bilgisayar çalıştığı sürece faaliyetine devam eden, sistemin kapatılması halinde verileri silen ya da değiştirebilen, veri okuma hızının fazla olduğu bellektir[28].

#### 1.4.1.4. Çevre Giriş (Input) - Çıkış (Output) Birimleri

Bilgisayarda bir işlem yapmak istendiğinde, bu işlemin bilgisayarın anlayacağı şekle çevrilmesi gerekir ki buna giriş birimleri denilmektedir. Aynı şekilde bilgisayarda bir işlem yapıldığı zaman kullanıcısının anlayabileceği şekle çevrilmesi gerekir ki buna da çıkış birimleri denir[29].

Çevre giriş çıkış birimleri, bilgisayara veri girişlerinin yapıldığı, fare, klavye, tarayıcı, disket sürücüsü, CD/DVD, USB kart, kamera, mikrofon gibi giriş birimleri ile hoparlör ve yazıcı gibi çıkış birimlerinden oluşur. Ekran (monitör), disket, sabit disk, flash bellek ve optik disk hem giriş hem de çıkış birimlerindendir[30]. Gerçekten de bir disketin içerisindeki bilgilerin bilgisayara yükleneceği zaman giriş birimi olurken, bilgisayardan herhangi bir şeyin diskete yükleneceği zaman çıkış birimi olacaktır[31]. Bilgisayar, çevre giriş çıkış birimiyle dış ortam yani kullanıcı ile irtibatını sağlar. Bu çevre giriş ve çıkış birimleri teknolojinin gelişmesine paralel olarak değişmekte hem de artmaktadır. Örneğin, önceleri bilgisayarın giriş birimlerinden olan klavye olmaksızın herhangi bir şey yapılamazken, şimdilerde dokunmatikler aracılığıyla klavyeye ihtiyaç duyulmaksızın istenilen işlemler yapılabilmektedir. Aynı şeyler fare için de geçerlidir. Benzer şekilde dizüstü bilgisayarlarının, tabletlerin artmasıyla birlikte çok fazla yer kaplayan bilgisayar kasalarına ihtiyaç duyulmamaktadır[32].

---

27 Yenidünya, Değirmenci, age. s. 24.
28 Dülger, age. s. 67; Yenidünya, Değirmenci, age. s. 24; Pallı, age. s. 12.
29 Kurt, age. s. 34; Gürler, age. s. 20.
30 Pallı, age. s. 12; Gürler, age. s. 20.
31 Demircan, M. T., (2016). *Bilişim Alanında Suçlar*. İstanbul: Legal Yay. s. 14.
32 Dülger, age. s. 67.

### 1.4.2. Yazılım Unsuru (Software)

Yukarıda da belirtildiği üzere, bilgisayarın yazılım unsuru, donanım unsurunun aksine elle tutulamayıp maddi yönü olmayan bilgisayarın soyut unsurunu oluşturur. Her türlü bilgisayar programları, program parçaları, yazılım dilleri bilgisayarın yazılım kısmını oluşturur[33]. TDK yazılımı, "*bir bilgisayarda donanıma hayat veren ve bilgi işlemede kullanılan programlar, yordamlar, programlama dilleri ve belgelemelerin tümü*" şeklinde ifade etmiştir[34].

Özellikle uygulama yazılımları, bilgisayar programı olarak ifade edilir. İngilizcede software kelimesinin dilimizdeki karşılığıdır. Bir bilgisayarın istenilen şekilde çalışmasına yardımcı olan, bilgisayar ile kullanıcısı arasında köprü vazifesi gören[35], bilgisayarın çalışmasının kullanıcısı tarafından denetlenmesine ve istenilen şekilde çalışmasına müdahale edilmesine olanak veren, sonuçlardan kullanıcısının faydalanmasını sağlayan, sistematik olarak bir araya getirilmiş veri dizileri olarak belirtilebilir[36]. 5846 sayılı FSEK 3. maddesinde yazılım yani program "*Bir bilgisayar sisteminin özel bir işlem veya görev yapmasını sağlayacak bir şekilde düzene konulmuş bilgisayar emir dizgesini ve bu emir dizgesinin oluşum ve gelişimini sağlayacak hazırlık çalışmaları*" şeklinde tanımlamıştır.

İki tür yazılım vardır. Bunlar, işletim yazılımı ve uygulama yazılımlarıdır.

#### 1.4.2.1. İşletim Yazılımı (Operating System)

İşletim sistemleri, anti virüs programları gibi yazılımlar işletim yazılımlarındandır[37]. Sistem yazılımı olarak da isimlendirilen işletim yazılımları, bilgisayarların fonksiyonlarını yerine getirebilmesi için kullanılan bir yazılım türüdür. Sistemin etkin ve verimli çalışma gösterebilmesi için bilgisayarın işleyişini kontrol eder. Diğer yazılımların çalışmalarını yönlendirir. Kullanıcının direkt olarak temasta bulunduğu yazılım türüdür. Bilgisayar ile kullanıcısı arasında köprü görevi görür[38].

Bilgisayarın donanımlarıyla bilgisayar kullanıcıları arasında köprü işlevi gören ve kodlardan oluşan yapılarla, donanım parçalarının yönetimini sağlayan

---

33 Demircan, age. s. 14.

34 http://www.tdk.gov.tr/index.php?option=com_gts&arama=gts&guid=TDK.GTS.5aba1ebb2f3809.69038226 (Erişim tarihi: 05/01/2018)

35 Yenidünya, Değirmenci, age. s. 23; Pallı, age. s. 14.

36 Pallı, age. s. 14.

37 Yaycı, E. (2007). *Bilişim Suçları.* (Yayımlanmamış Yüksek Lisans Tezi). Gazi Üniversitesi/Sosyal Bilimler Enstitüsü. Ankara. s. 9.

38 Yenidünya, Değirmenci, age. s. 23

yapılara işletim yazılımları denir[39]. Bir bilgisayarda hangi işin, hangi yöntemle ve bilgisayarın hangi özellikleri kullanılarak yapılacağını belirleyen, bilgisayar çalıştığı esnada onun donanım parçalarını denetleyen ve donanım ile yazılım özellikleri arasında bağ kuran ana kontrol programlarıdır[40].

Bu yazılım türü genellikle konunun uzmanları yani yazılım şirketleri veya bilgisayar üreten şirketler tarafından yapılmaktadır. En iyi bilinen işletim yazılımı bilgisayarın işletim sistemidir. Bu işletim sistemleri yani kısaca bilgisayarlar, bilişim suçu açısından bir delil toplama yeridir. Uzman bir kişi tarafından gerçekleştirilecek bir delil toplama faaliyeti ile çok sayıda olay aydınlatılabilir[41].

#### 1.4.2.2. Uygulama Yazılımı (Application Program)

Yukarıda da belirtildiği üzere uygulama yazılımları, programlar olarak da bilinirler. Herhangi bir problemi çözmek ya da belirli bir fonksiyonu yerine getirmek için yazılan, bilgisayarda baştan beri kurulu olan işletim sistemiyle uyumlu olarak çalışan yazılım türüdür[42]. Günlük hayatta yaptığımız resim çizme, hesap işleri, yazı yazma gibi işleri bilgisayar ortamında yapmamızı sağlayan yazılımlardır[43].

İşletim yazılımından farkı, işletim yazılımları yukarıda da belirtildiği üzere genel amaçlı hizmet verip bilgisayarın işlemesini sağlamak için çalışırken, uygulama yazılımları kullanıcının amacı doğrultusunda hizmet verip kullanıcısı için faydalı sonuçlar elde edebilmesi için kullanılan bir yazılım türüdür[44].

Uygulama yazılımları olmasaydı, bilgisayarda yapılması gereken her iş ile ilgili kullanıcı kendi yazılımını yapmak zorunda kalacak ya da bu iş için uzmanlaşmış kişilere her seferinde bu tarz işleri yaptırmak zorunda kalacaklardı[45].

Eskiden sadece askeri veya ticari alanlarda ilgili yazılımlar bilişim suçlarına konu olurken, günümüzde neredeyse bütün yazılımlar bilişim suçlarının konusu olabilmektedir. Özellikle konumuz çerçevesinde düşünüldüğünde bir çok suç, zararlı yazılım programları üretilmek ve bunların kullanılması suretiyle işlenebilmektedir[46].

---

39 Orta, M. (2015). *Bilişim Suçlarında Adli Analiz*. (Yayımlanmamış Doktora Tezi). Selçuk Üniversitesi/Sosyal Bilimler Enstitüsü. Konya. s. 12.

40 Demircan, age. s. 15.

41 Orta, age. s. 12.

42 Kurt, age. s. 36.

43 Yaycı, age. s. 10.

44 Dülger, age. s. 68.

45 Yenidünya, Değirmenci, age. s. 25.

46 Dülger, age. s. 68.

## 2. VERİ

İngilizcede "data" kelimesinin karşılığı olarak dilimizde veri kelimesi kullanılmaktadır[47]. Bilişim sistemlerinin amacı veriyi işlemek, sonuç çıkarmak ve saklamaktır. Veri ise bilgisayar tarafından iletişim işlem ve açıklama amacıyla herhangi bir amaç, durum, konu, fikir, koşul veya diğer unsurları açıklamak için harfleri, simgeleri, sayıları belirtmek üzere kullanılan genel bir terimdir[48]. Yani kısaca veri, bilgilerin belirli bir formata dönüştürülmüş halidir. Bir bilişim sisteminde saklanan her şey örneğin bir resim, yazı, program birer veridir[49].

ASSS'nin 1. maddesinde veri, "*belirli durumların, bilgilerin kaydı ya da bir bilgisayarın bir işlemi gerçekleştirmesini sağlayacak biçimleri de içeren bilgisayar sistemince icra edilebilecek bir işlemler bütünü*" şeklinde ifade edilmiştir.

5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun'un tanımlar bölümünü düzenleyen 2. maddesinde veri, "*bilgisayar tarafından üzerinde işlem yapılabilen her türlü değer*" olarak belirtilmiştir.

5070 sayılı Elektronik İmza Kanunun 3. maddesinde elektronik veri, elektronik, optik veya benzeri yollarla üretilen, taşınan veya saklanan kayıtları ifade ettiği belirtilmiştir.

TCK'nın 243. maddesinin gerekçesinde de sistem içerisindeki bütün soyut unsurların veri teriminin kapsamında olduğu ifade edilmiştir.

Sonuç olarak veri, bilgisayarın soyut unsurlarından olan, sistemin varlık sebebi sayılan ve sistemin istenilen doğrultuda çalışmasını sağlayan genel bir kavramı ifade etmektedir.

## 3. İNTERNET

### 3.1. Genel olarak

Bilişim ve bilgisayar denildiğinde ilk akla gelen kavram kuşkusuz ki internettir. İnternet bir iletişim aracı olarak hayatımızda çok önemli değişiklikler ortaya çıkarmıştır. İnternet sayesinde günümüzde bilgiye en hızlı, kolay ve ucuz şekilde ulaşılabilmesi mümkün kılınmıştır. Ancak internetin bu gibi olumlu

---

47 Dülger, age. s. 84.

48 Ersoy, Y., (1994). *Genel Hukuki Koruma Çerçevesinde Bilişim Suçları*. Ankara Üniversitesi Siyasal Bilgiler Fakültesi Dergisi. C. 49, S. 3-4. s. 169.

49 Yenidünya, Değirmenci, age. s. 47-48; Güngör, age. s. 22.

yanlarının yanı sıra bir takım olumsuzlukları da söz konusudur. Bilişim suçlarının da işlenme hususu aynı derecede kolay ve hızlı bir hale gelmeye başlamış[50], birçok suçun işlenebilmesi için rahatça başvurulabilen bir araç durumuna gelmiştir[51].

İnternetin en önemli özelliği herhangi bir kişinin ticari malı olmamasıdır. Yani internetin bir sahibi, yöneticisi ya da denetleyicisi bulunmamaktadır. Büyük bir ağ sistemi ve bu sisteme giren kişilerin katkısıyla oluşmuş anonim bir yapı durumundadır. Bu sebeple internete bağlanmak için herhangi bir özel izin, onay ya da başvuru gerekmemektedir[52]. Bu durum kişiler için paylaşımlarında bir özgürlük alanı oluşturmakta, sansür yapılma olasılığını neredeyse sıfır seviyesine düşürmekte, sınırsız bir ifade özgürlüğünün ortaya çıkmasına yol açmaktadır[53].

Bununla birlikte internetin kullanımının daha da yaygınlaşması neticesinde birçok sorunlar da ortaya çıkmaktadır. İnternet bünyesinde, bütün diğer teknolojik sistemler gibi birtakım boşlukları ve riskleri de barındırmaktadır[54]. Klasik anlamdaki hırsızlık, dolandırıcılık gibi suçlar açısından yeni işleniş şekilleri ortaya çıkarmış, verileri yok etme veya değiştirme gibi yeni suç tiplerinin ortaya çıkması da bu şekilde gerçekleşmiştir.

### 3.2. Tanımı

İnternet aslında veri iletim ağlarından yalnızca birini oluşturmaktadır. Sanal alanın yalnızca bir parçası olmakla birlikte yine de günümüzde en geniş ve en çok bilinen parçası durumundadır. Sanal alan ise bilişim sistemleri ve bilişim sistemlerini birbirine bağlayan çeşitli veri iletişim ağından meydana gelen, sayısal verilerden oluşan bir alandır[55].

İnternet, INTERnational ve NETwork kelimelerinin birleştirilmesinden oluşan çok geniş kapsamlı bir ağdır[56]. Dünya üzerindeki tüm ağların ve bilgisayarların birbirine bağlanması ile oluşan ağların her geçen gün daha da hızlı bir şekilde büyümesi ve yeni ağların bu sisteme dahil olması sebebiyle internete "tüm

---

50 Orta, age. s. 30-31; Dülger, age. s. 86-87.

51 Özen, M., Baştürk İ., (2011). *Temel Hak ve Özgürlükler Bağlamında Bilişim – İnternet ve Ceza Hukuk*. 1. Baskı. Ankara: Adalet Yay. s. 2.

52 Dülger, age. s.89; Orta, age. s.35.

53 Dülger, age. s. 90; Orta, age. s.32.

54 Orta, age. s.36.

55 Dülger, age. s.86.

56 Dülger, age. s. 86; Orta, age. s.31; Güngör, age. s. 15.

dünya bilgisayarlar ağlarının ağı", "ağların ağı" veya "ağlar arası ağ" da denilmektedir[57].

Daha da teknik bir ifadeyle internet, dünya üzerinde bulunan tüm ağların ve bilgisayarların TCP/IP denilen bir yöntemle birbirine bağlanmasıyla oluşan dünyadaki en kapsamlı insan ve makine birliğini sağlayan ağ olarak ifade edilmektedir[58].

Başka tanıma göre ise internet, birden çok haberleşme ağının birlikte oluşturduğu, resim, yazılı metin, müzik, grafik gibi dosyalar ile bilgisayar yazılımlarının, yani insanlar tarafından oluşturulan her türlü bilginin veri olarak paylaşıldığı ve iletildiği bilişim sistemleri arasındaki ağdır[59].

### 3.3. Tarihsel Gelişimi

İnternetin temelleri ilk olarak 1980'li yılların sonlarında atılmış olmakla birlikte, halkın erişimine 1990'lı yıllarda açılmış ve sonrasında hızlı bir şekilde büyüme göstermiştir[60]. Ülkemizde ise ilk internet bağlantısı 1993 yılında TÜBİTAK ve ODTÜ'nün ortak projesiyle gerçekleştirilmiştir[61].

İnternetin halk arasında yaygınlaşması bir çok iletişim aracına oranla daha hızlı bir şekilde gerçekleşmiştir. Uluslararası Telekomünikasyon Birliği'nin (ITU) 1999 yılı verileri nazara alındığında, internetin 50 milyon kullanıcıya ulaşması için 4 yıl gibi çok kısa bir zaman diliminin yetmiş olmasına rağmen, aynı koşullarda bu süreç telefon için 74 yıl, televizyon için 13 yıl, radyo için ise 38 yıl sürmüştür[62].

## 4. BİLİŞİM KAVRAMI

Bilişim kavramı, yeni bir bilim dalını tanımlamak amacıyla Fransız Akademisi tarafından 1967 yılında kabul edilmiş[63], Türkiye'de ise ilk defa Prof. Dr. Aydın KÖKSAL tarafından kullanılmıştır. “Bilmek” fiilinin bir türevi olan “bilişmek” fiilinden türetilmiştir[64].

Bu bilimin kökleri fizik, matematik ve elektromanyetiktir. Bir tür mühendislik alanıdır. Verileri depolayabilen, aktarabilen ve algoritmalar yardımıyla

---

57 Dülger, age. s. 86; Orta, age. s.31.
58 Dülger, age. s.86; Güngör, age. s.15-16.
59 Dülger, age., s.86-87.
60 Dülger, age. s.87; Orta, age. s.31-32.
61 Özen, age. s. 9; Orta, age. s. 33; Güngör, age. s. 17.
62 Dülger, age., s. 87; Orta, age. s. 32.
63 Erdoğan, age. s. 5.
64 Pallı, age. s. 34.

verileri işleyebilen matematiksel makineler tasarlar. Bu sayede bilişim, gerçek süreçlerin simulasyonunu mümkün kılar. Bir yardımcı bilim olarak düşünülmesi halinde bilişim, diğer bilimlerdeki olguları soyutlaştırarak bu olguları algoritmalar yardımıyla işleyebilmektedir[65].

Ülkemizde hukuk alanında bilişim kavramı ilk olarak 1989 yılında TCK'nın Ön tasarısında kullanılmıştır. Bu tasarının 342. maddesinin gerekçesinde bilişim alanı, "*bilgileri depo ettikten sonra bunları otomatik işleme tabi tutan ve sistemlerden oluşan alan*" olarak ifade edilmişti. Ancak 765 Sayılı TCK'da bilişim alanındaki suçları düzenleyen 525/a ve 525/b maddelerinde bu kavrama yer verilmemiş, madde metninde yer almayan bu kavrama, ilgili maddelerin yer aldığı 11. babın başlığında yer verilmiştir. 5237 sayılı gerek TCK'nın maddesinde gerekse gerekçesinde bilişim kavramı tanımı yer almamaktadır[66].

Bilişim kelimesi doktrinde farklı şekillerde tanımlanmıştır. Yazıcıoğlu, Fransızca informatique kelimesinin Türkçeleştirilmiş hali olduğunu, "*bilginin otomasyona tabi tutulması sonucunda işlenmesini yani verilerin saklanması, organize edilmesi, değerlendirilmesi, nakledilmesi, çoğaltılması, anlamlarını*" içerdiğini belirtmiş[67], Aydın "*bilginin ve iletişim yapısı ve özellikleri; bilginin aktarılması, organize edilmesi, saklanması, tekrar elde edilmesi, değerlendirilmesi ve dağıtımı için gerekli kuram ve yöntemler ve öte yanda da; bilgiyi kaynağından alıp kullanıcıya aktaran ve genel sistem bilimi, siberteknik, otomasyon ile insanın çalışma çevrelerindeki yerinde ve zamanında kullanılan teknolojileri temel alan bilgi sistemleri, şebekeleri, işlevleri, süreçleri ve etkinleri*"[68], Dülger "*insanların teknik, ekonomik, siyasal ve toplumsal alanlardaki iletişimde kullandığı bilginin, özellikle bilgisayar aracılığıyla düzenli ve akılcı biçimde işlenmesi, her türden düşünsel sürecin yapay olarak yeniden üretilmesi, bilginin bilgisayarlarda depolanması ve kullanıcıların erişimine açık bulundurulması bilimi*"[69], Yenidünya-Değirmenci "*teknik, ekonomik, sosyal, hukuk ve benzeri alanlardaki verinin saklanması, saklanan bu verinin otomatik olarak işlenmesi, organize edilmesi, değerlendirilmesi ve*

---

65 Özbek, V. Ö. (2007). Banka Veya Kredi Kartlarının Kötüye Kullanılması Suçu. Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi. Prof. Dr. Ünal NARMANLIOĞLU'na Armağan. C. 9. s. 1023.

66 Taşkın, Ş. C. (2008). *Bilişim Suçları*. Bursa: Beta Yay. s. 6; Dülger, age. s. 76-77.

67 Yazıcıoğlu, R. Y. (2005). Yeni Türk Ceza Kanunundaki Bilişim Suçlarının Genel Değerlendirilmesi. Yeditepe Üniversitesi Hukuk Fakültesi Dergisi. C. II. S. 2. s. 403.

68 Aydın, age. s. 3.

69 Dülger, age. s. 75.

*aktarılması ile ilgili bir bilim dalı*"[70], Özen- Baştürk "*bilgisayardan da faydalanılmak suretiyle bilginin saklaması, iletilmesi ve işlenerek kullanılır hale gelmesini konu alan akademik ve mesleki disipline verilen isim*"[71], Akbulut ise "*insanların teknik, ekonomik ve toplumsal alanlardaki iletişimde kullandığı ve bilimin temeli olan bilginin elektronik araçlarla özellikle bilgisayarlar aracılığıyla işlenip, ses, görüntü ve veri taşıyan iletişim hatları aracılığıyla aktarılması bilimi*" olarak tanımlamıştır[72].

TDK ise "*bilişim insanoğlunun teknik, ekonomik ve toplumsal alanlardaki iletişiminde kullandığı ve bilimin dayanağı olan bilginin özellikle elektronik makineler aracılığıyla düzeni ve akla uygun biçimde işlenmesi bilimi*" olduğunu ifade etmiştir[73].

## 5. BİLİŞİM SİSTEMİ

Eski 765 sayılı TCK'da yer alan "bilgileri otomatik işleme tabi tutma" ifadesi 5237 sayılı Yeni TCK'da haklı olarak terk edilmiş ve yerine bilişim sistemi terimi kullanılmıştır. 5237 sayılı Kanun'un 243. maddesinin gerekçesinde bilişim sistemi, "*verileri toplayıp, yerleştirdikten sonra bunları otomatik işlemlere tabi tutma olanağını veren manyetik sistemler*" olarak belirtmiştir[74]. Ceza Muhakemesinde Ses ve Görüntü Bilişim Sisteminin Kullanılması Hakkında Yönetmeliğin 3. maddesi de bilişim sistemini, "*Bilgisayar, çevre birimleri, iletişim altyapısı ve programlardan oluşan veri işleme, saklama ve iletmeye yönelik sistem*" olarak tanımlanmıştır.

Hukukumuzda her ne kadar bilişim sistemi terimi kullanılsa da ASSS bu kavram yerine bilgisayar sistemi terimini tercih etmiştir. Buna göre ASSS bilgisayar sistemini, "*bir veya birden fazlası belirli bir yazılım çerçevesinde otomatik olarak veri işleyen bir cihazı veya birbirlerine bağlı veya birbirleriyle ilişkili bir dizi cihaz*" şeklinde ifade etmiştir. Bakıldığı zaman bilişim sistemi terimi sadece bilgisayar ile sınırlı bir terim değildir. Bu sebeple ve aynı zamanda gelişen teknolojiye paralel

---

70 Yenidünya, Değirmenci, age. s. 27.

71 Özen, Baştürk, age. s. 11

72 Akbulut, *Bilişim Suçları*. s. 546.

73 bkz. www.tdk.gov.tr (Erişim tarihi: 25/01/2018)

74 Erdoğan bu tanımda yer alan verilerin toplanması ve yerleştirilmesiyle ne kastedildiği, kimler tarafından bu veriler toplanmakta ve yerleştirilmekte vb konuların açık olmadığını, muğlak olduğunu ifade etmiştir. bkz. age. s. 10-11.

hareket edilmesi açısından da hukukumuzda bilgisayar sistemi yerine bilişim sistemi teriminin kullanılması son derece isabetli olmuştur[75].

Taşkın, bir sistemin bilişim sistemi sayılabilmesi için 3 farklı kriter olduğunu belirtmiştir. Birinci kriter, bir sistem bilgisayar temelli çalışıyorsa, bilgisayar olmadan sistem çalışamazsa yani sistemin olmazsa olmazı bilgisayar ise o sistem bilişim sistemidir. İkinci kriter, eski 765 sayılı Kanun döneminde ortaya konulan, bilgileri otomatik işleme tabi tutma ölçütüdür. Eğer bir sistem bilgileri otomatik olarak işleme tabi tutuyorsa ve aynı zamanda o bilgileri işleyebiliyorsa o sistem artık bir bilişim sistemidir. Üçüncü kriter ise sistemin genel amaçlı çalışıyor olmasıdır. Buna göre Taşkın, belli bir amaca özgülenmemiş olması halinde o sistemin artık bilişim sistemi olarak kabul edilmesi gerektiğini ifade etmiştir[76].

Doktrinde Taşkın ile beraber Kurt ve Yazıcıoğlu da, bir sistemin bilişim sistemi kabul edilebilmesi için onun manyetik özelliğinin yanı sıra genel amaçlı kullanımının da olması gerektiğini ifade etmiştir. Bu çerçevede, buzdolabı, çamaşır makinesi, kumandalar genel amaçlı işlem yapamıyor olmaları sebebiyle bilişim sistemi olarak kabul edilemeyeceklerdir[77]. Orta da bilişim sisteminin, "*verilerin belli bir düzen içinde bilgisayar ortamında saklandığı ve tanımlanan bilgi gereksinimlerini karşılamak üzere dönemsel ya da talep üzerine raporlar üreten, gereken veriye kısa sürece erişim olanağı sağlayan belli bir donamım üzerinde işletilen yazılım ve veriler bütünü*" olduğunu ifade etmiştir[78]. Erdoğan ise Taşkın ve Kurt'un aksine bilişim sistemi belirlenirken kullanılan genel amaç kriterini benimsemeyip veri depolama, işleme ve veri iletişimi yapabilen sistemlerin bilişim sistemi olacağını kabul etmiş, bir sistemde eğer bir veri depolama, işleme ve iletme özelliği varsa artık o sistem bilişim sistemi olarak kabul göreceğini belirtmiştir[79].

YCGK bilişim sisteminin, bilgisayardan daha üst bir kavram olduğunu, bilginin otomasyona tabi tutulması sonucunda işlenmesini, yani verinin organize edilmesini, saklanmasını, değerlendirilmesini, çoğaltılmasını, nakledilmesini de kapsadığını, bilişim sistemlerinde veri iletişiminin, bilgisayarla birlikte, manyetik,

---

75 Aynı doğrultuda bkz. Erdoğan, age. s.11-12, 16; Kurt, age. s. 139.

76 Taşkın, C. (2009). Bilişim Hukuku Uluslararası Uyuşmazlıklar. TBB Dergisi. S. 85. s. 333-334

77 Kurt, age. 141; Yazıcıoğlu, *Genel Değerlendirme.* s. 404.

78 Orta, age. s. 23.

79 Erdoğan, age. s. 12-13.

elektronik veya bazı mekanik araçlarla bir ağ üzerinden sağlanabileceğini ifade etmiştir[80].

Tanımlarda da belirtildiği üzere bilişim sistemi, bilgi teknolojilerini ve bilgisayarı da kapsayan üst ve geniş bir kavramdır. Her bilgisayar bir bilişim sistemi iken her bilişim sistemi bilgisayar olmayabilir [81]. Bununla birlikte cep telefonları, kişi veya araçları elektronik olarak tanıyan güvenlik araçları, cep bilgisayarları da bilişim suçlarının konusu olabilir. Nitekim Yargıtay vermiş olduğu bir kararında ilk derece mahkemesince cep telefonunun bilişim sistemine dahil olmadığını belirten kararı bozarak cep telefonunun da bilişim sistemine dahil olduğunu ifade etmiştir[82].

Yargıtay, bilgisayar haricinde para çekme makinesi olan ATM'lerin de bilişim sistemi içerisinde sayıldığını belirtmiştir, ATM'lere karşı işlenen suçları bilişim sistemlerine karşı işlenen suçlardan saymıştır[83].

Bununla birlikte yukarıda da belirtildiği üzere, akıllı cep telefonları dışındaki telefonlar, dekoderler, takoğraf cihazlarının bilişim sistemine dahil oldukları kabul görmemektedir. Bununla birlikte bir sisteminin bilişim sistemi olup olmadığı noktasında tereddütlerin hasıl olması halinde alanında uzman bilirkişi incelemesi yaptırılarak sonuca ulaşılması pek tabi mümkün olacaktır[84].

Ceza kanunlarında belirginlik asıl olandır. Bilişim alanında yaşanan gelişmeler bu belirginliği ortadan kaldırmaktadır. Nitekim İngiliz düzenlemelerinde, bilişim sisteminin karşılığı olarak söylenebilecek bir bilgisayar tanımına yer verilmemiştir. Bir tanıma yer verilmesi İngilizler tarafından gereksiz ve saçma görülmüş, verilecek bir tanımın gelişen teknolojinin gerisinde, eksik ve yetersiz kalacağı düşüncesiyle, bir tanım yapılmasından kaçınılmıştır[85]. Hukukumuzda Erdoğan da İngiliz düzenlemelerine benzer yönde düşünerek, teknolojinin bu denli gelişmesine karşın kanun yapımının zaman alması sebebiyle bilişim sistemi

---

80 Bkz. YCGK 19/06/2007 T., 6-136/150; YCGK 17/11/2009 T., 2009/11-193 E., ve 2009/268 K . sayılı ilamları (UYAP'tan alınmıştır; ayrıca çalışmamızın devamında kaynak belirtilmeyen diğer kararlar için de bahsi geçen kaynak kullanılmıştır.)

81 Aynı doğrultuda bkz. Dülger, age. s. 75; Yenidünya, Caner, age. s. 31; Erdağ, age. s. 278; Erdoğan, age. s. 9; Orta, age. s. 23.

82 bkz. YRG. 8. CD. 18/03/2015 T, 2014/30037 E. ve 2015/2015 K. sayılı ilamı.

83 YCGK. 10/04/2001 T., 2001/76-30E., 2001/757 K. sayılı ilamı.

84 Taşkın, Uluslararası uyuşmazlıklar, s. 334.

85 Sarı, O., (2013), *Uluslararası Hukuk ve Türk Ceza Hukuku Bağlamında Siber Güvenlik ve Bilişim Sistemine Yönelik Suçlar*. (Yayımlanmamış Yüksek Lisans Tezi).Harp Akademileri, Stratejik Araştırmalar Enstitüsü. s. 77.

kavramının her somut olayın özelliğine göre yorumlanması gerektiğini ifade etmiştir[86].

## 6. BİLİŞİM SUÇU

### 6.1. Terimi Sorunu

Bilişim suçları için ABD'de, computer related crime (bilgisayar bağlantılı suç), computer assisted crime (bilgisayarla işlenen suç), crimes against computer (bilgisayara karşı işlenen suç) gibi kavramlar kullanılsa da en yaygın olarak kullanılan terim computer crime (bilgisayar suçu) terimidir. Bu terim ABD hukukunda "*bilgisayar verilerinin çalınması veya sabote edilmesi ya da herhangi bir suçun işlenmesi için bilgisayarların kullanılması gibi bilgisayar teknolojisini gerektiren suç çeşidi*" olarak tanımlanmaktadır[87].

Ülkemizde ise gelişen teknolojilere paralel olarak bu konuda tam bir kavram kargaşası yaşanmış ve bir çok terim ortaya atılmıştır. Siber suç, internet suçu, sanal suç, bilgisayar suçu, bilgisayar ile ilgili suç, bilgisayara karşı işlenen suç, bilgisayarlar aracılığıyla işlenen suç, bilişim suç hukuku, bilişim sistemi aracılığıyla işlenen suç ve bilişim suçu terimleri farklı farklı yazarlarca kullanılmıştır[88].

2000'li yıllardan itibaren gerek mevzuatlarımızda, gerek uygulamada gerekse doktrinde bu denli fazla olan kavram karmaşası azalmış ve bilişim suçları terimi üzerinde uzlaşma sağlanmıştır[89].

### 6.2. Tanımı

Bilişim alanının yeni bir alan olması, bunun yanında her geçen gün yeni bir bilişim suçunun işlenme şekli ortaya çıkması sebebiyle bilişim suçu kavramı üzerinde görüş birliği mevcut değildir[90]. Hukukumuzda da bilişim suçunun tanımına ilişkin herhangi bir bilgi yer almamaktadır[91].

Doktrinde bilişim suçu kavramı üzerine bir çok tanım yapılarak farklı kriterler ortaya atılmıştır. Birinci kriter, bilgisayarın amaç veya araç olması kriteridir. Bu kritere göre bilgisayarın, fiilin aracı veya hedefi olduğu davranışlar bilişim suçu olarak tanımlanmaktadır. Yazıcıoğlu, bilgisayar suçlarını bilgisayarın konusunu ya

---

86 Erdoğan, age. s. 16.

87 Diğer ülkelerde kullanılan terimler için bkz. Dülger, age. s. 77-78; Kızıltan, age. s.18-19.

88 Bu terimlerin hemen hepsine ayrı ayrı getirilen eleştiriler için bkz. Dülger, age. s. 78-79.

89 Dülger,age.s. 80; Yaycı, age. s. 24;

90 Kızıltan, age. s. 20.

91 Dülger, age. s. 80.

da vasıtasını yahut simgesini oluşturduğu suç olgusunu içeren fiiller şeklinde tarif ederek bu kriteri esas almıştır[92]. İkinci kriter, bilgisayarı malvarlığı itibariyle sınırlayan kriterdir. Buna göre, kasıtlı ve hukuka aykırı malvarlığı ihlalleri bilişim suçu sayılacaktır. Üçüncü kriter, bilişim sistemleriyle hangi suretle olursa olsun bağlantılı olan suçları esas alır. Buna göre, bilişim suçları, bilgisayarla ve veri iletişimiyle bağlantılı mağdur veya mağdurların zarar gördüğü ya da görme ihtimali olduğu her türlü suçu kapsayan kriterdir. Önder, "*kanunlara aykırı, ahlaki bakımdan kabul edilmeyen ya da haksız davranışların otomatik bilgi işleyen sistem ile ilgili olarak işlenmiş suçlar*" olarak belirtmesi sebebiyle bu kriteri esas almıştır[93]. Dördüncü kriter, bilgisayar kullanımını esas alan kriterdir. Bu kriter, bilişim suçunun işlenebilmesi için bilgisayar kullanımını zorunlu gören kriterdir. Beşinci ve son kriter ise suçu işleyen faili esas alan kriterdir. Bu kriter, bilgisayar bilgisine sahip olanların işledikleri suçları esas alan kriterdir[94]. Akbulut bilişim suçunun karma nitelikte kriterlere sahip olduğunu ve bilişim suçunun "*verilerle veya veri işlemle konu bağlantısı olan ve bilişim sistemleriyle veya bilişim sistemine karşı işlenen suçlar*" olduğunu ifade etmiştir[95]. Aydın "*Elektronik bilgi işlem kayıtlarına yasadışı yollarla erişilmesi veya bu kayıtların yasal olmayan şekilde değiştirilmesi, silinmesi veya bu tür kayıtlara girilmesi veyahut bilgi tecavüzü için hazırlık yapılması*"[96], Ersoy "*bilgisayarı da kapsayan ancak daha geniş olan bilişim araçlarına karşı veya bilişim araçları ile işlenen suçlar anlaşılması*"[97], Erdoğan "*bilişim sistemine yönelik veya bilişim sisteminin kullanıldığı suç*"[98], Dülger *"verilere ve/veya bilişim sistemlerine veya sistemin/verilerin düzgün ve işlevsel işleyişine, güvenilirliğine ya da bütünlüğüne karşı işlenen suçlar*"[99], Eker "*bilişim araçlarına/sistemlerine karşı veya bilişim araçları/sistemleri vasıtasıyla işlenen, verilere, veri-işlem ile veri-*

92 Yazıcıoğlu, *Bilgisayar Suçları*. s. 142.

93 Önder, A. (1994). *Şahıslara ve Mala Karşı Cürümler ve Bilişim Alanında Suçlar*. İstanbul: Filiz Kitapevi. s. 505.

94 Konu hakkında ayrıntılı bilgi için bkz. Akbulut, Bilişim suçları s. 550; Kızıltan, age. s. 21-22.

95 Akbulut, bilişim suçları, s. 551.

96 Aydın, age. s. 27-28

97 Ersoy, age. s. 151.

98 Karagülmez, A., (2014). *Bilişim Suçları ve Soruşturma-Kovuşturma Evreleri*. Genişletilmiş ve Gözden Geçirilmiş 2. Baskı, Ankara: Seçkin Yay. s. 57.

99 Dülger, age. s. 83.

*aktarımlarıyla ilgili olan suç şekli*"[100], Turan "*bilgisayarların, ağların ya da elektronik ortamların araç olarak kullanıldıkları ya da bir hedef olarak maruz kaldıkları hukuka aykırı fiiller*" olduğunu ifade etmiştir[101].

Avrupa Ekonomik Topluluğu Uzmanlar Komisyonu'nun Mayıs 1983 yılında yapılan toplantısında bilişim suçları, "*bilgileri otomatik işleme tabi tutan veya verilerin nakline yarayan bir sistemde gayri kanuni, gayri ahlaki veya yetki dışı gerçekleştirilen her türlü davranış*" olarak tanımlanmıştır[102].

Yukarıda tanımlardan da yola çıkarak üç görüş ileri sürülmüştür. İlk görüş bu suçların ekonomik suçlar olduğu, ikinci görüş bilgisayardan anlayan, teknolojisini bilen ve bunları uygulayan kişilerin gerçekleştirdikleri eylemler olduğunu, üçüncü ve son görüş ise yukarıda Avrupa Ekonomik topluluğunun Mayıs 1983 yılında belirttiği görüştür[103].

### 6.3. Tarihsel Gelişimi

Yukarıda bilgisayara ilişkin bilgiler verdiğimiz bölümünde açıkladığımız üzere, transistörlerin yerine tümleşik devrelerin bulunmasıyla bilgisayarlar küçülmüş aynı zamanda maliyetleri de azalmıştır. Bu sayede birçok kişinin bilgisayar sahibi olabilmesinin önü açılmıştır. Buna paralel olarak ticari alanda da yaygınlaşan bilgisayarlar, ticari işletmelerde kullanılmış, eski yöntemler terk edilmiştir. Buna bir de 1990'lı yıllarda internetin herkesin kullanıma açılması eklenince bilgisayar kullanıcılarının sayıları inanılmaz boyutlara ulaşmıştır. Bu şekilde gelişen teknolojik gelişmeler beraberinde bir çok farklı suçu da getirmiştir[104].

Artık günümüzde neredeyse bütün resmi veya özel kurumların internete bağlı olarak çalışmaları veya kendi bilişim ağlarıyla işlem yapmaları, bu alanda suç işleyen faillerin oturdukları yerden, aynı zamanda yakalanma riskleri de çok az olacak şekilde suç oluşturan eylemlerini gerçekleştirebilmelerine olanak tanımaktadır. Örneğin önceki senelerde, güvenliği en üst seviyede tuttuğu bilinen Pentagon,

---

100 Eker, Ö. U. (2006). Türk Ceza Hukuku'nda Bilişim suçları" Eski TCK Bağlamında Hukukumuzda Yer Alan İlk Düzenlemeler ve 5237 Sayılı Yeni Türk Ceza Kanunu'nun İlgili Hükümlerinin Yorumu. TBB, Y. 19, S. 62
s.105.

101 Turan, M. (2016). *Bilişim Hukuku*. Ankara: Seçkin Yay. s. 43-44.

102 Karagülmez, age. s.56.

103 Tulum, İ. (2006). *Bilişim Suçları İle Mücadele*. (Yayımlanmamış Yüksek Lisans Tezi). Süleyman Demirel Üniversitesi/Sosyal Bilimler Enstitüsü. s. 20-21.

104 Dülger, age. s. 111-112

NASA, NATO vb. bir çok kurumun bilişim sistemlerine sızılarak çok değerli veriler ele geçirilmiş veya sistemlerin işleyişleri geçici bir süreyle de olsa engellenmiştir[105].

Bilişim alanında işlenen suçlarda iki önemli dönem bulunmaktadır. İlki kişisel bilgisayarların yaygın olarak kullanılmaya başlandığı dönem, ikincisi ise internetin ortaya çıktığı ve kullanıldığı dönemdir.

Bilişim suçları ise 1960'lı yıllarda kendisini göstermektedir. Bu tarihten önce bilinmeyen bir olgu olan bilişim suçları, bu yıllarda bilgisayar sabotajı, bilgisayar manüpülasyonu, bilişim sistemlerinin hukuka aykırı kullanımları ve bilgisayar casusluğu gibi kavramların ortaya çıkması ile ilk bilişim suçlarının örnekleri olarak kabul edilmektedir. Bu çerçevede bilinen ilk bilişim suçu 18 Ekim 1966 yılında bir gazete yayımlanan "bilgisayar uzmanı banka hesabında tahrifat yapmakla suçlanıyor" başlıklı haber ile gün yüzüne çıkmıştır. Bu doğrultuda ABD hukukunda bu alanda ilk hukuki düzenlemeler yapılmaya başlanmıştır. 1970'li yıllardan sonra bu alanda hukukçular tarafından çalışmalar yapılmış, konuya ilişkin kavramlar yerlerini almaya başlamıştır. 1980'li yıllarda kişisel bilgisayarların kullanılmasına başlanmasıyla bilişim suçlarında da önemli değişiklikler meydana gelmiştir. Bu bağlamda hastane bilgisayarlarına erişilerek kişisel gizliliğin ihlal edilmesi gibi yeni suç modelleri meydana gelmiştir[106].

1994'lü yıllarda özellikle internetin bulunmasıyla birlikte hukuka aykırı eylemler artmıştır. Özellikle virüs ve truva atı verilen zararlı yazılımların bilişim sistemlerini çökertmesi, içeriğinin öğrenilmesi, değiştirilmesi gibi suçların işlenmesiyle beraber hukuki alanda yeni çalışmalar yapılmasını kaçınılmaz kılmış ve bu doğrultuda çeşitli ülkelerce hukuki düzenlemeler yapılmıştır[107].

1990'lı yılların sonlarına doğru organize suç ve terör örgütlerinin bu alanı kullanmaları sebebiyle ulusal hukuk haricinde uluslararası hukuk alanında da bu konuda çalışmalar yapılması zorunluluğunu doğurmuştur. Bu çerçevede 23 Kasım 2001 yılında Macaristan'da ASSS imzaya açılarak yürürlüğe girmiştir. Bu sözleşme ülkemiz tarafından 10 Kasım 2010 tarihinde imzalanmış, 22 Nisan 2014 tarih 6533 sayılı kanun ile onaylanması uygun bulunarak 02 Mayıs 2014 tarih 28988 sayılı RG'de yayımlanarak yürürlüğe girmiştir.

---

105 Dülger. age. s. 112.

106 Aydın, age. s.13; Dülger, age. s. 113-114.

107 Dülger, age.s.115.

Bilişim alanı ülkemizde ilk olarak 1991 yılında 3756 sayılı yasayla 765 sayılı eski TCK'ya eklenen "Bilişim Alanında Suçlar" ile kendisini göstermektedir. Bu düzenlemeyi 1995 yılında 4110 sayılı yasayla FSEK'e bilgisayar programlarının eklenmesi takip etmiş, 2004 yılında 5070 sayılı Elektronik İmza Kanunu ile de yeni suç tipleri oluşturulmuştur. 5237 sayılı TCK'da ayrı bir bölüm olarak düzenlenen bilişim suçları[108], 2007 yılında 5651 sayılı yasa ile internet kişilerinin sorumluluklarının tayin edilmesi, buna bağlı bir dizi yönetmelik, vb idari düzenleyici işlemler, son olarak da TBK, TTK ve HMK'da bilişim alanına ilişkin yaptığı düzenlemeler birbirlerini izlemiştir [109].

[108] Pallı, age. s. 27-28, Dülger, age. s.116.

[109] Dülger, age. s. 116;

# İKİNCİ BÖLÜM
# BİLİŞİM SUÇLARININ İŞLENME ŞEKİLLERİ

## 1. GENEL OLARAK

Bilişim, yapısı ve konumu itibariyle saldırılara açık bir alandır. Çok hızlı gelişen bilişim alanının saldırılara açık olmasının başlıca nedenlerinden birisi, ağlarının yapısının büyük, parçalı, dağınık ve karmaşık olmasıdır[110].

Bilişim suçları diğer suçlara nazaran çok kısa bir zaman dilimi içerisinde gerçekleşip arkasında çok az sayıda ipucu bırakmakta, bu sebeple failin tespiti güç olmaktadır. Bununla birlikte, bilişim alanında işlenen suçlar çok büyük zararlara da neden olmakta, aynı doğrultuda bir bilişim sistemine verilen zararla bazen toplumun bütün üyeleri zarar görebilmektedir.

Gerçekten de bilişim alanı çok hızlı bir gelişme sürdürmektedir. Eskiden sadece çok az sayıdaki bilgisayarda bulunan internet erişimi şimdilerde neredeyse tüm cihazlarda mevcuttur. Başta telefon olmak üzere saatlerde dahi artık internet erişimi mevcuttur.

Bilişim alanında, suçu oluşturan maddi unsur farklı şekillerde karşımıza çıkabilir. Bu hareketler bazen bir virüs, bazen truva atı, mantık bombası şeklinde olabileceği gibi karşı tarafın aldatılması şeklinde de olabilir. Bilişim teknolojisindeki bu hızlı gelişim nedeniyle her geçen gün yeni bir bilişim suçu işleme şekli ortaya çıkmaktadır. Bu sebeple aşağıda en sık karşılaşılan işlenme şekillerini özellikle konumuz olan TCK'nın 244. maddesini oluşturabilecek olanları inceleyeceğiz.

## 2. İŞLENME ŞEKİLLERİ

### 2.1. Truva Atı (Casus Yazılımlar-Trojan Horse)

Truva atı adını, Yunan Mitolojisinde Troyalılar ile Akhalıların yapmış oldukları savaşta, Troyalılara masum bir hediye gibi görünen büyük tahta attan almaktadır. Tahtadan yapılmış büyük bir at Akhalılar tarafından savaştan çekiliyor gibi yapılarak Troyalılara hediye verilir. Savaştan çekildiklerini gören Troyalılar

[110] Orta, age. s. 74.

kazandıklarını düşünerek zaferi kutlamaya başlarlar. Gece olunca hediye edilen atın içerisinden çıkan Yunan savaşçıları şehrin kapılarını açıp dışarıda bekleyen Yunan savaşçılarının içeriye girmesini sağlayarak, savaşı kazanmalarına büyük bir katkı sağlamıştır[111].

Truva atı zararlı yazılımı da yukarıda belirtilene benzer şekilde çalışmaktadır. Bir uygulama programı içerisine zararlı bir yazılım olan truva atı eklenir. Bilgisayar kullanıcısı tarafından sisteme uygulama programı indirilmekle beraber program içerisinde çok küçük yer kaplayan truva atı zararlı yazılımı da yüklenecektir. Bu halde sistem sahibinin istemediği ve tahmin etmediği ve isteği olmaksızın genellikle kötü amaçlı faaliyette bulunan yazılım da bilgisayara yüklenmiş olacaktır. Truva atı kendisini bir oyun gibi zararsız gösterir. Görünümü ve ilk aktivitesi zararsız bir uygulama gibi çalışarak gösterir ancak çalıştığı zaman çok büyük tehlikelere yol açabilir[112].

Bu yazılım yukarıda belirtildiği üzere kendisini bir uygulama programı içerisinde gösterebileceği gibi internetten indirilen müzik, oyun ya da herhangi bir dosyanın içerisinde de gösterebilir. Yine aynı doğrultuda elektronik postanın gönderilmesi yoluyla da bu yazılım kullanıcılara ulaşabilir. Bu zararlı yazılımın yüklenmesiyle bu yazılımı gönderen kişinin mağdurun tüm bilgisayarı üzerinde hakimiyet kurmasına sebep olur[113]. Bununla birlikte truva atları diğer kötü yazılımlar gibi kendi başlarına çalışmaz, işlem yapamazlar. Bu zararlı yazılım ancak mağdurun programı çalıştırmasıyla harekete geçer[114].

Truva atı iki kısımdan meydana gelir. İlki hedefteki bilgisayara yüklenmiş olan zararlı yazılımın çalışması yani sunucu kısmı, ikincisi ise karşı taraftaki bilgileri çekmeye ya da karşı taraftaki sisteme komut verme yani istemci kısmıdır[115].

Bu yazılımın kullanım alanları çok geniştir. Bu zararlı yazılım ile bu yazılım sahibi ya da kullanıcısı bilişim sisteminde hemen hemen her türlü eylemi

---

111 Doğan, R. (2014). *5237 Sayılı Türk Ceza Kanunu'nda Bilişim Suçları*. Ankara: Adalet Yay. s. 23; Dülger, age. s.120; Turhan, O. (2006). *Bilgisayar Ağları İle İlgili Suçlar (Siber Suçlar).* Başbakanlık Devlet Planlama Teşkilatı Müsteşarlığı Hukuk Müşavirliği. Uzmanlık Tezi. Ankara. s. 47.

112 Dülger, age. s. 120; Çakır, H., Kılıç, M. S.,(2014). *Güncel Tehdit Siber Suçlar.* Ankara: Seçkin Yay. s. 28; Balcı, age. s. 30.

113 Dülger, age. s. 120; Çakır, Kılıç, age. s. 28.

114 Akarslan, H., (2015). *Bilişim Suçları,* 2. Baskı, Ankara: Seçkin Yay. s. 94.

115 Güngör, age. s. 62; Çakır, Kılıç, age. s. 29; Boğa,U. (2011). *Bilişim Suçlarıyla Mücadele Yöntemleri*. RTÜK Yayımlanmamış Uzmanlık Tezi. Ankara. s. 35.

gerçekleştirebilmektedir. CD-ROM'u açıp kapatabilir, sisteme ekranına istediği yazıları gönderebilir, istediği dosyaları silebilir, sistemi kapatabilir, istediği bilgileri kendi bilgisayarına internet vasıtasıyla transfer edebilir, istediği bir uygulamayı bilgisayara yükleyebilir, hedef bilgisayarın giriş şifresi, kredi kartı şifresi gibi önemli bilgiler ele geçirilebilir[116]. Bu sebeple bilişim alanındaki suçların büyük bir çoğunluğu bu yöntemle işlenmektedir[117]. Bu yöntemle bankaların bilişim sistemlerine girilebilmekte, ülkelerin savunma sanayilerine, askeri kuruluşlarına sızılabilmektedir[118]. Truva atı yöntemi her ne kadar bilişim virüsü veya solucanlarına benzese de, virüs ve solucanlardan farklı olarak kendi kendilerine çoğalarak yayılma özelliklerinin olmaması ve zararsız bir yazılım gibi görünebilmeleri sebebiyle bunlardan ayrılır[119].

Truva atının atası "IBM Christmes Tree" virüsü olarak anılmaktadır. 9 Aralık 1987 tarihinde Almanya'da üniversite okuyan öğrencilere "cristmas" adlı bir elektronik posta gönderilir. Bu elektronik postada "bırakın bu exec işleşin ve keyfinize bakın" yazar devamında tırnak işaretiyle oluşturulmuş noel ağacı resmi yer alır. Resmin altında "bu dosyada gezinmek hiç de eğlenceli değil sadece Chritmas yazın" şeklinde mesaj yer alır. Christmas yazanlar noel ağacı ile ödüllendirilirler. Bu dosyayı silmeye çalışanlar bilgisayarı tekrar açtıklarında silemediklerini anlarlar. Bu program her ne kadar noel ağacı çiziyor gibi gözükse de aslında bilgisayarlardaki elektronik posta adreslerine girip orada bulunan kişilere de aynı şekilde bir kopya göndermiştir. Bu e-posta IBM şirketinin özel elektronik e-postasına da ulaşmış ve şirketin ağdaki işleri durma noktasına gelmişti. İşte bu yüzden bu virüsün adı "IBM Chritmas Tree" olarak anıldı ve bu truva atının ilk kullanımı olarak tarihe geçti[120].

Truva atı yöntemini birçok ülke de kullanmıştır. Örnek olarak, ABD ve İsrail tarafından ana belleğinde promis adlı yazılımı içeren bir bilişim sisteminin Ürdün'e satılması gösterilebilir. Bu yöntemle Ürdün'ün Filistin hakkında, özellikle Filistin ve Filistin Kurtuluş Örgütü hakkındaki çok sayıda dosya ABD ve İsrail'in eline geçmiştir[121].

---

116 Doğan, age. s. 24; Güngör, age. s. 62.
117 Dülger, age. s. 120.
118 Dülger, age. s. 120.
119 Dülger, age. s. 120.
120 Güngör, age. s. 62-63; Boğa, age. s. 36-37.
121 Yaycı, age. s. 30; Dülger, age. s. 120.

### 2.2. Çöpe Dalma (Scavengig)

Çöpe dalma, çöplenme veya atık toplama olarak da adlandırılır. Bu yöntemde, bilişim sisteminde gerçekleştirilen bir veri işleminin ardından kalan bilgiler toplanmaktadır. Bu bilgiler öncelikle bir karbon kağıdından, bilgisayar çıktısının çevreden toplanmasıyla, çöpe atılan kağıt veya mürekkep şeridi gibi materyaller üzerinde kalan bilgilerin toplanmasıyla elde edilebilir. Diğer bir yöntem ise bilişim sisteminin belleğinde ve ihtiyaç duyulmadığı için silinen bilgilerin gelişmiş yöntemlerle tekrar geri getirilmesi yoluyla elde edilebilir[122].

Çöpe atılan kağıt veya mürekkep şeridinden toplanan bilgiler fazla bir bilgi ya da teknolojiye ihtiyaç duyulmadan gerçekleşirken, ikinci yöntemde bir programlanma ve bilişim sistemine direkt ya da ağ ile ulaşılmasına ihtiyaç duyulmaktadır. Bir bilişim sistemindeki ya da bir bilgisayarın içerisindeki bir dosyanın gerçekten silinebilmesi için, üzerine yeni bir bilginin yazılması gerekir. Bu sebeple bazı veri depolama ünitelerinde silinmiş bazı bilgiler kalabilmektedir. İşte bazı özel programlarla bu silinmiş bilgiler yeniden elde edilebilmektedir, bu sebeple bu yöntem biraz zor ve karmaşık bir yöntemdir[123].

Bu yöntemle kişisel, ticari, askeri, istihbari sırlar elde edilebilir. Örneğin, 1980'li yıllarda başta Amerikan Hava Kuvvetleri bilgisayarları olmak üzere MIT, Pentagon ve Beyaz Saray'ın bilgisayarlarından birçok veri bu yöntemle elde edilmiştir[124].

### 2.3. Gizlice Dinleme (Eavesdropping)- Ağı Koklama (Sniffing)

Teknolojinin hızlı ilerlemesine paralel olarak güvenlik açıkları da giderek artış göstermektedir. Özellikle iki cihazın birbirleriyle haberleşmesinde bu güvenlik açıkları önem kazanmaktadır[125].

Bir veri, ağ üzerinden başka bir yere taşınırken her an kopyalanma, yok olma veya değiştirilme tehlikesiyle karşı karşıyadır. Verileri bu şekilde ele geçirme yöntemlerinden bir diğeri de gizlice dinleme yöntemidir. Gizlice dinleme, bir

---

122 Dülger, age. s. 134; Doğan, age. s. 22; Güngör, age. s. 59; Çakır, Kılıç, age. s. 29; Çakır, H. (2013). İnternet, Etik ve Bilişim Suçları. s. 11. http://android.eng.ankara.edu.tr/wp-content/uploads/sites/656/2017/10/9_%C4%B0nternet-Etik-ve-Bili%C5%9Fim-Su%C3%A7lar%C4%B1_H%C3%BCseyin-%C3%87AKIR.pdf (erişim tarihi: 05/02/2018)

123 Güngör,age. s. 60; Doğan, age. s. 22.

124 Ayrıntılı bilgi için bkz. Güngör, age. s. 60; Çakır, Kılıç, age. s. 29.

125 Orta, age. s. 82.

bilgisayar ağındaki veriye iletişim halindeyken erişme şeklinde olabileceği gibi bilişim sisteminin yaydığı elektromanyetik dalgaların yakalanması ve ekran görüntüsüne dönüştürülmesi şeklinde de olabilir. Bu yöntemde araya konulacak yükselteçler çok uzaklardan bu dalgaları yakalayabilmekte ve kullanıcısına avantajlar sağlayabilmektedir. Aynı doğrultuda bilgisayarlar arası veri naklinde kullanılan ağa fiziki saldırı yapılmak suretiyle de veriler gizlice ele geçirilebilmektedir. Bu şekilde veri trafiğinin aksamasına engel olunmayacak şekilde verinin bir kopyası, ağı gizlice dinleyen yani koklayan kişinin bilgisayarına yönlendirilmektedir[126].

Bu yöntem en çok bilgisayar ekranlarının yaydığı elektromanyetik dalgaların araya konulacak yükselteçler vasıtasıyla yakalanarak, kendi ekranlarına yansıtılması ile yapılmaktadır. Bu şekilde çok büyük bilgiler ele geçirilmektedir.

Bu yöntem, başka suçların işlenmesine aracı olabileceği gibi bizatihi dinleme saikiyle yani iletişim verilerinin ele geçirilmesi amacıyla da yapılabilir. Bu yöntem, telefon dinlemelerine de benzemektedir[127].

### 2.4. Bilgi ve Veri Aldatmacası (Data Diddling)

Veri aldatmacası, sisteme veri girilirken yanlış bir verinin girilmesi, veriler girildikten sonra değiştirilmesi ya da kasten bazı verilerin bırakılması halidir[128].

Bilgi ve veri aldatmacaları, bilişim alanında işlenen suçlarda basit, güvenli ve yaygın bir yöntemdir. Bu yöntemi işleyen kişinin ortaya çıkmasının zor olması nedeniyle en çok kullanılan suç işlenme yöntemlerinden bir tanesidir. Bu yöntemi kullanabilmek için kişinin ileri düzeyde bilgisayar bilmesine gerek yoktur. Bu yöntemle, bazı verilerin tahrif edilmesi, başka bir veriyle değiştirilmesi, ek veri yüklenmesi, bazı verilerin silinmesi veya kontrol süreçlerinden kaçırılması gibi eylemler gerçekleştirilebilir[129]. Bu hareketlere örnek olarak, disketlerin, sabit disklerin ya da manyetik bantların önceden hazırlanan kopyasıyla değiştirilmesi gösterilebilir[130].

Güney Almanya'da işçi bulma dairesinde çalışan bir memur, çocuk zammı ödenmesine ilişkin düzenlenen evrakta kendi imzası ile beraber bulunması gereken başka bir memura ait imzayı taklit etmiştir. Bu şekilde fazlaca bir meblağı kendisine

---

126 Orta, age. s. 82; Akarslan, age. s.102; Güngör, age. s. 60.

127 Orta, age. s. 83;

128 Aydın, age. s. 48; Doğan, age. s. 22; Yaycı, age. s. 33; Güngör, age. s. 60; Çakır, Kılıç, age. s. 27.

129 Doğan, age. s. 22; Güngör, age. s. 61; Çakır, Kılıç, age. s. 29.

130 Çakır, Kılıç, age. s. 29; Yaycı, age. s. 33-34.

veya bir yakınının hesabına aktarmıştır. Suçu kapatabilmek için ise bilgisayar tarafından hazırlanan kontrol fişlerinin üzerilerinde değişiklik yaparak bir takım verileri silmiştir[131].

Bu suç, bilgisayar programını yapan, nakleden, kaydeden, şifreleyen, denetleyen kısacası bilgisayarla çalışma imkanı olan herkes tarafından işlenilebilir[132]. Bu zararlı yazılım ile yapılan eylem TCK'nın 244. maddesinin 2. fıkrasındaki suçu oluşturacaktır[133].

### 2.5. Gizli Kapı (Trap Doors)

Gizli kapıya, hile kapısı, tuzak kapısı, arka kapı veya açık kapı da denilebilir. Gizli kapı, bilişim sisteminin yazılımını yapan kişi tarafından, yazılımın içerisine gizli bir şekilde yerleştirdiği virüs yazılımıdır. Bu sebeple yazılımı yapan kişi tarafından bilerek bu şekilde açık bırakılmıştır. Bu program ile virüsü yerleştiren kişi uzaktan erişim yöntemiyle yakalanmadan bilişim sistemine erişebilmektedir[134].

Öncelikle bu şekilde bir açık bırakan yazılımcı sistemde ileride çıkabilecek olumsuzluklara karşı müdahalede bulunabilmek için bu şekilde bir açık bırakmıştır. Bu sebeple gizli kapılar hataları gidermek için konulduğu zaman meşrudur. Tabi yazılımın sıkıntısız çalışması halinde bu gizli kapıların temizlenmesi gerekir. Bazı durumlarda bu gizli kapılar hatayla ya da ileride kullanılmak üzere kapatılmazlar. Kapatılmayan gizli kapılar kötü niyetli kişiler tarafından kullanılabilirler[135].

### 2.6. Sosyal Mühendislik

Bilişim suçlarında çok karşılaşılan yöntemlerden bir diğeri de sosyal mühendisliktir. Kişinin içerisinde bulunduğu zaafları kullanarak istenilen bilgiyi ya da veriyi elde etmeye sosyal mühendislik denir. Diğer bir deyişle, insanlar arasındaki iletişimde karşı tarafı ikna ya da başka bir şekilde yanıltıp güvenlik süreçlerini atlatma halidir. Bazı sistemlerden önemli bilgileri ele geçirmek teknikten çok sosyal mühendislik ile mümkündür. Bu teknik ile normalde tanımadıkları insanlara yapmayacakları şeyleri ikna, inandırma veya hile yöntemleri kullanılarak yaptırma

---

131 Güngör, age. s. 61.

132 Doğan, age. s. 23.

133 Uçar, H. (2014). *5237 Sayılı Türk Ceza Kanunu'nda Bilişim Suçları. (*Yayımlanmamış Yüksek Lisans Tezi*).* Çankaya Üniversitesi/Sosyal Bilimler Enstitüsü. Ankara s. 22.

134 Çakır, Kılıç, age. s. 32.

135 Güngör, age. s. 65.

ya da bilgi elde etmek mümkündür. Ancak o bilginin elde edilebilmesi için karşı tarafın etkilenmesi ve inandırılması gerekir[136].

Bilişim suçlarında failler isteklerini akıllıca ortaya koyarak kuşku uyandırmayacak şekilde karşı tarafın güveninden yararlanır. Bu sebeple sosyal mühendislik uzmanları daha çok karşı tarafın dış yüzü olarak adlandırılan yani servis elemanları, çağrı merkezi elemanları, müşteri hizmetleri personeli gibi hareket ederek kişilere ulaşıp onlarla iletişime geçerler. Onlardan normalde vermemeleri gereken bir takım bilgileri almaya çalışırlar[137].

Sosyal mühendislik yukarıda da belirtildiği üzere dört aşamalıdır. İlk aşamada kişi, karşı taraf hakkında bilgiler toplar. İkinci aşamada, bu topladığı bilgiler doğrultusunda karşı taraf ile iletişime geçer ve bu bilgileri hem kullanır hem de amacı doğrultusunda kullanabileceği araçları tespit eder. Üçüncü aşamada kişi artık elindeki bilgiler ile uygulamaya geçerek ulaşmak istediği bilgilere ulaşır ve son aşamada artık bu bilgiler istismar edilerek istenilen amaçlara ulaşılabilir[138].

Örneğin, bir hacker, şirket çalışanı gibi hareket edip çağrı merkezini arayarak şirket ağına dahil olabilir. Bunun için öncelikle çağrı merkezindeki çalışanı etkilemesi ve ikna etmesi gerekir[139]. Sosyal mühendisliğin bir başka yöntemi de kurum çalışanlarıyla iyi arkadaş olmak, kurum çalışanı gibi kurumun içerisine sızmak, teknik servis gibi davranılarak kurumdan arıyormuş gibi görünüp bilgi toplamaktır[140].

Sosyal mühendislik bu yönüyle telefon dolandırıcılığına çok benzer. Bir telefon dolandırıcısı ilk başta mağdur hakkında onun güvenini kazanabilmek için gerekli araştırmalar yapar. Bu araştırmalarda eşinin adı, oğlunu adı, oturduğu yer, T.C. Kimlik numaraları gibi bilgileri temin eder. İkinci aşamada bu bilgiler ile mağdur ile iletişime geçer. Mağdur hakkında bildiklerini söyleyerek karşı tarafın güvenini kazanır ve son aşamada artık istediği şeyleri özellikle de maddi menfaatleri mağdurdan temin etmeye çalışır. Benzer durum failin kendisini polis veya savcı olarak tanıtması ve mağdurdan maddi menfaat temin etmesi halinde de söz konusudur.

### 2.7. Salam Tekniği

136 Orta, age. s. 76.
137 Orta, age. s. 76.
138 Akarslan, age. s. 104-105.
139 Orta, age. s. 76.
140 Çakır, Kılıç, age. s. 32.

Bu teknik genellikle bankalarda yaygın olarak kullanılan bir yöntemdir. Bu yöntemle banka hesaplarında bulunan küsuratlar ya da çok düşük meblağlar failin ya da bir yakınının hesabına aktarılmaktadır. Aktarılan miktarlar çok düşük olması nedeniyle mağdur tarafından anlaşılmayabilir. Failin farklı farklı kişilerden temin edeceği bu miktarların kendi hesabında birleşmesi halinde ise çok büyük miktarlar ortaya çıkacaktır. Bu yöntemde genellikle truva atı yazılımının çeşitleri ya da benzer işleve sahip yazılımlar kullanılmaktadır[141].

Bir banka çalışanının milyonlarca mevduat hesabında dört ayda bir yapılan faiz ödemelerini bir yazılım kullanılarak yuvarladığı, yani bir doların 0.0075 üstünü bir üst cente kişilerin hesaplarına, altını da aşağı yuvarlanmakta ve bankanın hesabına geçtiğini tespit eden banka memurunun sistemin işleyişini değiştiren bir yazılım yaparak aşağı yuvarlanan miktarların banka hesabına değil de kendi açtığı bir hesaba gitmesini sağlayarak üç yıl içerisinde milyonlarca dolar hukuka aykırı yarar sağladığı tespit edilmiştir[142].

Bu zararlı yazılım ile yukarıda belirtilen örnekten de anlaşılacağı üzere 5237 sayılı TCK'nın 244. maddesinde yer alan suçu oluşacaktır[143].

### 2.8. Mantık Bombası (Logis Bombs)

Mantık bombası, bilinen en eski ve basit bir yazılım türüdür. Kökeni 1960'lı yıllara kadar dayanır[144]. Truva atı yazılımın bir türüdür. Bilişim sistemlerini bozmak, şaşırtmak veya felç etmek için bilgisayara mantık dışı veya yapılan işlemin aksine durmadan bilgi göndermek suretiyle meydana gelir[145].

Başka bir tanıma göre mantık bombaları, aynen truva atı gibi yararlı bir programmış gibi görünerek sisteme dahil olmakta ve sistem içerisinde normal şekilde çalışarak sisteme hiçbir zarar vermemektedir. Ancak saatli bomba gibi çalışıp[146] belirli bir olayın meydana gelmesi ya da belirli bir tarihin yaşanmasıyla faal hale gelirler. Belirlenen tarih gelmeden aktif hale gelmeyeceği için o tarihe kadar herhangi bir zararı yoktur. Bu yöntemle fail, istihbarat, şantaj, hırsızlık, zarar verme gibi suçları işleyebileceği gibi sırf eğlence olsun diye de eylemlerini yapabilir[147].

---

141 Dülger, age. s. 121.
142 Dülger, age. s. 121.
143 Uçar, age. s. 22.
144 Orta, age. s. 81.
145 Doğan, age. s. 27; Balcı, age. s. 32.
146 Aydın, mantık bombası ile saatli bomba yazılımlarını farklı farklı ele almış fakat aynı yapıya sahip olduklarını ifade etmiştir. bkz. age. s. 52.
147 Dülger, age. s. 127; Orta, age. s. 81.

Mantık bombası sistemin işleyişine zarar vermekte, meydana getirdiği zararlar yıkıcı olabilmektedir. 1999 yılında ortaya çıkan Çernobil virüsü bu konuya örnek teşkil eder. Bir bilişim konferansında yararlı bir program olarak dağıtılmış kısa sürede ABD, Rusya, İngiltere, İsrail, İsviçre, İsveç, Avusturya, Avustralya, Şili gibi ülkelere ulaşmıştır. Bu yazılım her ayın 26'sında harekete geçer ve sistemlere kullanılamayacak şekilde zarar verir[148].

Bir başka örnek de 2002 yılında Amerika'nın New Jersey eyaletinde yaşanmıştır. İşvereni ile arası iyi olmayan bir çalışan işten ayrılmadan önce sisteme zaman ayarlı bir kod yerleştirir, bu kod sistemin yazılımlarını ve satış bilgilerini siler. Bu olay nedeniyle şirket 10 milyon dolarlık zarar eder. Bu eylemi gerçekleştiren kişi de 41 ay hapse mahkum edilir[149].

### 2.9. Bilişim Virüsleri

Virüsler, kendi kendilerine kopyalanarak çoğalabilen ve kendi kendilerine çalışabilen programlardır. Küçük ve kısa bir yazılım olan virüslerin tespit edilmesi çok zordur. Her ne kadar küçük ve kısa bir yazılım olsalar da bilişim sistemlerini kullanılamayacak hale getirebilecek kadar güçlüdürler[150].

Bilişim virüsleri en çok karşılaşılan, en zarar verici ve en çok bilinen bilişim suçu yöntemidir. Virüsler, çok kolay çoğalabilirler. Sistemden sisteme, yazılımdan yazılıma, dosyada dosyaya kolaylıkla çoğalabilirler. Bu çoğalma işlemine virüs bulaşması denilmektedir[151].

Bilişim virüsü terimi ilk defa 1985 yılında Amerika'da bir üniversitede yüksek lisans tezinde tez danışmanının önerisi üzerine kullanılmıştır. Tezde bilişim virüsü "*kendisinin azıcık değiştirilmiş bir kopyasını içerecek şekilde değiştirmek yoluyla, diğer yazılımları enfekte edebilen bir yazılım*" olarak tanımlanmıştır[152].

Bilişim virüslerinin bir çok farklı türü olmakla birlikte, özellikle üç türü dikkat çekmektedir. Bunlar makro/mail virüsleri, dosya virüsleri ve boot virüsleridir. Makro virüsleri özellikle çok tehlikeli bir türdür. Metin dosyalarına saklanarak elektronik posta yoluyla bir çok bilişim sistemine bulaşabilirler. Günümüzde de en çok kullanılan ve en zarar verici virüs türü bunlardır[153].

---

148 Dülger, age. s. 127; Çakır, Kılıç, age. s. 29; Orta, age. s. 82.; Balcı, age. s. 32.
149 Orta, age. s. 82.
150 Dülger, age. s. 128; Doğan, age. s. 29; Balcı, age. s. 32.
151 Dülger, age. s. 128; Doğan, age. s. 29; Balcı, age. s. 32.
152 Güngör, age. s. 68-69; Dülger, age. s. 128.
153 Doğan, age. s. 29-30; Dülger, age. s. 129.

Tarihte belgelenen ilk virüs saldırısı 22 Ekim 1987 tarihinde olmuştur. Pakistanlı iki kardeş zarar verme amacı olmaksızın "brian virüsü" olarak tanımlanan virüsü meydana getirmişlerdir. Bu virüsü temizleyebilmek için çok büyük çaba harcanmış ancak temizlenebilmiştir[154].

Virüsler ile diğer bilişim suçlarının işlenme yöntemleri birbirlerine benzeseler de solucanlar, mantık bombaları ve truva atlarının aksine virüsüler kendi kendilerine çoğalabilir diğer programlara bulaşabilirler. Mantık bombaları, solucanlar, truva atları, şayet kendi kendilerine çoğalabilir olsalardı artık bunların da virüs programı olarak nitelendirilmeleri gerekecekti[155].

2011 yılında bir internet sitesinde yer alan bilgilere göre, virüsler yüzünden iş dünyasının 85 milyar dolarlık zarara uğradığı, en tehlikeli virüs olan Mydoom virüsü her ne kadar 2004 yılında ortaya çıksa da kim tarafından yazıldığının halen tespit edilemediği ve dünya çapında 38 milyarlık zarar verdiği ifade edilmiştir[156].

ABD merkezli bir sivil toplum kuruluşu 2012 yılının ilk çeyreği için bir rapor yayınladı. Bu raporda dünyadaki bilgisayarların yüzde 35,51'inin virüslü olduğu, bu virüslerin 2011 yılına göre üç puan azaldığı, yine de ürkütücü boyutlarda olduğu belirtilmiştir[157].

Bu zararlı yazılım, mantık bombasına benzer nitelikte TCK'nın 244. maddesinin ikinci fıkrasındaki verileri bozma suçunu oluşturacaktır.

### 2.10. Hukuka Aykırı İçerik Sunulması

İletişim ağları vasıtasıyla hukuka aykırı içerikler bilişim sistemlerine bulaşabilir. Bu içerikler şiddeti teşvik edici, ayrımcı, insan ticareti, çocuk pornografisi ve kişilik haklarına tecavüz eden içerikler olabilir. Bu yöntem çok karşılaşılan bir türdür. Bu yöntem web sayfaları, elektronik postalar, forumlar ve dosya paylaşımı ile gerçekleştirilebilir[158].

Özellikle çocuk pornografisi ile ilgili içeriklerin internetin yaygınlaşmasıyla beraber artış göstermesi ile bir çok ülke bu içeriklerin bulundurulmasını suç olarak yaptırım altına almıştır. Bu konuda örnek 2001 yılında yaşanmıştır. Buna göre, İngiliz polisi tarafından gerçekleştirilen operasyonda çocuk pornografisini diğer

---

154 Dülger, age. s. 129; Güngör, age. s. 69.

155 Doğan, age. s. 30.

156 https://shiftdelete.net/en-tehlikeli-10-bilgisayar-virusu-28544 (erişim tarihi: 10/02/2018)

157 http://www.hurriyet.com.tr/bilgisayar-kullanicilari-oltaya-geliyor-21226684 (erişim tarihi: 10/02/2018)

158 Dülger, age. s. 131; Güngör, age. s. s.75; Yaycı, age. s. 33.

kişilerin erişimine açan grup izlenmeye alınmış ve Türkiye'nin de aralarında bulunduğu on dokuz ülke ile işbirliği yapılarak bu kişiler yakalanmıştır[159].

### 2.11. İstem Dışı Alınan Elektronik Postalar (Spam)

İstem dışı alınan elektronik postalar son dönemlerde önemli bir sorun haline gelmiştir. Türkçe'de "istem dışı ileti" ya da "yığın ileti" terimleriyle ifade edilen[160] spamlar kısaca, istem dışı alınan e-postaları ifade eder[161]. UTÖ (Uluslar Arası Ticaret Örgütü) 1996 yılında spamı, bir bülten ya da haber grubu üzerinden ticari amaç taşımayan, forum konuları ile ilgili olmayan ve gönderilmesine açık bir şekilde izin verilmeyen reklam olarak tanımlamıştır[162].

Spamları gönderen kişiye spammer adı verilmiştir. Her türlü ticari, ideolojik veya pornografik duyuru yapmak isteyen kişiler spammerlara başvurarak geniş kitlelere ulaşabilirler. Spammerlar bu e-posta adreslerini, web siteleri, haber grupları, posta listeleri, forumlar, Usenet, yeniden iletilen e-postalar, sohbet odaları gibi yerlerden temin ederler[163].

Bir ürünün pazarlanması, reklamı ve pornografik içerikli reklam veya mesajların dünya çapında geniş kitlelere ulaştırılması amacıyla spamlar kullanılmaktadır[164].

Spammerların, kişilerin e-posta adreslerini sahibinin rızası dışında ele geçirmeleri kişinin manevi haklarına saldırı niteliği taşımaktadır. Aynı zamanda bu spamlarla meşgul olan insanların bu spamları silmeye çalışmaları bir hayli zamanlarını alacaktır. Amerika'da bir şirkete günde 1.8 milyon spam gelmesi sebebiyle şirketin hem büyük bir vakti gitmekte hem de masraf yönünden ek maliyetlerin ortaya çıkmasına neden olmaktadır. Aynı zamanda bu spamlarin internet üzerinden gönderilmeleri sebebiyle şirketin internet servis sağlayıcı kaynakları israf edilmektedir[165].

Bu şirkete günlük gelen e-postaların %40'ını spamlar oluşturmaktadır. Bu spamlar, şirketin en iyi hizmeti sunabilmesi için daha fazla yatırım yapmasına neden

---

159 Dülger, age. s. 131; Güngör, age s. 75; Yaycı, age. s. 33.

160 Orta, age.s 77; Doğan, age. s. 31.

161 Ünal, C., Şahin, İ. (2017). İstenmeyen Elektronik Postaların (SPAM) Filtrelenmesi İçin Bir Uzman Sistem Tasarımı ve Gerçekleştirilmesi. Polieknik Dergisi. Y. 2017 S. 20. s. 268; Soysal, T. (2007). Elektonik Posta Yoluyla Kişilik Haklarına Müdahaleden Doğan Hukuki Sorumluluk. Ankara Barosu Dergisi. Y. 2007. S. 1. s. 156.

162 Dülger, age. s. 129; Güngör, age. s. 72.

163 Çakır, Kılıç, age. s. 31; Güngör, age. s. 71-72.

164 Dülger, age. s. 130.

165 Orta, age. s. 78.

olacaktır[166]. Bununla birlikte spamlar, kişilerin e-posta kutularını da gereksiz yere doldurur. Bu spamler dolu olan e-posta kutusuna, bilgi sağlayıcı, yararlı herhangi bir e-posta geldiğinde otomatik olarak e-postanın reddedilmesi ihtimali söz konusu olduğundan kişilerin mağduriyet yaşamasına sebep olacaktır[167]. İşte bu gibi olumsuzlukların önüne geçebilmek için çeşitli ülkeler konuya ilişkin düzenlemeler yaparak bu tarz eylemleri yaptırım altına almışlardır. Bu konuda en kapsamlı ve etkili çalışmayı Avusturya ülkesi yapmış ve spamları açık bir hükümle yasaklamış ayrıca suçu işleyene 500 bin Şili'ye kadar ceza öngörmüştür[168].

Ülkemizde spam konusunu düzenleyen yasal bir düzenleme 2014 yılına kadar mevcut değildi. Elektronik ticareti düzenleyen yasa metninin 5 Kasım 2014 tarihinde Resmi Gazetede yayımlanarak yürürlüğe girmesiyle spamlar mevzuatımıza girmiş oldu. Bu kanun'un 6. maddesinde kişilere ticari amaçlı gönderilen e-postalarda kişilerin önceden onayının alınması şartı getirildi. Bu onayın yazılı olması gerektiği ayrıca kanunda belirtildi. Bu madde ile spamı doğrudan yasaklayan bir hüküm Türk Ticaret Kanunu'nda yerini aldı[169]. Bu kanun haricinde spamlar herhangi bir yerde bahsedilmemektedir. Fakat yasalarda açıkça belirtilmese de haksız rekabet, Medeni Kanun ve Tüketicinin Korunması Hakkında Kanun hükümlerine göre konunun çözümlenmesi mümkün olabilir. Gönderilen e-postanın içerisinde tehdit, hakaret ya da yasal olmayan diğer propagandaların bulunması halinde Türk Ceza Kanunu ve diğer ceza içeren yasalar doğrultusunda işlem yapılabilir. Aynı zamanda istem dışı alınan e-postalar bilişim sistemlerini engellemesi halinde TCK'nın 244. maddesinde yazılı cezai müeyyidenin uygulanması gerekecektir[170].

Spamlardan korunmanın en iyi yolu kişisel bazda alınacak önlemlerdir. Spam mesajlarına cevap verilmemesi ve bu mesajların açılmadan silinmesi bu konuda alınabilecek en iyi önlemlerdendir[171]. Bir diğer yöntem de "blacklisting" adıyla bilinen bloklama yöntemidir. Bu blacklisting kara liste olarak da bilinilir. Bu liste, spam gönderen serverlara karşı önlem almak için IP'lerin tutulduğu bir listedir. Bu yöntem ile 1,8 milyar e-posta kutusu spamlerden korunmaktadır. Spam gönderen bu

166 Güngör, age. s. 72-73.
167 Orta, age. s. 78.
168 Yaycı, age. s. 35; Dülger, age. s. 130.
169 Orta, age. s. 78.
170 Kurt, age. s. 72.
171 Dülger, age. s. 131.

tür sitelerin şikayet edilmesi halinde hızlı bir şekilde listeye alınır ve spamların kesilmesi mümkün hale gelir[172].

Yapılan bir araştırmada, 2007 yılında internet üzerinden gönderilen e-postaların yaklaşık %95'inin reklam amaçlı olarak gönderildiği ve istenmeyen e-posta oldukları belirtilmiştir[173].

### 2.12. Ağ Solucanları (Network Worms)

Ağ solucanları, virüsler gibi sisteme zarar verme zorunluluğu bulunmadan sistemin içerisinde dolaşabilirler. Virüsler aktif hale getirilinceye kadar hareketsiz kalırken solucanlar herhangi bir talimata gerek kalmaksızın aktif hale gelir ve eylemlerine başlayabilirler. Bu yönleriyle solucanlar virüslerden ayrılır. Solucanların kendi kendilerine çoğalabilme özellikleri vardır. İyi oluşturulmamış güvenlik duvarlarını aşarak sisteme girmekte ve eylemlerine başlayarak sistem içerisinde serbestçe dolaşabilmektedirler. Bu güvenlik duvarını tahmin edilmesi kolay şifreleri veya verileri kendi seçtiği şifreleri kullanıp deneyerek sonuca ulaşmaya çalışırlar. Üzerinde taşıdığı truva atı yazılımını sisteme bırakabileceği gibi doğrudan kendisi de yazılıma zarar verebilir. Ağ solucanları bunları yaparken arkasında bıraktığı izleri silmekte ve bu sebeple bulunmaları imkansız hale gelmektedir[174].

Ağ solucanlarını Truva atından ayıran başlıca özelliklerden ilki; truva atı sisteme bulaştığında aktif hale gelebilmesi için hangi programla bulaşmışsa o programın açılmasını bekler, program açılmazsa truva atı aktif hale gelmez. İkinci olarak, truva atı doğrudan işletim sistemine zarar verirken, solucanlar zarar vermez, sadece sistemde yapılan her şeyi sahibine iletir. Son olarak da truva atı, bulaştığı bilgisayarın ekranını kapatabilir, istediği programı açabilir, klavye ışıklarını yakıp söndürebilirken, solucanların bu tür özellikleri yoktur[175].

Ağ solucanları ilk olarak 2 Kasım 1988 tarihinde ABD'de ortaya çıkmıştır. O günkü veri iletim ağına yüklenen yazılım, ülkenin tüm bilim kuruluşlarına ve askeri araştırma merkezlerinin sistemlerine bulaşmış ve çok hızlı bir şekilde yayılarak sistemleri kullanılamaz hale getirmiştir. Bu ağ solucanın, yapılan araştırmaya göre

---

172 Doğan, age. s. 70.

173 Çakır, Kılıç, age. s. 31.

174 Dülger, age. s. 125-126; Akarslan, age. s. 93; Yaycı, age. s. 35; Güngör, age. s. 66; Boğa, age. s. 37; Turhan, age. s. 52-53.

175 Uçar, age. s. 24.

iki bin adet bilgisayara bulaştığı tespit edilmiş ve tahmini zararın 150.000 Dolar olduğu ifade edilmiştir[176].

### 2.13. Tavşanlar (Rabbits)

Tavşanlar, bilgisayar virüslerindendir. Adını aldıkları hayvanlar gibi çok hızlı bir şekilde üreyebilmektedirler. Bu yazılım bilişim sistemindeki işlemciye sürekli komutlar vererek işlemcinin normal işlemesini sağlayacak komutlar vermesini engellemekte ve giderek sitemin daha yavaş çalışmasına neden olmakta, en sonda da sistemi çalışamaz hale getirmektedir[177].

Tavşanları, virüslerden ayıran en önemli özellik, asalak özelliklere sahip olmamaları, kullanıcı veri kütüklerinin sonuna eklenmeleri ve kendi kendileri yetebilmeleridir[178].

Tavşanlar durmaksızın üredikleri için sistem durma noktasına gelir. Tavşanların, virüslerin aksine "pay-load"ı yoktur. Sadece sisteme girerek sistemin işleyişinin durmasına neden olmaktadır. Tavşanların harekete geçebilmesi için tavşan bulaştıran dosyanın açılması ve çalıştırılması gibi bir işleme gerek yoktur[179].

İngiltere'de yaşanan bir olayda bir üniversitenin bilişim sistemine yüklenen tavşan, sisteme durmaksızın "*sanırım benim çılgın olduğumu biliyorsunuzdur. Ayrıca bunalımdayım ve meydan okuduğunuzu görüyorum*" şeklinde yazılar yazması sebebiyle sistemi işlevsiz hale getirmiştir[180].

### 2.14. Bukalemunlar (Chameleon)

Bu yazılım truva atı yazılımı gibi aldatma ile sisteme dahil olurlar. Sistem içerisinde normal bir şekilde zararsız bir yazılım gibi davranıp o niteliklere sahipmiş gibi görünerek sistem içerisine dahil olurlar. Sisteme girdikten sonra gerçek yüzünü göstererek zarar verici eylemlerine başlarlar. Bu yazılıma kendisini saklamaktaki başarısı nedeniyle bukalemun adı verilmiştir[181].

Bukalemunlar, çok kullanıcılı sistemlerde sistem içerisindeki kullanıcıların adlarını ve şifrelerini, verileri taklit edebilme özelliği sayesinde gizli bir dosyaya kaydeder bundan sonra sistemin monitöründe "sistemin bakım için geçici bir süre

---

176 Dülger, age. s. 126.
177 Aydın, age. s. 52-53.
178 Aydın, age. s. 53; Doğan, age. s. 31.
179 Henkoğlu, T. (2014*). Adli Bilişim Dijital Delillerin Elde Edilmesi ve Analizi*. İstanbul: Pusula Yay. s. 190; Doğan, age. s. 31.
180 Dülger, age. s. 126-127.
181 Dülger, age. s. 127; Doğan, age. s. 31.

kapatılacağı" uyarısını verdikten sonra sistemin kapanmasının hemen ardından bu yazılım vasıtasıyla sistemde istenilen yere ulaşılabilir, eylemlerini gerçekleştirebilir[182].

### 2.15. Sistem Güvenliğini Kırma (Hacking)

#### 2.15.1. Genel Olarak

Hacking, bir şey elde etmek veya zarar vermek için bir bilişim sistemine yetkisiz erişime verilen addır[183]. Bilişim sistemine hacking yapan, sistemin işleyişine müdahale eden, yetkisiz erişen kişiye hacker denilmektedir. Hackerler kendilerini efsane zannedip üst düzey bilişim uzmanı olarak görürler. Hackerler şeytanca hareketleri severler. Davranışlarının temelinde duygusal bir yapı veya heyecan görülür çoğunlukla. Yaptıkları işleri bilişim sanatı olarak görürler. Yaptıkları eylemlere kendi imzalarını atmaktan hoşlanırlar[184]. Hackerlara nazaran daha üst düzey, donanımlı ve tecrübeli kişilere ise cracker denir. Crackerler diğerlerine oranla daha nitelikli faaliyetlerde bulunurlar. Bu kişilere bir bütün olarak bilişim korsanları adı verilmiştir[185].

Bilişim korsanları, internet üzerinden sistemlerin güvenliğinin kırarak, tespit edilene kadar sistem içerisinde istediği bilgiye ulaşabilmekte, istedikleri verileri ele geçirebilmektedir. Bu yöntemlerle hackerler, haberleşme özgürlüğü, özel hayatın gizliliğini ihlal gibi bir çok hakları ihlal edebildikleri gibi sistemin işleyişini de bozabilirler[186].

Bilişim güvenliğine yönelik saldırılar genellikle beş aşamalıdır. İlk aşama, saldırı yapılacak hedef hakkında gerekli bilgilerin toplanması aşaması yani keşif aşamasıdır. İkinci aşama tarama aşamasıdır. Bu aşamada bilişim güvenliğine saldırmak isteyen kişi sistemin zafiyetlerini belirlemeye çalışır. Üçüncü aşama erişim sağlama, sisteme sızma aşamasıdır. Bu aşamada hazırlıklar tamamlanmış, kullanılacak yöntem belirlenmiş ve hedefteki sisteme erişilmiştir. Dördüncü aşama erişime devam etme, kalıcılığı sağlama aşamasıdır. Bu aşamada saldırgan başkaları tarafından anlaşılmamaya ve sisteme sahip olmaya çalışır. Beşinci ve son aşama da izlerin temizlenmesi aşamasıdır. Saldırgan bu aşamada hedefine ulaşmıştır. Adli

---

182 Aydın, age. s. 51; Dülger, age. s. 127; Çakır, Kılıç, age. s. 31.

183 Karagülmez, A., (2014). *Bilişim Suçları ve Soruşturma-Kovuşturma Evreleri*. Genişletilmiş ve Gözden Geçirilmiş 2. Baskı, Ankara: Seçkin Yay. s. 87.

184 Karagülmez, age. s. 88.

185 Dülger, age. s. 122; Yaycı, age. s. 31.

186 Yaycı, age. s. 31.

bilişim görevlilerinin delil elde etmelerini engellemek ve yakalanmamak için arkasında bıraktığı izleri silmekle uğraşır[187].

Sistemin güvenliğini kırıp içeri girilmesi eylemini, diğer bilişim suçlarının işlenme yöntemlerinden ayıran en önemli özellik, herhangi bir yazılım kullanılmadan bizzat bilişim korsanlarının becerisine dayalı olarak yapılmasıdır. Her ne kadar yazılım kullanmasalar da bazen güvenlik duvarını kırmak için kombinasyon hesabını yapan yardımcı yazılımlar kullanabilirler. Bunun haricinde bilişim korsanının sistem içerisinde gezintisi ve verileri ele geçirmesi bizzat kendisi tarafından yapılır[188].

1997 yılında ABD'de bulunan bir havaalanının bilişim sistemine genç bir korsan girmiş ve havaalanı telefonlarını altı saat boyunca devre dışı bırakmıştır. Buna bağlı olarak havaalanı bir süre kullanılamamıştır. Aynı bilişim korsanı bir eczanenin bilişim sistemine girerek hastalarla ilgili bütün kayıtları ele geçirmiştir. Bu korsan ABD'de yargılanan ilk korsan olmuş ve iki yıl boyunca gözetim altında tutulma ve 250 saat sosyal hizmetlerde çalıştırılma cezası verilmiştir. Aynı şekilde 2008 yılında bir grup bilişim korsanı 40 milyon kredi kartı bilgilerini ele geçirmiştir[189].

Ülkemizde ise TBMM basın mensuplarına "tbmm.gov.tr" uzantılı bir e-posta gönderilir. Hatta bu e-posta meclis başkanlığından gönderilmiş gibi gösterilmiştir. Bu e-postada tüm milletvekillerimize geçmiş olsun, sistemin bu kadar basit ele geçirilmemesi gerektiği, bilgi işlem dairesinde çalışanların aforoz edilmesi gerektiği, bu karışık ortamda bu konunu önemsenmesi gerektiği, saygılarımla; MUSE (tırnak içerisinde yazılabilir)yazılmış ve basın mensuplarına gönderilmiştir[190].

### 2.15.2. Ethical Hacker

Bilişim alanının hızlı gelişimine paralel olarak bilişim alanındaki suçlar da bir hayli artış göstermiştir. Bilişim sistemini kullanan kişiler veya kurumlar bu suçlardan korunmak için mecburen yeni güvenlik arayışı içerisine girmişlerdir. Bu güvenlik önlemlerinin aktif halde çalışıp çalışmadığını denetleyerek test etmeye çalışmışlardır. Bu gelişmelere paralel olarak "ethical hacker" kavramı ortaya çıkmıştır[191].

Bir bilişim sisteminin güvenliğinin, daha önceden korsanlık yapmayan bir kişiye kontrol ettirilmesi yeterince başarı göstermemiştir. Gerçekten de bir bilişim

187 Akarslan, age. s. 89-90; Karagülmez, age. s. 89-90.
188 Dülger, age. s. 123.
189 Dülger age. s. 124.
190 Dülger, age. s. 124.
191 Karagülmez, age. s. 91.

uzmanı kendisini ne kadar zorlasa da bir hacker gibi düşünemez onun gibi davranamaz. İşte bu yüzden daha önceleri bilişim korsanlığı yapmış olanlar, yani suç işleyenler ethical hackerleri olarak kullanılmaya başlanmıştır.

Ethical hackerleri, test edilecek bilişim sistemine gerçekten bir saldırı olması halinde ilk nerenin hedef alınacağını ve bu hedef alınan yerlerden ne gibi bir bilgilere ulaşılabileceğini belirlemeye çalışırlar. Bu belirlemeler çerçevesinde sisteme neler yapılabileceğini belirlerler. En son olarak sisteme yetkisiz erişim halinde bu yetkisiz erişimler fark edilebiliyor mu bunun üzerinde dururlar. Bu son kontrol bir nevi koruyucu hekimlik gibi düşünülebilir[192].

Başarılı ethical hackerlerine öncelikle güvenin tam olarak sağlanması gerekir. Ethical hackerler sistemi test ederken müşterilerinin gizli bilgileri hakkında bilgi sahibi olmaktadırlar. Ethical hackerlerinin bunun yanında bilgi ve güçlü bir donanıma sahip olmaları gereklidir. Onlar bilgisayar konusunda uzman olmalıdırlar. İleri teknolojiyi iyi bilmelidirler. İnisiyatif sahibi ve çok sabırlı olmalıdırlar. Yetkisiz erişimlerde korsanların tersine testler uzun zaman alacağı için bu zamanı talep etmeli ve ısrarla testlerini sürdürmelidirler. Aynı zamanda ethical hackerler, gelişmeleri takip ederek kendilerini sürekli yenilemelidirler. Alanda yaşanan teknolojik gelişmeleri, eğitim programlarını sürekli takip etmelidirler[193].

Ülkemizde ethical hackerler fazlaca duyulan bir kavram değildir. ABD'de yasal düzenleme altına alınmışken ülkemizde herhangi bir yasal düzenleme bulunmamaktadır. Ülkemizde bu şekilde bilişim sistemlerini ethical hackerlerine test ettirmek istenmesi halinde eylemin suç oluşturup oluşturmayacağı konusunda yasal bir düzenleme bulunmadığı için bir takım sorunlar ortaya çıkabilmektedir. Özellikle tezimizin konusu olan TCK'nın 244. maddesinde yazan suçun re'sen takip edilen suçlardan olması sebebiyle eylem bir bütün halinde değerlendirilmeli manevi unsur yokluğu ya da ilgilinin rızasına dayanması sebebiyle hukuka uygunluk nedeni çerçevesinde değerlendirilmelidir[194].

### 2.16. Oltalama (Phishing)

Oltalama (pishing), "password" (şifre) ve "fishing" (balık avlama) sözcüklerinin birleşmesinden oluşturulmuş, Türkçe'ye yemleme, oltalama olarak

192 Karagülmez, age. s. 92-93.
193 Karagülmez, age. s. 96-97.
194 ABD'de olduğu gibi konunun iç hukukta düzenlenmesi gerektiğini belirten görüş için bkz. Karagülmez, age. s. 97-98.

çevrilmiştir[195]. Son zamanların en gözde saldırılarındandır. Bu yöntemle mağdurlar her yıl milyarlarca zarara uğratılmaktadır. Bu yöntem, kişilerin kredi kartı bilgilerinin ya da şifresinin öğrenilmesi amacıyla kullanılır. Bu saldırılar için sahte olarak banka, sosyal paylaşım sitesi, online oyunlar gibi web sayfaları hazırlanmakta, bu web sayfaları ile kişilerden kart bilgileri şifreleri vb. bilgiler istenmektedir. Bu şekilde sahte olarak yapılan siteyi dikkate alan kullanıcıların, sitenin istediği bilgileri sisteme girmeleriyle bilgileri çalınmaktadır[196]. Bu saldırılara internet aldatmacası, dolandırıcılığı denilmekte[197], bir tür sosyal mühendislik yöntemi olduğu da ifade edilmektedir[198].

Örneğin, dolandırıcılar tarafından bazı banka web siteleri sahte olarak hazırlanmakta, arama motorunda söz konusu bankayı aratıp sahte bankanın sitesine girerek kart bilgilerini yazan kişilerin bilgileri çalınmaktadır[199].

Bir diğer pishing yöntemi de kişiye sahte e-posta göndermektir. Bir bankadan geliyormuş gibi sahte e-posta gönderilir. Bu e-postada kişisel bilgilerin güncellenmesi istenir. Kişi bu şekilde e-postaya cevap vermesi halinde bilgileri ele geçirilmiş olur[200].

ABD merkezli bir sivil toplum kuruluşu 2012 yılının ilk çeyreği için bir rapor yayınladı. Bu raporda, özel phishing sitelerinin sayısı 56 bin 859 ile tüm zamanların en yüksek düzeyine ulaştığı ifade edilmiştir[201].

Bu tür saldırılardan kurtulmanın en basit yolu bu tür bankaları adres çubuğuna manuel yani el ile yazılmasıdır[202]. Diğer bir korunma yöntemi de bu konuda kullanıcıların bilgilendirilmesi, gereksiz e-postaları açmamaları konusunda aydınlatılmalarıdır. Bu tür saldırılar facebook, messenger, twitter gibi sosyal medya üzerinden de gönderilebileceği düşünülerek kullanıcıların tanımadıkları kişileri arkadaş olarak eklememeleri, şüpheli kişilerden gelen mesajları açmamaları,

---

195 http://www.hurriyet.com.tr/bilgisayar-kullanicilari-oltaya-geliyor-21226684 (erişim tarihi: 15/03/2018)
https://tr.wikipedia.org/wiki/Yemleme (erişim tarihi: 15/03/2018); Doğan, age. s. 28.

196 Dülger, age. s. 132.

197 Orta, age. s. 85.

198 Ünver, M., Mızaoğlu, A.G. (Şubat 2011). *Yemleme ("phıshıng") Raporu*. Bilgi Tekonolijleri ve İletişimi Kurumu Dairesi Başkanlığı. s. 2

199 Dülger, age. s. 132.

200 https://www.garanti.com.tr/tr/bireysel/subesiz/internet_bankaciligi/guvenlik/phishing.page (erişim tarihi: 15/03/2018)

201 http://www.hurriyet.com.tr/bilgisayar-kullanicilari-oltaya-geliyor-21226684 (erişim tarihi: 15/03/2018)

202 Dülger, age. s. 132.

istenmeyen e-postaları önlemeleri, filtrelemeleri ve bu konuda dikkatli olmaları gerekmektedir[203].

### 2.17. Tarama (Scanning)

Tarama, sıralı bir diziyi takip ederek değeri her seferinde değişen verilerin, hızlı bir şekilde bilişim sistemine girilmesi, sistem tarafından olumlu cevap verildiği durumların raporlanması için yapılan işlemdir. Sistem bir telefon numarasından başlayarak arama işlemine başlar, eğer aranan numara bir bilişim sistemine bağlı olursa bağlantı sinyali gönderilir. İşlem her seferinde bir numara artırılarak tekrar edilir. Bu sayede belirli aralıkta bulunan telefon numaralarına bağlı bilişim sistemlerinin tespiti sağlanmış olur. Aynı işlem internete bağlı olan IP numaralarını bulmaya yönelik olarak da yapılabilir. Tarama işlemi, bilişim sistemindeki açıkları tespit etmek amacıyla IP üzerinde "port" taraması şeklinde de olabilir. Şifre ile korunmuş bilişim sistemlerinin şifrelerini bulmak için de şifre taraması yapılabilir[204].

Özellikle port taraması bilişim alanında işlenen suçlarda sıkça başvurulan bir yöntemdir. Burada kullanılan port, bilgisayarlarda kullanılan fiziksel seri ve paralel port olmayıp mantıksal porttur. Her IP adresi sanal veri yollarına bölünmüş yani portlara bölünmüştür. Bu sebeple aynı anda aynı IP adresinden farklı programlarla veri alışverişi yapılabilmektedir. Port taramasıyla bilişim sisteminin açıkları bulunabilmektedir[205].

Bir deneme yanılma işlemi olması ve milyonlarca ihtimali denemesi sebebiyle bir tarama programına ihtiyaç vardır. Bu programlar internet üzerinden kolaylıkla bulunulabilir. Bu tarama programları sistemin açıklarını tespit ederek bu açıkları kapatabilmek amacıyla kullanılması halinde sistemin güvenliğini artırmak için yapılan tarama işlemi olmuş olur. Fakat aynı açıkları tespit ettikten sonra saldırı yapılması halinde ise saldırı amaçlı tarama işlemi yapılmış olur[206].

### 2.18. Parola Kırma Saldırıları

Parola kırma saldırıları, bir bilgisayarda saklanan veya sisteme iletilen verilerin şifrelerini öğrenme ya da çözme işlemine denir. Bu yöntem bütün tahminlerin denenmesiyle gerçekleşir. Bu yöntem şifresini unutan insanlara yardım

---

203 Hekim, H. (2015). Oltalama (Phishing) Saldırıları. Tombul, F., Güneştaş, M., Başıbüyük, O. (Ed.). Siber Suçlar Tehditler, Farkındalık ve Mücadele. Ankara: Global Politika ve Strateji. s. 75-78.

204 Güngör, age. s. 63; Dülger, age. s. 135.

205 Dülger, age. s. 135.

206 Güngör, age. s. 63.

ettiği gibi siber suçlarda gizli verilere ulaşma imkanı sağlaması sebebiyle suçlulara da yardım etmektedir[207].

Bir şifreyi kırmak basit konulan şifreler için çok kısa bir zaman alırken, karmaşık ve içeriğinde bazı karakterler olan şifreler için hem uzun hem de daha zor olmaktadır.

### 2.19. DoS ve DDoS Atakları

DoS (Denial of Sevice) saldırısı bir tür hizmet aksatma yöntemi olup, bu alan içerisinde en meşhur saldırı türü olarak bilinir[208]. Bu yöntemde sisteme düzenli ve arka arkaya yapılan saldırılar sonucu hedefteki sistemin hizmet veremez hale gelmesi ya da o sisteme ait tüm kaynakların tüketilmesi hedeflenir. Kısaca, bir sunucuya durmadan istekte bulunularak hem sunucuyu hem de bilişim sistemini meşgul etme olarak ifade edilebilir. Farklı yöntemlerle hizmet aksatma saldırıları gerçekleştirilebilir[209]. Bir markete sadece gezinmek amacıyla bir yığın insan gönderilmesi, bu insanlar yüzünden gerçek alışveriş yapmak isteyen kişilerin kalabalıktan dolayı alışverişlerini yapamaması hali örnek olarak gösterilebilir. Bu tür saldırılar genellikle internet alt yapısından kaynaklandığı için engellenmesi de çok zor olan bir saldırı çeşididir[210].

DoS saldırıları iki aşamalıdır. ilk aşaması toplu güvenlik kırma aşamasıdır. Bu aşamada DoS saldırısı yapılacak olan sisteme erişilecek ardından saldırıyı yapacak olan program yüklenecektir. İkinci aşama saldırı aşamasıdır. Bu aşamada hedefteki sisteme saldırı yapılır[211].

Günümüzde en tehlikeli saldırı türlerinden bir tanesidir. Engellenemez oluşu ve sistemi çalışamaz hale getirebilmesi sebebiyle hacker aktivist gruplarınca tehdit unsuru olarak kullanılmaktadır[212].

DDoS ise daha önceden tasarlanan bir çok sistem üzerinden hedefteki bilgisayarlara saldırı yapılarak sistemin kimseye hizmet veremeyecek şekle

---

207 Dülger,age. s. 133.

208 Hekim, H., Başıbüyük, O., (2013). Siber Suçlar ve Türkiye'nin Siber Güvenlik Politikaları. Uluslararası Güvenlik ve Terörizm Dergisi. S. 4. s. 143.

209 Dülger, age. s. 132.

210 Ünal, A., (2015). Dağıtık Servis Dışı Bırakma (DDOS) Saldırıları: Güncel Yöntemler ve Mücadele. Tombul, F., Güneştaş, M., Başıbüyük, O. (Ed.). Siber Suçlar Tehditler, Farkındalık ve Mücadele. Ankara: Global Politika ve Strateji. s. 14, 15.

211 Bilgi İşlem Dairesi Başkanlığı, http://bidb.itu.edu.tr/eskiler/seyirdefteri/blog/2013/09/07/denial-of-service-(dos)-sald%C4%B1r%C4%B1lar%C4%B1-ve-korunma-y%C3%B6ntemleri (erişim tarihi: 15/03/2018)

212 Doğan, age. s. 37.

getirilmesini amaçlayan yöntemdir. Eşzamanlı olarak yapılan bu saldırılar saldırının boyutunu arttıracağı gibi saldırıyı yapan kişinin de gizlenmesini sağlar. Bu işlemleri yapan araçlara "zombie" denir. Bu tür saldırı yapan failin tespiti çok zordur[213].

DoS saldırısını DDoS saldırısından ayıran en önemli fark, DoS saldırısında genelde tek bilgisayar ve tek internet bağlantısı kullanılırken, DDoS saldırılarında aynı anda birden fazla bilgisayar ve birden fazla bağlantı desteği vardır. Bu yüzden DDoS saldırıları daha kapsamlı ve büyüktür Dolayısıyla verebileceği zararlar daha fazladır ve önlem alınması da bir o kadar zordur[214].

22 Aralık 2014 tarihinde yayınlanan bir makalede DoS/DDoS saldırılarının sayısının her yıl yaklaşık ikiye katlandığı, 2014 yılında yapılan saldırılarda toplam maliyetin milyarlarca dolardan fazla olduğu ifade edilmiştir. Bu saldırılarla bir bölgenin elektriğinin kesilmesi, sularının boşa akıtılması, uçakların rotalarından çıkartılması, kurumların alt yapısının çökertilmesi gibi saldırılar yapılabilmektedir. Bu nedenle bu saldırılar daha şimdiden bir çok istihbarat örgütleri tarafından kullanılmaya başlanılmıştır[215].

DoS saldırıları, engellenmesinin çok zor ve yıkıcı etkilerinin olması sebebiyle genellikle askeri ve istihbarat birimlerini hedef almaktadır. 2014 yılında İngiltere İstihbarat birimine Anonymous adlı hacker grubu tarafından DDoS saldırısı düzenlenmiş, aynı şekilde Esad yönetimine bağlı istihbarat birimlerine de 2008-2014 yıllarında DoS saldırıları yapılmıştır[216].

Aynı şekilde Estonya ülkesindeki birçok kamu kurumu ve özel sektörlerin internet sitelerine bu tür bir saldırı gerçekleştirilmiştir. Bu saldırının arkasında Rus Hackerler olduğu iddia edilmiştir. Saldırının nedeni olarak da Estonya'nın başkentinde bulunan "The Bronze Soldier" adlı heykelin kaldırılması ileri sürülmüştür[217].

---

213 Dülger, age. s. 132.

214 http://www.teknokulis.com/dosyalar/internet/2015/12/30/dos-ve-ddos-saldirilari-nedir-belirtiler-farklar-ve-onlemler (erişim tarihi: 15/03/2018)

215 Bölükbaş C. (22 Aralık 2014). Yeni Nesil Teknolojik Silahlar: DoS/DDoS. https://siberbulten.com/makale-analiz/yeni-nesil-teknolojik-silahlar-dosddos/ (erişim tarihi: 15/03/2018)

216 Bölükbaş, age.

217 Ünal, age. s. 17.

Bu tür saldırılardan kurtulmanın en etkili yolları, güvenilir bir anti virüs programı yüklenmesi, bir güvenlik duvarı oluşturulması, güvenilir olmayan e-maillerin açılmaması ve e-mail filtreleme yapılması ile mümkündür[218].

### 2.20. Botnet Saldırıları

Botnet, robot kelimesinin "bot"u ile network kelimesinin "net"i kullanılarak oluşturulmuş bir kelimedir. Saldırganlar çeşitli yollarla bilişim sistemlerini ele geçirirler. Bu ele geçirilen bilişim sistemleri zombi (bot) bilgisayar olarak adlandırılır. Botnet programı da bilişim sistemine gizlice yüklenen programlardan olup, bu program ile sisteme uzaktan erişim sağlanmaktadır. Bu şekilde birçok bot programının bulaştığı cihazlar bir araya gelerek büyük bir bot ağı oluştururlar ki bu bot ağının yönetilmesine Botnet denilmektedir[219]. Kısaca, bir çok bilişim sisteminin kötü amaçlar doğrultusunda tek bir noktadan yönetilmesi olarak ifade edilebilir[220].

Bot'u kullanacak zararlı yazılım sahibi öncelikle bir sunucu (server) kiralar, daha sonra zararlı bot'u yayar ve bu şekilde sistemlere bulaşan bot'lar saldırganın sunucusu ile iletişime geçer ve saldırganın istekleri doğrultusunda hareket eder[221].

Bu tür saldırı ile, kurbanın haberi dahi olmadan bir web sitesinin hiti artırabilir, mağdurun e-posta adresindeki kişiler, şifreler, kullanıcı adları ele geçirebilir. Aynı şekilde sosyal medya hesaplarına erişilebilir, mağdurun bilgisayarı kullanılarak DDoS atakları yapılabilir, bir web sitesine girilerek sitedeki rekramlara tıklanılması sağlanılabilir. Saldırgan bu bilgileri haksız kazanç sağlamak için toplayabileceği gibi bu bilgileri satmak ya da şantaj yapmak için de toplayabilir. Sonuç olarak, bu yöntemle mağdurun hesap bilgileri, şifreleri, projeleri, programları, kişisel verileri, dosyaları ele geçirebilmektedir[222].

### 2.21. Süper Darbe (Super Zapping)

Süper darbe, bir bilgisayar sisteminin, işlemez hale gelmesi halinde, kısa bir süre içerisinde sistemin tekrar çalışabilmesi için tüm güvenlik kontrollerini aşıp değişiklik yapılabilmesine yarayan programa verilen addır. Bu program, kopya koruma programını atlatan bir yazılım olarak ortaya çıkmıştır[223].

---

218 Doğan age. s. 39.
219 Dülger, age. s. 133.
220 Muğla Emniyet Müdürlüğü, http://www.mugla.pol.tr/fethiye/Sayfalar/Botnet-Nedir.aspx. (erişim tarihi: 15/03/2018)
221 Dülger, age. s. 133.
222 Dülger, age. s. 133-134.
223 Aydın, age. s. 49; Turhan, age. s. 52; Boğa, age. s. 49.

Bu program amacı doğrultusunda kullanılması halinde kullanıcısına çok büyük faydalar sağlarken, kötü amaçlara alet edilmesi halinde çok tehlikeli olabilmektedir. Bu program bilişim sistemlerinde büyük zararlara yol açmak isteyen saldırganlara, tüm güvenlik önlemlerini aşabilmesinden dolayı çok büyük avantajlar sağlayabilmektedir[224].

Amerika'da bulunan bir bankada bilişim sistemi görevlisinin, sistemlerde meydana gelen hatayı giderebilmek için bu programı çalıştırmış ve sistemdeki tüm tedbirlerin kalktığını farketmiştir. Bundan faydalanmak isteyen banka görevlisi, arkadaşlarının hesaplarına yüklü miktarlarda paralar aktarmış ancak bir müşterinin hesabındaki paranın azaldığını fark etmesiyle suç ortaya çıkmıştır[225].

### 2.22. Eşzamansız Saldırılar (Asynchronous Attacks)

Bilgisayarların birden fazla işlemi aynı anda yapabilmelerine eşzamanlı çalışma adı verilir. Ancak bazı durumlarda bilgisayarlar eşzamanlı yerine belirli bir sırada da çalışabilmektedir. Bir işlemin başlayabilmesi için diğer işlemin sonucu beklenebilir. Bu çalışma sistemine de eşzamansız çalışma denir. Örneğin, bir bilgisayardan bir çıktı alma işleminde, çeşitli görevler sırayla çağrılması gerekir. İşletim sistemi bu istekleri sistemde bekletir, yazıcıya ulaşılabilir olduğunda istek sırasına veya öncelik sırasına göre istekler yerine getirilir[226].

Başka bir tanıma göre ise eşzamansız çalışma sırasında, işletim sisteminde bekleyen veriler üzerinde değişiklik, ekleme ya da silme işlemi yapılabilir. Bu tür veriler üzerinde değişiklik yapılması işlemine eşzamansız saldırı denir[227]. Bu saldırı ile TCK'nın 244 maddede yazılı suçların işlenmesi mümkündür. Örneğin sistemde sırasını bekleyen bir işleme eşzamansız saldırı ile müdahale edilerek sırasına bekleyen veriyi değiştiren ya da silen fail bu kanun maddesinden yargılanacaktır.

---

224 Aydın, age. s. 49; Turhan, age. s. 52; Boğa, age. s. 49.

225 Yazıcıoğlu, *Bilgisayar Suçları*. s. 156.

226 Boğa, age. s. 51.

227 Yazıcıoğlu, *Bilgisayar Suçları*. s. 158.

# ÜÇÜNCÜ BÖLÜM
# 5237 SAYLI TÜRK CEZA KANUNUNDA BİLİŞİM SİSTEMİNİ ENGELLEME, BOZMA, VERİLERİ YOK ETME VEYA DEĞİŞTİRME SUÇU İLE HAKSIZ ÇIKAR SAĞLAMA SUÇU

## 1. GENEL OLARAK

Günümüz modern yaşamında bilişim sistemi ekonomi, sağlık, eğitim, bilimsel araştırmalar, savunma, idare vb. pek çok alanda vazgeçilmez bir hal almıştır. Hemen hemen tüm devlet kurumları ve ticari işletmeler bütün iş ve işlemlerini bilişim sistemlerini kullanmak suretiyle gerçekleştirmektedir. Vazgeçilemez hale gelen bilişim sisteminin geçici süreyle de olsa çalışamaması büyük zararlara neden olabilmektedir. Özellikle çok iyi bir şekilde üretilmiş olan kurtçuklar, virüsler, truva atları gibi zarar verici yazılımlar gün geçtikçe artmaktadır. Aynı şekilde bir web sitesini çökertmek için kullanılan DDoS saldırıları ile pek çok kamu kurumu işleyemez hale gelebileceği gibi şirketlerin ticaret yapması da engellenebilmektedir. Yasa koyucu bu gibi yıkıcı etkileri olan eylemleri düzenleme altına alarak bir nebze de olsa bu suçun işlenmesinin önüne geçmek istemiştir[228].

Bilişim alanındaki suçlar hakkında, karşılaştırmalı hukuka bakıldığı zaman, iki temel sistemin uygulandığı görülmektedir. Bir kısım ülkeler bu tür suçları mevzuatlarında ayrı özel bir kanun yaparak düzenlemekteyken diğer bir takım ülkeler mevcut ceza yasaları içerisinde düzenleme altına almışlardır. Mevcut ceza yasaları içerisinde bu suçlara yer veren ülkeler hukuki yarar çerçevesinde o hukuki yararı koruyan maddelere ekleyerek veya bu maddeleri yeniden düzenleyerek ya da ülkemizde olduğu gibi bu maddeleri ayrı bir bölüm halinde değerlendirerek düzenleme altına almıştır. Bakıldığı zaman ülkemizde bu suçlar hem "*bilişim*

[228] Dülger, age. s. 410

*alanında suçlar*" adı altında ayrı bir bölümde hem de dolandırıcılık, hırsızlık gibi suçların içerisinde nitelikli hal olarak düzenleme altına alınmıştır[229].

Bu çerçevede Eski 765 sayılı TCK'nın 525/b maddesinin karşılığı olarak 5237 sayılı TCK'nın 244. maddesi düzenlenmiş ve kendi içerisinde üç ayrı suç tipine yer verilmiştir. 1. fıkrada *"Bir bilişim sisteminin işleyişini engelleyen veya bozan kişi*" ile 2. fıkrada "*sistemin bozulması "bir bilişim sistemindeki verileri bozan, yok eden, değiştiren veya erişilmez kılan, sisteme veri yerleştiren, var olan verileri başka bir yere gönderen kişi*" nin cezalandırılacağı, 4. fıkrada ise *"fiillerin işlenmesi suretiyle kişinin kendisinin ya da başkasının yararına haksız bir çıkar sağlanmasının başka bir suç oluşturmaması halinde"* kişinin cezalandırılacağı belirtilmiştir. Maddenin 3. fıkrası ile de ilk iki fıkranın nitelikli halinden bahsedilmiştir.

Maddenin ilk iki fıkrası doğrudan doğruya bilişim sistemini veya verilerini korumaya yönelik suçları içermektedir. Dördüncü fıkrada, bilişim sistemleri ile haksız yarar sağlama suçu yaptırım altına alınmıştır. Biz bu çalışmamızda maddenin 1. ve 2. fıkrasını bir; 4. fıkrasını ayrı olarak ele alacağız.

## 2. BİLİŞİM SİSTEMİNİ ENGELLEME, BOZMA; VERİLERİ YOK ETME VEYA DEĞİŞTİRME SUÇU

### 2.1. Genel Olarak

ASSS'nin 4. maddesi verilere müdahale konusunu düzenlemektedir. Buna göre, "*taraflardan her biri, bilgisayar verilerine haksız yere zarar verilmesi, verilerin silinmesi, tahrip edilmesi, değiştirilmesi veya engellenmesinin, kasten gerçekleştiği zaman, kendi iç hukuku kapsamında cezai suç olarak tanımlaması için gerekli olabilecek yasama tedbirlerini ve diğer tedbirleri kabul edecektir*" şeklindedir. 5. maddesi ise sisteme müdahale konusunu düzenlemektedir. Buna göre, "*taraflardan her biri bilgisayar sistemlerine veri girişi yaparak, bu verileri ileterek, bilgisayar verilerine zarar vererek, bunları silerek, tahrip ederek, değiştirerek veya engelleyerek bir bilgisayar sisteminin işleyişinin haksız yere engellenmesinin, kasten gerçekleştirildiği zaman, kendi iç hukuku kapsamında cezai suç olarak tanımlaması*

---

229 Yazıcıoğlu, *Genel Değerlendirme*, s. 396; Yazıcıoğlu, Y. (2009). *5237 s. TCK.nun 244/4 üncü Maddesinde Düzenlenen "Bilişim Sistemi Marifetiyle Haksız Çıkar Sağlanması" Suçu ile md.142/2-e ve 158/1-f Maddesinde Düzenlenen "Bilişim Sistemlerinin Kullanılması Suretiyle" "Hırsızlık" ve "Dolandırıcılık" Suçlarının İşlenmesi Sorunsalı Üzerine Düşünceler*. Suç ve Ceza. S. 4. s. 1; Yılmaz, S. (2011). *5237 Sayılı TCK'nın 244. Maddesinde Düzenlenen Bilişim Alanındaki Suçlar.* TBB Dergisi. S. 92. s. 64.

*için gerekli olabilecek yasama tedbirleri ve diğer tedbirleri kabul edecektir"* şeklindedir. Düzenlemelerden de anlaşılacağı üzere taraf devletlerin bu tür suçları kendi iç hukuklarında yaptırım altına almaları gerektiğinin belirtilmesi sebebiyle, 5237 sayılı TCK'nın 244/1. maddesi ile ASSS'nin 5. maddesine paralel bir düzenleme ile konu yaptırım altına alınmıştır. Buna göre "*Bir bilişim sisteminin işleyişini engelleyen veya bozan kişi, 1 yıldan 5 yıla kadar hapis cezası ile cezalandırılır*" şeklindedir. Aynı maddenin 2. fıkrası ise ASSS'nin 4. maddesine paralel olacak şekilde düzenlemiştir. Buna göre, *"bir bilişim sistemindeki verileri bozan, yok eden, değiştiren veya erişilmez kılan, sisteme veri yerleştiren, var olan verileri başka bir yere gönderen kişi 6 aydan 3 yıla kadar hapis cezası ile cezalandırılır"* şeklindedir[230].

Bu iki fıkranın nitelikli hali 3. fıkrada düzenlenmiştir. Buna göre, "*bir banka ya da kredi kurumuna veya bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinde işlenmesi halinde, verilecek ceza yarı oranında arttırılır"* şeklindedir.

### 2.2. Suçla Korunan Hukuki Yarar

#### 2.2.1. Genel Olarak

Kanunun 1. ve 2. fıkrasında yer alan suçlarda korunan hukuki değer konusunda doktrinde görüş birliği yoktur. Dülger'e göre, yasa koyucu hem bilişim sistemlerinin soyut unsurlarından olan veri ve yazılımları hem de bilişim sistemlerinin somut unsuru olan donanım kısmını koruma altına aldığını belirterek suçla korunan hukuki yararın karma nitelikte olduğunu belirtmiş, bilişim sistemiyle oluşturulan yazılım, ekonomik bilgiler, bilimsel çalışmalar, bilgi ve benzeri değerleri haksız müdahaleden korumak istediğini belirtmiştir[231].

Kurt'a göre öncelikle bilişim sistemi sahibinin mülkiyet hakkı, zilyedinin bilişim sisteminin dokunulmazlığı, iletişim kurma teknolojik gelişim özgürlüğünü korurken ikinci fıkra, bazen mülkiyet hakkı, bazen fikri mülkiyet hakkı, özel hayatın gizliliği, ticari sırların korunduğunu belirtmiştir[232].

Erdoğan, bilişim alanında yapılan her saldırı kişilerin sisteme olan güvenilirliğini zedeleyeceğini aynı zamanda maddenin topluma karşı suçlar başlığı adı altında düzenlenmesi sebebiyle sistemin toplu nazarında güvenilirliğini ve toplumun tamamının menfaatlerini korumak istediğini aynı zamanda sistem sahibinin

---

230 https://www.tbmm.gov.tr/sirasayi/donem24/yil01/ss380.pdf. (erişim tarihi: 20/03/2018)

231 Dülger, age. 411.

232 Kurt, age. 161-162.

maddi ve manevi çıkarlarını, sistem kullanıcılarının özel hayatlarının korunduğunu ifade etmiştir[233].

Akbulut ise maddenin birinci fıkrası bilişim sistemleri sahipleri, işletmecileri ile kullanıcılarının sistemin arızasız çalışmasındaki yararı koruduğunu, ikinci fıkra ile de tasarruf yetkisi elinde olan kişilerin veriler bozulmadan, verilere müdahale olmadan kullanılmasındaki yararın korunduğunu; mülkiyetin korunmadığını, yalnızca malikin yararlarının korunduğunu, özel hayat veya haberleşmenin korunduğuna ilişkin görüşlere düzenleme yeri itibariyle katılmadığını ifade etmiştir[234].

Erdağ, bu suçun mala zarar vermenin elektronik bir türü olduğunu, bununla birlikte bilgisayarın dokunulmaz olması ve sistemin istenilen şekilde hizmet görmesini dolayısıyla hukuki değerin karma nitelik taşıdığını ifade etmiştir[235].

Pallı, bu suçla korunan hukuki yararın, bilişim sistemi ve sistemin güvenliği olduğunu belirtmiş, diğer değerleri saymaya gerek olmadığını aynı zamanda saymakla da bitmeyeceğini ifade etmiştir. Bu konuda görüşünü şu örnekle ifade etmiştir. Hastanede yatan bir hastanın yaşamını devam ettirebilmesini sağlayan bir bilişim sistemine müdahale yapılarak hastanın ölmesi halinde, korunan hukuki değerin yaşam hakkı olduğunu, bu sebeple bu suçla korunan hukuki yararın çeşitlilik gösterdiğini belirtmiştir[236].

TCK'nın 244. maddesine paralel olan ASSS'nin veriye müdahale konusunu düzenleyen dördüncü maddesinin açıklayıcı raporunda, bilişim sisteminde yer alan verilere veya yazılımlara zarar verilmesinin, veri veya yazılımların bozulmasının, zarar görmesinin engellenmesi, beşinci maddesi ise bilişim sistemlerine yapılan saldırıların önüne geçilebilmesi, sistemlerin ve verilerin sağlam bir şekilde çalışabilirliğinin korunması olduğu ifade edilmiştir[237].

---

233 Erdoğan, age, s. 184.

234 Akbulut, B. (2016). *Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme*. SÜHFD. C.24. S.2. s.17.

235 Erdağ, age. s. 280.

236 Pallı, age. s. 164.

237 Karagülmez, age. s. 236-237; Dülger, age. s. 41; Ketizman, M. (2008). *Türk Ceza Hukukunda Bilişim Suçları.* Ankara: Adalet Yay. s. 119 .

Yaygın görüşe göre sistem ve veriye müdahalenin mala zarar vermenin özel bir şekli olduğunun kabul edilmesi sebebiyle, bu suçla korunan hukuki değerin mülkiyet hakkının korunması olduğu çalışmamızda birçok kez ifade edilmiştir[238].

Kanaatimizce, bu kanun maddesiyle yasa koyucu toplum için vazgeçilmez bir hal alan bilişim sistemine güveni sağlamak istemiştir. Yani sisteme sağlam, güvenli ve gecikmesizin girilebilmesini korumasıyla beraber o bilişim sistemi sahibinin mülkiyet hakkının da korunması amaçlanmıştır.

### 2.2.2. Mala Zarar Verme Suçu Açısından Konunun Değerlendirilmesi

Her ne kadar suçun hukuki konusunu, mala zarar verme suçunun hukuki konusu ile benzer şekilde kişilerin mülkiyet haklarının korunması olarak ifade etmiş isek de kanunun düzenleniş şekli bakımından durum çelişkilidir. TCK'nın 151. maddesinde yazılı mala zarar verme suçunun TCK'nın ikinci kısım onuncu bölümünde yer almasına rağmen, TCK'nın 244. maddesinde düzenlenen suç TCK'nın üçüncü kısım onuncu bölümünde düzenlenmektedir. Her ikisinin de koruduğu hukuki değerin birbirleri ile benzer olmasına rağmen ayrı ayrı bölümlerde düzenlenmiş olması çelişki oluşturmaktadır.

Bununla birlikte kanunun 167. maddesinde, bu suçların haklarında ayrılık kararı verilmemiş eşlerden birisinin, altsoy veya üstsoy veya bu derece kayın hısımlarından birisinin veya evlat edinen ile evlatlığın, aynı konutta beraber yaşayan kardeşlerden birisinin zararına işlenmesi halinde fail hakkında cezaya hükmolunmayacağı, haklarında ayrılık kararı verilmiş eşlerden birisinin, aynı konutta beraber yaşayan amca, hala, dayı, teyze, yeğen veya ikinci derecede kayın hısımlarının, aynı konutta beraber yaşamayan kardeşlerden birisinin zararına işlenmesi halinde fail hakkında şikayet üzerine verilecek cezanın yarı oranında indirileceği düzenlenmiş olmasına rağmen TCK'nın 244. maddesinde bu şekilde bir şahsi cezasızlık sebebi öngörülmemiştir.

Benzer bir durum TCK'nın 168. maddesinde de yer almaktadır. Bu maddede belirtilen suçlardan dolayı, suçun tamamlanmasından fakat hakkında kovuşturma başlanmadan önce veya sonra, failin, azmettirenin veya yardım edenin pişmanlık göstererek mağdurun uğradığı zararı aynen geri iade etmesi ya da zararlarını

[238] Ersoy, age. s. 166; Tezcan, D., Erdem. M. R., Önok, M. (2015). *Teorik ve Pratik Ceza Özel Hukuku*. Ankara: Seçkin Yay. s. 911; Özbek, Doğan, Bacaksız, Tepe, age. s. 945; Ketizman, age. s. 128; Yılmaz, S. (2016). *Türk Ceza Hukuku Sisteminde Siber Suçlar*. Ankara: Adalet Yay. s. 193; Yılmaz, *Bilişim*. s. 68; Avşar, B. Z., Öngören, G. (2010). *Bilişim Hukuku*. İstanbul, Türkiye Bankalar Birliği Yayını, Yayın No: 270. s. 135.

karşılaması halinde fail hakkında verilecek olan cezada indirim öngörülmüş olmasına rağmen, aynı hukuki değeri koruyan TCK'nın 244. maddesinde bu şekilde bir düzenlemeye yer verilmemiştir. Oysa TCK'nın 244. maddesi tıpkı mala zarar verme suçu gibi ikinci kısım onuncu bölümde yer almış olsa idi yukarıda belirtilen yasal olanaklardan yararlanılmış olunacaktı. Benzer durum TCK'nın 245. maddesi için de belirtilmekteyken 5360 sayılı Kanun'un 11. maddesi ile bu eksiklik giderilerek faile etkin pişmanlık ve şahsi cezasızlık sebebinden yararlanma imkanı getirilmiştir. Bu doğrultuda mala zarar verme suçuyla benzer hukuki değeri koruyan TCK 244. maddesine de TCK 245. maddesinde olduğu gibi benzer bir düzenleme yapılarak çelişkinin giderilebileceği kanısındayız.

### 2.3. Suçun Unsurları

5237 sayılı TCK'nın sistematiği dikkate alındığında suçun unsurları, tipiklik, maddi unsur, manevi unsur ve hukuka aykırılık olmak üzere dörde ayrılır[239].

#### 2.3.1. Maddi Unsur

Suçun maddi unsuru hareket, netice ve bunlar arasındaki illiyet bağı olarak üç ana başlık altında incelenmektedir. İnsandan sadır olan ve dış dünyaya yansıyan, ihmali ya da icrai davranış, hareket; insanın dış dünyada meydana getirdiği değişikliğe netice; meydana gelen neticenin yapılan hareketten doğmuş olmasına da illiyet bağı denir[240].

##### 2.3.1.1. Suçun Faili

Maddenin faile ilişkin herhangi bir hüküm içermemesi sebebiyle suçun faili herkes olabilir. Kişi, başkalarının haklarını ihlal etmediği sürece kendi bilişim sistemini engellemesi veya bozması suç oluşturmayacağı için bu suç için failin tespiti önemlidir.

Hukuka aykırı fiilin bilişim sisteminin hangi unsuruna yöneldiğinin tespiti, suç açısından önemlidir. Fiilin bilişim sisteminin kendisine yönelmesi halinde sisteminin kendisine ait mülkiyet ve tasarruf yetkisinin, verilerine yönelmesi halinde verilere ait mülkiyet ve tasarruf yetkisinin, hem bilişim sisteminin kendisine hem de verilerine yönelmesi halinde ise her ikisine de ait mülkiyet ve tasarruf yetkisinin

---

239 Artuk, M. E. Gökçen, A. Yenidünya, C. A. (2007). *Ceza Hukuku Genel Hükümler*. Ankara: Turhan Kitapevi. içindekiler kısmı; Centel, N. Zafer, H. Çakmut, Ö. (2008). *Türk Ceza Hukukuna Giriş*. İstanbul: Beta Basım. s. içindekiler kısmı.

240 Artuk, Gökçen, Yenidünya, *Genel Hükümler*, s. 388; Centel, Zafer, Çakmut, age. s. 228.

kimde olduğu ve zararı kimin meydana getirdiği ayrı ayrı belirlenmelidir[241]. Bu hususun araştırılması gerektiği pek çok yargıtay kararında da açıkça ifade edilmiştir[242].

Kanun'un 246. maddesinde suçun bir tüzel kişinin faaliyetleri çerçevesinde tüzel kişi yararına işlenmesi halinde ilgili tüzel kişi hakkında bunlara özgü güvenlik tedbiri uygulanacağı ayıca hüküm altına almıştır.

**2.3.1.2. Suçun Mağduru**

Bu suçun mağduru kural olarak, bilişim sistemi veya verileri üzerinde tasarruf yetkisini elinde bulunduran kişidir. Sistemi engelleme veya bozma suçu açısından bakıldığında ise mağdur, sistemin kullanıcısı, işleticisi veya sahibi olabilir. Ancak bu suçların mağduru olabilmek için mutlaka bilişim sisteminin ya da verilerin maliki ya da zilyedi olunmasına gerek yoktur. Bu yönden bakıldığında bu suçta mağdur herkes olabilir. Örneğin, kamu kurum veya kuruluşlarının bilişim sistemlerine karşı işlenen suçlarda mağdur herkes olabilir[243].

Bilişim sisteminin herhangi bir engel, arıza ya da gecikme olmaksızın kullanılmasında yararı bulunan herkes bu hakkının zedelenmesi halinde bu suçun mağduru olabilir. Bununla birlikte bilişim sisteminin maliki ya da zilyedi de aynı zamanda suçun mağduru olacaktır[244].

Hafızoğulları-Özen, herkes için güvenli bir bilişim ortamının sağlanması kamu düzeninden olduğu için suçun mağdurunun kamu idaresi olduğunu belirtmiş ve suçun kişilere karşı suçlar arasında yer almaması sebebiyle kişi veya kişilerin sadece suçtan zarar gören olduğunu ifade etmiştir[245].

**2.3.1.3. Suçun Konusu**

Kanunun birinci fıkrasında yer alan bilişim sisteminin işleyişinin engellenmesi ve bozulması suçunun hukuki konusu bilişim sistemi iken; ikinci fıkrasında yer alan verilerin yok edilmesi veya değiştirilmesi suçunun hukuki konusu

---

241 Dülger, age. s.414; Soyaslan, age. s. 699.

242 Bkz. Yar. 11 CD. 28/01/2009 T., ve 2008/16570E, 2009/101 K. sayılı ilamı,

243 Koca, M., Üzülmez. İ. (2017). *Türk Ceza Hukuku Özel Hükümler*, 4. Baskı, Ankara: Adalet Yay. s. 826; Akbulut, Sistemi Engelleme. s. 21.

244 Dülger, age. s. 414.

245 Hafızoğulları, Z., Özen, M. (2012). *Türk Ceza Hukuku Özel Hükümler Topluma Karşı Suçlar.* Ankara: Usa Yay. s. 48.

bilişim sisteminde yer alan verilerdir. Bu iki fıkrayı birbirinden ayırmaya yarayan en önemli husus da her iki fıkranın hukuki konularıdır[246].

Bilişim sistemi yazılımı ve donanımıyla bir bütündür. Yazılım olmadan donanım, donanım olmadan da yazılım bir anlam ifade etmez. Bu sebeple TCK'nın 244/1 maddesi anlamında gerek yazılım gerekse donanım unsurları, suçun hukuki konusu dahilindedir[247].

TCK'nın 244/2 maddesinde yazılı veri kavramından ne anlaşılması gerekeceği konusunda TCK'nın 243. maddesinin gerekçesi bize yol göstermektedir. Buna göre "*sistem üzerinde bütün soyut unsurlar, fıkrada geçen veri teriminin kapsamındadır*" şeklindeki ifade ile veri kavramının çerçevesi çizilmiştir. Aynı doğrultuda 5651 S. İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun'un 2/1-k maddesinde veri, "*bilgisayar tarafından üzerinde işlem yapılabilen her türlü değer"* olarak tanımlanmıştır[248].

Doktrinde verinin mutlaka bilişim sisteminde yer alan bir veri olması gerekeceği belirtilmektedir. Yani disket, CD, flash bellek gibi yalnızca veri saklama ve taşıma görevi gören cihazların bozulması, fiziki olarak kullanılamaz hale getirilmesi halinde bu suçun değil TCK'nın 151. maddesinde yazılı mala zarar verme suçunun oluşacağı belirtilmiş ise de[249], kanaatimizce veri soyut ya da somut unsurlarıyla bir bütün halinde incelenmeli, suçun tespiti için failin güttüğü amacın açıkça tespit edilmesi gerekmektedir. Buna göre failin bir flash bellek, CD gibi veri depolama aracının içerisindeki bilgilere, verilere zarar vermek kastıyla hareket etmesi halinde TCK'nın 244. maddesinde yazılı suçtan, bunun haricinde failin amacının sırf mala zarar vermek olması halinde ise TCK'nın 151. maddesinde yazılı mala zarar verme suçunun uygulanması gerekecektir. Nitekim failin satışa hazır bir bilgisayara zarar vermesi halinde bilişim sistemine zarar verme kastıyla hareket etmemesi sebebiyle yalnızca mala zarar verme suçu, bununla birlikte failin bir ticari işletmenin işleyişini durdurmak, müşteri profilini çalmak amacıyla bilişim sistemine

---

246 Dülger, age. s.415; Artuk, Gökçen, Yenidünya, şerh, s. 6929; Soyaslan, age. s.700; Özbek, Doğan, Bacaksız, Tepe, age. s. 946-947; Koca, Üzülmez, age. s. 826.

247 Özbek, Doğan, Bacaksız, Tepe, age. s. 946-947.

248 "veri" konusunda ayrıntılı tanımlar için bkz. eserin 13. sayfası.

249 Ketizmen, age. s. 143.

zarar vermesi halinde zarara uğrayan bilgisayar için TCK'nın 244. maddesi uygulanması gerekecektir[250].

TCK'nın 244. maddesinde yazılı suçun mala zarar verme suçunun özel bir şekli olduğunu yukarıda belirtmiştik. Madem mala zarar vermenin özel bir şekli o halde suçun hukuki konusu da mala zarar vermenin hukuki konusuyla benzer niteliktedir[251]. Hafızoğulları-Özen, bilişim alanının sanal aleme ait olduğunu, reel aleme ait bir malvarlığı değerinin olmadığını, yasa koyucu tarafından suçun mala zarar verme suçunun düzenlendiği, kişilere karşı suçlar arasında yer almayıp topluma karşı suçlar başlığı altında düzenlediğini, yasa koyucunun bilinçli olarak kişilere karşı suçlar arasında bu suça yer vermediğini, suçun topluma karşı suçlardan olduğunu, bu sebeple suçun hukuki konusunun, bilişim ortamının oluşturulmasına, geliştirilmesine, sağlıklı, güvenilir işlenmesinin sağlanmasına, istenmeyen bir zarar tehlikesinin veya zararın ortaya çıkmasının önlenmesine ilişkin kamusal yarar olduğunu ifade etmiştir[252]. Aynı şekilde Tezcan/Erdem/Önok'ta suçun hukuki konusunu bilişim sistemleri ve bilişim sistemlerindeki veriler olduğunu, bunların TCK'nın 151. maddesine göre mal sayılamayacağı için, mala zarar vermeden bağımsız olarak düzenleme altına alındığını ifade etmiştir[253]. Yazıcıoğlu, Özbek ve Taşdemir de benzer şekilde verinin taşınabilir bir mal olmadığını ayrıca ifade etmiştir[254].

#### 2.3.1.4. Fiil (hareket) ve Netice

TCK'nın 244. maddesi birbirinden farklı iki suçu düzenlemiştir. Bunlardan ilki, birinci fıkrada yer alan bilişim sisteminin işleyişini engellemek veya bozmak; ikincisi ise ikinci fıkrada yer alan bilişim sistemindeki verileri bozmak, yok etmek, değiştirmek veya erişilmez hale getirmek, sisteme veri yerleştirmek, var olan verileri başka bir yere göndermektir. Her iki fıkra için de suç tipi seçimlik hareketli olarak düzenlenmiştir. Ayrıca maddede suçun nasıl işleneceğine dair herhangi bir

---

250 Aynı doğrultuda görüş için bkz. Akbulut, Sistemi Engelleme. s. 26-27; Demircan, age. s. 91.

251 Toroslu, N. (2009). *Ceza Hukuku Özel Kısım,* Ankara: Savaş Yay. s. 155; Ketizmen, age. s. 128; Yılmaz, Siber. s. 193.

252 Hafızoğulları, Özen, age. s. 447-448.

253 Tezcan, Erdem, Önok, age. s. 911.

254 Yazıcıoğlu, TCK 244/4 üzerine düşünceler, s. 6; Yazıcıoğlu, Genel Değerlendirme, s. 398; Özbek, V. Ö. (2007). *Banka ve Kartlarının Kötüye Kullanılması Suçu (TCK m. 245)*. Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi, C. 9. Özel Sayı, s. 1058. Taşdemir, K. (2009). *Bilişim, Banka ve Kredi Kartlarının Kötüye Kullanılması ve Dolandırıcılık Suçları*. Ankara: Cantekin Mat. s. 276

özelleştirme yapılmadığı için her türlü eylemle suç işlenebilir, bu yüzden her iki fıkra da serbest hareketli suçlardandır.

Suç kural olarak icrai hareketlerle işlenebilir. Ancak bir bilişim sistemi sorumlusu, sisteme yüklemesi gerekli programları yüklemez, güncelleştirmeleri yapmaz, ya da sisteme virüs bulaştığını görmesine rağmen bunu engellemeye çalışmazsa ihmal suretiyle söz konusu suçu işlemiş olacaktır[255].

Uygulamada hangi seçimlik hareketin meydana geldiği tam olarak tespiti yapılamamaktadır. Ancak bunun tespit edilememesinin suç için bir önemi yoktur. Suç açısından seçimlik hareketlerden herhangi birinin meydana gelmesi yeterlidir. Uygulamada birden çok seçimlik hareketin aynı anda gerçekleştiği görülmektedir. Her ne kadar birden çok seçimlik hareket aynı anda gerçekleşmiş olsa da tek suç işlenmiş sayılacaktır. Fakat ceza belirlenirken alt sınırdan uzaklaşılarak ceza tayin edilecektir. Yargıtay ve BAM da vermiş olduğu bir çok kararda sanığın eylemi tam olarak belirlenemediği için uzman bilirkişiden rapor alınıp cezanın buna göre belirlenmesi gerektiği belirtilmiştir[256].

#### 2.3.1.4.1. TCK'nın 244/1. Maddesinde Düzenlenen Fiiller

##### 2.3.1.4.1.1. Bilişim Sisteminin İşleyişini Engelleme

Eski 765 sayılı TCK'nın 525/b-1 maddesinde düzenlenen sistemi tahrip etmek, işlenmesine engel olmak, yanlış biçimde işlemesini sağlamak eylemlerinin karşılığı olarak TCK'nın 244/1. maddesi düzenlenmiştir.

Eski metinde yer alan sistemin yanlış biçimde işlemesini sağlamak yeni metinde yer almamış, bu eylemle sistem işleyişinin de engelleneceği düşüncesiyle bu fiil içerisinde değerlendirilmiştir.

Maddenin ilk fıkrasında, bilişim sisteminin işleyişini engelleyen kişinin cezalandırılacağı hüküm altına alınmıştır. Söz konusu suçun oluşabilmesi için sistemin işleyişinin engellenmesi gerekir. Sistemin engellenmesi suçun neticesini oluşturur. Bu sebeple suç neticeli bir suçtur. Aynı zamanda her türlü hareketle işlenebilmesi sebebiyle de serbest hareketli bir suçtur[257].

Suç kural olarak icrai hareketle işlenebilir. Ancak sistem sorumlusunun sistemi virüs saldırılarından korumak için gerekli yazılımı yüklememesi ya da yüklü

---

255 Akbulut, Sistemi Engelleme. s.37; Dülger, age. s. 418.

256 Bkz. Yar. 8 CD. 31/03/2014 T. 2013/10236 E, 2014/8040 K . sayılı ilamı.

257 Koca, Üzülmez, age. s. 827; Akbulut, Sistemi Engelleme. s. 27; Özbek, Doğan, Bacaksız, Tepe, suç ancak kanunda yazan hareketin gerçekleşmesi suretiyle işleniyor olması sebebiyle, bağlı hareketli bir suç olduğunu ifade etmiştir, bkz. age. s. 951.

olan yazılımın güncelleştirmelerini yerine getirmemesi ve bu şekilde sistemi dışarıdan yapılacak saldırılara karşı savunmasız halde bırakması halinde ihmali davranışla suç işlenmiş sayılacaktır[258].

Kanunda bilişim sisteminin işleyişini engelleme noktasında herhangi bir tanımlama yer almamaktadır. Doktrinde konu hakkında görüş birliği yoktur. Ketizmen, "*sistem aracılığıyla veri işleme faaliyetlerinin gerçekleştirilmesinin engellenmesi*[259]", Karagülmez, *"sistemin geçici veya sürekli olarak çalışmasının herhangi bir şekilde kesintiye uğratılması*[260]*"*, Erdoğan, "*bilişim sisteminin varlık sebebi olan görevlerini yapamaz hale getirilmesi*[261]" Avşar/Öngören, "*sistemin gereği gibi çalışmasının önlenmesi, faaliyet ve kapasitesinin sınırlandırılması, sistemin işleyişinin yavaşlatılması veya tamamen kilitlenme noktasına getirilmesi*[262]" şeklinde ayrı ayrı ifade edilmiştir.

TDK'ya göre engellemek, "*bir şeyin gerçekleşmesini veya yapılmasını önlemek*" şeklinde ifade edilmiştir[263].

ASSS'nin 5. maddesine göre sistemin engellenmesinin, sisteme bilişim verilerinin girilmesi, bozulması, tahrip edilmesi, nakledilmesi, silinmesi suretiyle olabileceği belirtilmiştir[264].

Bu tanımlamalardan yola çıkarak bilişim sisteminin işleyişinin engellenmesine ilişkin genel bir tanımlama yapmak gerekirse, dışarıdan yapılan bir müdahale ile sistemin doğru bir şekilde çalışmasının engellenmesi olarak ifade edilebilir.

Bilişim sisteminin işleyişini engelleme, sistemin geçici olarak çalışmasının aksatılmasıdır. Bu fiilde sistem bozulmamakta, herhangi bir şekilde çalışması engellenmektedir. Doktrinde ağırlıklı görüşe göre, sistemin geçici ya da sürekli aksatılması sistemin işleyişinin engellenmesi çerçevesinde değerlendirilirken[265], Artuk/Gökçen/Yenidünya ve Erdoğan sistemin kalıcı engellenmesinin sistemin

---

258 Dülger, age. s. 418.

259 Ketizmen, age. s. 129,

260 Karagülmez, age. s.237.

261 Erdoğan, age. s. 189.

262 Avşar, Öngören, age. s. 136.

263 http://www.tdk.gov.tr/index.php?option=com_gts&arama=gts&guid=TDK.GTS.5a8d42cf4bab86. 88319603(erişim tarihi: 01/04/2018)

264 Karagülmez, age.s. 238; Erdoğan, age. s. 190-191

265 Hafızoğulları, Özen, age. s.449; Soyaslan, age. s.701; Pallı, age. s. 168; Dülger, age. s. 418; Karagülmez, age. s. 237; Yılmaz, *Siber*. s. 194; Akbulut, Sistemi Engelleme. s. 30; Taşkın, age. s. 45; Parlar, A.(2015). *Türk Ceza Hukukunda Bilişim Suçları*. Ankara: Bilge Yay. s. 41.

bozulması ile eş değer olduğunu, bu sebeple bu eylemde sistemin geçici olarak engellenmesi gerekeceğini savunmuştur[266]. Bize göre ikinci görüş geçerlidir. Çünkü gerçekten de sistemin kalıcı olarak engellenmesi aynı zamanda sistemin bozulmasıyla eş anlamlı olacaktır.

Doktrinde bir kısım yazarlarca sistemin somut unsurlarına verilen zararların bu suçu değil, TCK'nın 151. maddesinde tanımlı mala zarar verme suçunu oluşturacağı savunulsa da[267] bize göre her somut olayın ayrı ayrı değerlendirilmesi gerekmekte ve failin güttüğü saik suç için önemli kabul edilmelidir. Nitekim bilişim sistemi hem soyut (yazılım) hem de somut (donanım) unsurlardan meydana gelmektedir. Sistemin somut unsurlarına verilen zararlarla da sistemin işleyişi engellenebilir. Örneğin failin, sırf hasmına zarar vermek amacıyla bir bilişim sisteminin unsuruna, örneğin bilgisayarın klavyesine zarar vermesi halinde mala zarar verme, onun haricinde failin bir bilgisayardaki sistemin çalışmasını engellemek amacıyla kablosunu kesmesi halinde TCK'nın 244. maddesinin tatbik edilmesi gerekecektir[268]. Doktrinde bu konu şöyle ifade edilmiştir; bilişim sisteminin somut unsurlarından olan elektriğinin kesilmesi, kablolarının çıkartılması, sistemin donanımının sökülmesi gibi fiziki bir takım unsurlarına zarar verilmesi halinde söz konusu suçun oluşacağı gibi, sisteme virüs ya da mantık bombası, sistemde olmayan bir şifrenin sisteme yerleştirilmesi veya mevcut şifrenin değiştirilmesi gibi soyut olarak da gerçekleştirilebilir[269]. Aynı doğrultuda sistemin istenilen performansta çalışmaması, hızının düşmesi, veri alış-verişi yapamaması, dosyaları açamaması halleri bu maddi unsura örnek olarak gösterilebilir[270]. Bununla beraber sistemin işleyişini önemsiz derecede engelleyen hallerin TCK'nın 244. madde kapsamında tutulmaması gerektiği ileri sürülmüş, haksızlık içeriğinin azlığı sebebiyle ceza verilmemesi gerektiği, bu hususun kanun maddesinde belirtilmesi gerektiği savunulmuştur[271].

---

266 Artuk, Gökçen, Yenidünya, şerh, s. 6928; Erdoğan, age. s. 190, aynı görüş için bkz. Doğan, age. s. 118.

267 Koca, Üzülmez, age. s. 827.

268 Benzer görüşler için bkz, Dülger, age. s. 418; Akbulut, Sistemi Engelleme. s. 28-29; Gürler, age. s. 111; karşıt görüşler için bkz. Özbek, Doğan, Bacaksız, Tepe,age. s. 949; Koca, Üzülmez, age. s. 827-828; Ketizmen, age. s. 129-133.

269 Dülger, age. 418; *Akbulut,* Sistemi Engelleme. s. 28-29

270 Dülger, age. s. 418

271 Akbulut, Sistemi Engelleme. s. 30.

Konu hakkında Yargıtay'ın vermiş olduğu ve kanaatimizce isabetsiz olan bir karar aynen şu şekildedir. *"Sanığın katılan Fatma Can'a ait "facebook" hesabındaki verilere yönelik bozma veya değiştirme gibi bir eylemde bulunmadan bu hesaba ilişkin şifreyi değiştirip hesap sahibi gibi hareket etmek şeklinde gerçekleştirdiği eyleminin TCK'nın 244/1. maddesindeki bilişim sisteminin işleyişini engelleme suçunu oluşturduğu gözetilmeden sanık hakkında TCK'nın 244/2. maddesi gereğince uygulama yapılması*" şeklindeki hükümle ilk derece mahkemesince TCK'nın 244/2. maddesinden verilen kararı bozarak 244/1 olacağını ifade etse de[272]; eylem aslında TCK'nın 244/2 maddesini oluşturmaktadır. Nitekim Yargıtayın bu ceza dairesi ile diğer ceza daireleri kararları aynı zamanda BAM kararları çelişmiş, diğer dairelerce bu şekilde şifre değiştirmelerinin TCK'nın 244/2. maddesinin ihlalini oluşturduğu çok sayıda kararda belirtilmiştir[273]. Yargıtayın haklı olarak vermiş olduğu bir karar ise aynen şu şekildedir, "*Sanığın, mağdur Gizem'in, e-posta adresi ve şifresi ile facebook hesabı için yeni şifre oluşturarak hesabına girmesi, hesaba fotoğraf yerleştirdikten sonra e-posta adresi ve facebook hesabının şifrelerini değiştirerek mağdurun hesaplara erişimine engel olması biçimindeki eyleminin, TCK'nın 244/2. maddesine uygun bulunduğu gözetilmeden, olayda uygulama yeri bulunmayan aynı Kanunun 244/1. maddesi uyarınca hüküm kurulması, Kanuna aykırı*[274]*"* olduğunu açıkça belirterek eylemin TCK'nın 244/2 maddesini oluşturduğunu ifade etmiştir. Aynı şekilde 8. Ceza Dairesi "*Suça sürüklenen çocuğun, mağdurun elektronik posta adresinin ve bu adrese bağlı facebook sayfasının şifresini değiştirmek suretiyle erişimini engellemesinden ibaret eyleminin TCK.nun 244/2. maddesinde düzenlenen suçu oluşturduğu gözetilmeden, uygulama yeri bulunmayan TCK.nun 244/1. maddesince mahkumiyet kararı verilmesi*[275]" kanuna aykırı bulmuştur. Sonuç olarak, mağdurun bilişim sisteminde şifrelerinin değiştirilmesi eylemi bu maddi unsuru değil 244/2 deki maddi unsuru oluşturacaktır.

**2.3.1.4.1.2. Bilişim Sisteminin İşleyişini Bozmak**

---

272 Yar. 23 CD. 24/05/2016 T, 2015/9146 E, 2016/6542 K .

273 Yar. 15 CD. 18/05/2016 T, 2013/32575E, 2016/5124K; Yar. 12. CD. 02/02/2016 T, 2015/15291 E, 2016/1124 K,; 8 CD. 21/04/2014 T, 2013/13127 E, 2014/10178 K, 8 CD. 08/01/2014 T, 2012/33042 E, 2014/231 K. Ankara BAM. 8 CD. 19/12/2017 T, 2017/1422 E, 2017/1919 K.

274 Yar. 12 CD. 22/12/2014 T, 2014/10843E, 2014/26243 K .

275 Yar. 8 CD. 13/11/2014 T, 2014/20966 E, 2014/26063 K.

Maddenin ilk fıkrasında, bilişim sisteminin işleyişini bozan kişinin cezalandırılacağı hüküm altına alınmıştır. Suç elverişli her hareketle işlenebilen suçlardandır, bu yüzden serbest hareketli bir suçtur[276].

Yasada sistemin bozulmasıyla ne kastedildiği noktasında herhangi bir hüküm yer almamaktadır. TDK'ya göre bozmak, kendisinden beklenilen işi yapamayacak hale getirmek, geçersiz hale getirmek, zarar vermek şeklinde belirtilmiştir[277]. Akbulut, sistemin yapması gerekenden tamamen farklı şeyleri yapması[278]; Özbek-Doğan-Bacaksız-Tepe, kendisinden beklenilen işi yapamayacak şekilde kısmen ya da tamamen tahrip edilmesi[279]; Eker, sistemin işlemesi engellenmekten öte sistemin artık işlemesi olanaksız hale gelmesi, fonksiyonlarını yerine getirememesi[280]; Soyaslan, bilişim sistemine zarar verilmesi, sistemin düzeninin karıştırılması, sistemin kendisinden beklenen işi yapamayacak hale getirilmesi[281]; Ketizmen, sistemin işlem yapabilme eylemini kısmen ya da tamamen ortadan kaldırılması[282]; Artuk-Gökçen-Yenidünya, sistemden kalıcı olarak istifade edilememesi[283]; Erdoğan ve Tezcan-Erdem-Önok ise sistemin veri işleme faaliyetlerini yapamaması ya da doğru yapılmasına engel olacak şekilde sisteme müdahalede bulunulması şeklinde ifade etmişlerdir[284].

Kanaatimizce bozulma, her ne suretle olursa olsun bilişim sisteminin, kısmen ya da tamamen çalışamayacak hale getirilmesidir.

Sistemin nasıl bozulduğu suçun oluşumu açısından önemli değildir. Sistem , fiziki temasla bozulabileceği gibi sisteme hiç dokunulmadan da eylem gerçekleştirilebilir[285]. Sistemin çökertilmesi, program akışının bozulması, virüsler ve kurtçuklar ile sistemin işlemez hale getirilmesi halleri örnek olarak gösterilebilir. Aynı şekilde sistemdeki bazı verilerin silinmesi, hatalı program teslimi ve

---

276 Koca, Üzülmez, age. s. 827; Özbek, Doğan, Bacaksız, Tepe, suçun ancak kanunda yer alan hareketin gerçekleştirilmesi suretiyle işlenebiliyor olması sebebiyle bağlı hareketli suç olduğu belirtilmiştir. bkz. age. s. 951.

277 http://www.tdk.gov.tr/index.php?option=com_gts&arama=gts&guid=TDK.GTS.5a8e8080119b69.31487652 (erişim tarihi: 01/04/2018)

278 Akbulut, Sistemi Engelleme. s.30.

279 Özbek, Doğan, Bacaksız, Tepe, age. s. 949

280 Eker, age. s.125.

281 Soyaslan, age. s. 701.

282 Ketizmen, age. s.135.

283 Artuk, Gökçen, Yenidünya, şerh. s. 6929.

284 Tezcan, Erdem, Önok, age.s. 911; Erdoğan, age. s. 193

285 Erdoğan, age. s. 193.

yüklenmesi, sistemin parçalarının değiştirilmesi, sistemdeki verilerin değiştirilmesi halleri de örnek olarak gösterilebilir[286].

Sistemin bozulması halinde sistemin işleyişinin de engellenmesi söz konusudur. Yani sistemin bozulması aynı zamanda engellemeyi de kapsamaktadır. Bununla birlikte sistemin her engellenmesi hali bozmayı kapsamayabilir[287]. Bu sebeple, yasa koyucu her iki hali ayrı ayrı belirtme yoluna gitmiştir[288]. Doktrinde, bozma fiilinin aynı zamanda engelleme fiilini de kapsıyor olması sebebiyle, bozma kavramının gereksiz yere kullanıldığı ayrıca ifade edilmiş, ASSS'nin 5. maddesi gibi bozmanın da bir engelleme olduğunun belirtilmesi ile yetinilebileceği ifade edilmiştir[289].

#### 2.3.1.4.2. TCK'nın 244/2. Maddesinde Düzenlenen Fiiller

765 sayılı TCK'nın 525/c ve 525/b-1 maddelerinde düzenlenen verilerde sahtecilik ve verileri tahrip etmek suçlarına karşılık olarak yeni TCK ile verileri yok etme ve değiştirme suçları getirilmiştir. 765 sayılı kanunda suçun oluşması için zarar vermek veya yarar sağlamak amacıyla yapılması aranırken yeni düzenlemede bu eylemler yer almamış, dolayısıyla suç genel kastla işlenebilecek bir suç haline getirilmiştir. Bu suç aynı zamanda yukarıda da belirtildiği üzere ASSS'nin 4. maddesinde yer alan verilere müdahale suçuna karşılık gelmektedir[290].

Veri ile ne kastedilmek istendiği hususu, çalışmamızın ilk bölümünde bahsedildiği için bu kısımda yeniden bahsedilmeyecektir.

##### 2.3.1.4.2.1. Bilişim Sistemindeki Verileri Bozmak

Maddenin ikinci fıkrasında, bir bilişim sisteminin verilerini bozan kişinin cezalandırılacağı hüküm altına alınmıştır. Verilerin hangi yolla bozulması gerektiği konusunun açıkça belirtilmemesi sebebiyle her türlü eylemle bu suç işlenebilir, bu yüzden suç serbest hareketli bir suçtur.

Verilerin bozulmasını Akbulut, verilerin kullanılabilirliğine zarar verilmesi olarak ifade etmiş ve artık verilerin usulüne uygun olarak kullanılamayacağını

286 Akbulut, Sistemi Engelleme. s. 31.
287 Koca, Üzülmez, age. s. 827.
288 Ketizmen, age. s. 238; Erdoğan, age. s. 194; Akbulut, Sistemi Engelleme. s. 31.
289 Karagülmez, age. s. 238; Erdoğan, age. s. 194.
290 Pallı, age. s. 178.

belirtmiştir[291]. Artuk-Gökçen-Yenidünya da verilerden istenen faydanın elde edilememesine yönelik hareketler olarak ifade etmiştir[292]. Doktrinde ağırlıklı görüş, verinin yapısına müdahale edilerek kısmen ya da tamamen kullanılamaz hale getirilmesi olarak ifade edilmiştir[293].

Bilişim sistemine fiziki zararlar harici verilen zararlar, aynı zamanda verilere zarar verme halini de oluşturur[294]. Bu yüzden yukarıda bilişim sisteminin bozulması kısmında yaptığımız açıklamaların büyük bir çoğunluğu bu fiil için de geçerlidir.

TCK'nın 244/1 ve 2. fıkralarının birbirleri ile benzer olmaları sebebiyle karıştırılmakta, bazen yukarıda Yargıtay kararında da belirtildiği üzere yanlış uygulanmaktadır. Hangi fıkranın tatbik edilmesi gerektiği konusunun, her somut olay için ayrı ayrı değerlendirilmesi gerekecek ve failin güttüğü saik hangi fıkranın uygulanması gerekeceğini belirtecek olması sebebiyle tespiti önemli olacaktır. Bu çerçevede failin asıl amacı bilişim sistemini bozmak ise TCK 244/1; failin bilişim sisteminin işleyişine zarar vermek istemeyip sadece bilişim sisteminin içerdiği verilere zarar vermek amacıyla eylemini gerçekleştirmesi halinde TCK'nın 244/2 maddesi tatbiki gerekecektir[295].

Verileri bozmak, fiziki müdahale ile gerçekleşebileceği gibi sisteme virüs, mantık bombası veya kurtçuk gönderilerek de gerçekleşebilir. Sisteme gönderilen bu gibi zararlı yazılımlar bilişim sistemini ve verilerini kullanılamaz hale getirmektedir. Bunun haricinde sistemin verilerini içeren bir harici veri taşıyıcının (sabit disk) kırılması[296]; birbirine bağlı veri cümlelerinin yerlerini değiştirerek anlamının karıştırılması, veriye ilave bir şeylerin katılması, verilerden herhangi birinin silinmesi halleri verilerin bozulmasına örnek olarak verilebilir[297].

Veriye virüs gönderilmesi ya da kötü amaçlı kodların eklenmesi veriyi bozma kapsamında değerlendirilmemesi gerektiği, bu virüs ve kodların bilişim sitemindeki veriye eklendiği, bu yüzden veriyi tamamen ya da kısmen kullanılamaz hale

---

291 Akbulut, Sistemi Engelleme. s. 32.

292 Artuk, Gökçen, Yenidünya, Ceza Özel. age. s. 854.

293 Hafızoğulları, Özen, age. s.451; Koca, Üzülmez, age. s.829; Özbek, Doğan, Bacaksız, Tepe, age. s. 951; Ketizmen, age. s. 139;

294 Soyaslan, age. s. 702; Dülger, age. s.420.

295 Soyaslan, age. s.702; Dülger, age. s. 420.

296 Soyaslan, age. s.702; Dülger, age. s.420; Kızıltan, age. s. 80.

297 Akbulut, Sistemi Engelleme. s.32.

getirmediği, bu halin aşağıda belirtileceği üzere verinin değiştirilmesi fiilini oluşturacağı ayrıca ifade edilmiştir[298].

**2.3.1.4.2.2. Bilişim Sistemindeki Verileri Yok Etmek**

Eski 765 sayılı TCK'nın 525/b maddesinde verilerin silinmesinden bahsedilmişken, 5237 sayılı TCK'nın 244/2 maddesinde bu ifadeye yer verilmemiştir. Çünkü verilerin silinmesi ile aşağıda da açıkça belirtileceği üzere yok etme, bilişim hukuku açısından aynı anlama gelmektedir. Bu yüzden yasa koyucu yeni TCK'da silme fiiline haklı olarak yer vermemiştir[299].

TDK'ya göre yok etmek, varlığına son vermek, ortadan kaldırmak olarak tanımlanmıştır[300].

Her ne kadar yok etmek kelime anlamı olarak, geri ve eski hale getirilemeyecek şekilde tamamen ortadan kaldırmak anlamına gelse de bilişim alanında bu tanımlama pek fazla mümkün olamamaktadır. Bu nedenle yasa koyucu bu ifadeyle somut anlamda yok etmeyi değil, bilişim alanında geçerli olan soyut anlamda, mantıksal yok etmeyi kastetmektedir[301].

Bakıldığı zaman bilişim sisteminden yok edilmek istenen bir veri bazen kolay bazen uzun ya da masraflı çalışmalar sonucunda tekrar eski hale getirilebilmektedir. Örnek vermek gerekirse, bilgisayara atılan format ile bilgisayardaki tüm veriler silinmiş gibi gözükse de veri kurtarma programlarıyla bu veriler tekrar geri getirilebilmektedir[302]. Bu konu yani silinen bir verinin ya da geri dönüşüm kutusuna gönderilen bir verinin yok edilmiş sayılıp sayılamayacağı konusu doktrinde tartışmalıdır. Bir görüşe göre silinen bir veri geri dönüşüm kutusuna gönderilecek, verinin yeri değiştirilecek fakat tek tıkla eski hale getirilebilecektir. Bu sebeple bu halde verilerin yok edilmesi söz konusu olmayacaktır[303]. Özbek-Doğan-Bacaksız-Tepe, veriyi yok etmek için o verinin kayıtlı olduğu bellekten de silinmesinin gerekeceğini, bu sebeple bir verinin silinmesinin o verinin yok edildiği anlamına gelmeyeceğini ifade etmiştir[304].

---

298 Ketizmen, age. s. 140.
299 Erdoğan, age. s. 223.
300 http://www.tdk.gov.tr/index.php?option=com_gts&arama=gts&guid=TDK.GTS.5a8ec267484960. 45132459 (erişim tarihi: 01/04/2018)
301 Soyaslan, age.s. 702; Dülger,age. s. 420; Kızıltan, age. s. 81
302 Dülger, age. s. 421.
303 Koca, Üzülmez, age. s.830; Kurt, s. 168; Taşkın, age. s. 47.
304 Özbek, Doğan, Bacaksız,Tepe, age. s. 952.

Ağırlıklı olan ve bizim de katıldığımız diğer görüşe göre, verinin silinmesiyle yok edilmesi aynı anlama gelmektedir. Veri sahibinin verisini bıraktığı yerde bulamaması verinin yok edilmesi anlamına gelecektir[305]. Bu görüşü savunan yazarlara göre, çöp kutusuna atılan bir veri, çöp kutusundan çıkartılmadıkça kullanılamayacaktır. Her ne kadar bu işlem tek bir tuşla yapılabiliyor olsa da veri sahibinin bu işleme katlanması ondan beklenilemez. Bu sebeple silmenin yok etmek olduğu haklı olarak ifade edilmiş fakat kısmi silmeler ve kopyası bulunan verinin silinmesinin yok etmek sayılamayacağı da ifade edilmiştir[306].

Verilerin yok edilmesi, fiziki bir müdahale ile meydana gelebileceği gibi başka herhangi bir hareketle de meydana gelebilir. Sistemin işleyişini engellemeden veya bozmadan sisteme gönderilen virüsler[307], veri taşıma aracının veri kurtarma yazılımıyla geri getirilebilip getirilemeyeceği fark etmeksizin kırılması yok etme kavramı içerisinde sayılacaktır[308].

Verileri bozmak ile yok etmek arasındaki fark ise, bozulmada veri sahibinin mülkiyet hakkı devam etmekte yani veri bozulmuş da olsa ortada bir veri mevcut olup o veriye bir şekilde ulaşılabilir. Yok etmede ise verinin ortadan kaldırılması sebebiyle sahibinin mülkiyeti sona erecektir. Bir başka fark da bozulan verinin tamir edilerek eski hale getirilebilme imkanı varken, yok edilen bir verinin artık eski hale getirilmesi mümkün olamayacaktır[309].

#### 2.3.1.4.2.3. Bilişim Sistemindeki Verileri Değiştirmek

Verileri değiştirmekten ne anlaşılması gerektiği doktrinde, orijinal verilerin yerine başka veri koymak[310], bir verinin başka bir veriyle değiştirilmesi ya da orijinal halinden başka hale dönüştürmek[311], var olan verinin kullanımı engellenmeden verinin içeriği ya da orijinalliğini değiştiren her türlü değişiklik[312], bir verinin ya da veri grubunun yerine başka bir verinin konulması[313], bir şey ekleyerek ya da

---

305 İkinci görüşü savunan yazarlar için bkz Erdoğan, age. s. 222, Dülger, age. s. 421; Ketizmen, age. s. 139; Artuk, Gökçen, Yenidünya, Ceza Özel, age. s. 854; Soyaslan, age. s.703; Hafızoğulları, Özen, age. s. 751; Kızıltan, age. s. 81; Sarı, age. s. 179.

306 Erdoğan, age. s. 222; Akbulut, Sistemi Engelleme. s. 33; Doğan, age. s. 121.

307 Koca, Üzülmez, age. s. 830.

308 Dülger, age. s. 421; Soyaslan, age. s. 703.

309 Erdoğan, age. s. 220.

310 Eker, age. s. 126.

311 Yılmaz, Siber. s. 196.

312 Ketizmen, age. s. 140.

313 Soyaslan, age.s.703; Dülger, age. s. 421.

çıkartarak veriyi aslından başka bir hale getirmek[314], verinin içeriğinin değiştirilmesi, başka bir görünüm veya konuma getirilmesi, verinin yerine başka bir veri konulması[315], verileri başka bir şekle sokmak, başka bir görünüm kazandırmak[316] şeklinde ifade edilmiştir. Artuk-Gökçen-Yenidünya ise değiştirmenin, veriler üzerinde yapılan manipülasyonlar olduğunu, bunların verilere başka bir içerik kazandırması, verileri başka bir biçime sokulması, niteliklerin değiştirilmesi şeklinde olabileceğini belirtmiştir[317]. TDK ise değiştirmeyi, değişikliğe uğratmak, başka bir biçime sokmak, başka bir görünüme getirmek şeklinde tanımlamıştır[318].

Kurt, orijinal verinin tamamen değiştirilmesiyle veri kullanılamaz hale geleceğinden bu eylemde verinin değiştirilmesi fiili değil; verinin bozulması eyleminin gerçekleşeceğini belirtmiştir[319].

Akbulut da değiştirmenin ancak ve ancak orijinal verilerde yapılması gerekeceğini, kopya edilmiş verilerde yapılan değişikliklerin bu madde kapsamında uygulanamayacağını ifade etmiştir[320].

Bu fiilde veri yok edilmemekte ya da erişilmez kılınmamakta, veri sahibi bu halde yanlış bir veriye ulaşmakta, bu nedenle bu halde sistem işleyişine devam etmektedir[321].

Konuya örnek olarak, bilişim sistemindeki dosyaları ya da resimleri başkalarıyla değiştirmek[322], Virüs, Truva atı gibi yazılımların sisteme sokulması[323], kötü amaçlı kodların veriye yerleştirilmesi[324], sistemdeki bilgi notunun değiştirilmesi, sisteme konulan şifrenin yerine başka bir şifrenin konulması[325], banka hesap kayıtlarının değiştirilmesi[326], bilgisayarda bulunan word, excel gibi programların içeriğinin değiştirilmesi[327] hali gösterilebilir.

---

314 Hafızoğulları, Özen, age. s.451.
315 Koca, Üzülmez, age. s.830; Tezcan, Erdem, Önok, age. s. 912.
316 Gürler, age. s.119.
317 Artuk, Gökçen Yenidünya, Ceza özel, age. s. 854.
318 http://www.tdk.gov.tr/index.php?option=com_gts&arama=gts&guid=TDK.GTS.5a8ff70017f3e9.7 6038474 (Erişim tarihi: 01/04/2018)
319 Kurt, age. s. 168.
320 Akbulut, Sistemi Engelleme. 35.
321 Yılmaz, Siber. s. 196.
322 Dülger, age. s.421; Yılmaz, Siber. s. 196.
323 Yılmaz, Siber. s. 196.
324 Ketizmen, age. s. 140.
325 Dülger, age. s. 421.
326 Kızıltan, age. s. 82.
327 Gürler, age, s. 119.

TCK'nın 244/2 maddesinde yazılı verilerin yok edilmesi ve değiştirilmesi ile TCK'nın 243/3 maddesinde yer alan yetkisiz erişim ile verilerin yok edilmesi veya değiştirilmesi suçlarının birbirinden ayırt edilmesi sorunu karşımıza çıkmaktadır. 244/2 maddesinin oluşabilmesi için failin amacının yetkisiz erişim olmaması gerekir. Yetkisiz erişim ile başkasının bilişim sistemine giren, bu yetkisiz erişim ile bilişim sistemindeki verilerin yok edilmesine ya da değiştirilmesine sebebiyet veren fail yasanın 243/3 maddesindeki suçu işlemiş olacaktır. Bunun için failin saikinin, bilişim sistemindeki verilerin yok edilmesi veya değiştirilmesi olmaması gerekmektedir. Failin amacı, verileri değiştirmek veya yok etmek ise 243/3 değil 244/2 maddesinde suç oluşacaktır[328].

Somut olayda gerçekten de verilerin değiştirilip değiştirilmediği kuşkuya yer bırakmayacak şekilde belirlenmelidir. Yargıtayın bir çok kararında, bu husus dikkate alınmadan verilen kararlar eksik inceleme nedeniyle bozulmuş ve mahkemesine iade edilmiştir[329].

#### 2.3.1.4.2.4. Bilişim Sistemindeki Verileri Erişilmez Kılmak

Doktrinde erişilmez kılma, verinin içerdiği bilgiye müdahale edilmeden erişimin engellenmesi[330], verilere ulaşılabilirliği önleyen veya sona erdiren herhangi fiil[331], veri sahibinin verisine istediği zaman ulaşmasının engellenmesi[332], failin yaptığı hareketlerle mağdurun kendi verisine ulaşmasının imkansız hale getirilmesi[333] şeklinde ifade edilmiştir.

Bu halde veri ne yok edilmekte ne de bozulmaktadır. Veri bütünlüğünü korumaktadır. Sadece veriye ulaşım için gereken işlem bağı koparılmakta[334], verilere ulaşma olanağı ortadan kaldırılmaktadır[335].

Veriye erişimin geçici ya da kalıcı olması suç açısından önemli değildir[336]. Ancak doktrinde geçici olması gerektiği tartışılmış ve önemsiz olmayan bir sürenin

328 Artuk, Gökçen, Yenidünya, Ceza Özel. s. 855.
329 Örnek karar için bkz. Yar. 8. CD. 29/01/2014 T, 2013/9454 E, 2014/1798 K sayılı ilamı,
330 Özbek, Doğan, Bacaksız, Tepe, age. s.952.
331 Eker, age. s. 126.
332 Koca,Üzülmez, age. s. 830; Soyaslan, age. s. 703; Dülger, age. 422.
333 Artuk, Gökçen, Yenidünya, Ceza Özel. s. 855.
334 Hafızoğulları, Özen, age. s. 451; Özbek, Doğan, Bacaksız, Tepe, age. s. 952.
335 Tezcan, Erdem, Önok, age. s. 912; Dülger, age. s. 422.
336 Erdoğan, age.225; Soyaslan, age. s. 704; Dülger, age. s. 422.

geçmesi gerektiği ileri sürülmüştür[337]. Bize göre kanunda konuya ilişkin bir düzenleme bulunmadığı için çok kısa da olsa veriye erişilememesi suç için yeterli olacaktır.

Bu suçun, bir bilişim sistemi üzerinde işlenebileceği gibi veri taşıma aracında da işlenebileceği haklı olarak belirtilmiş ise de[338]; Erdoğan, veri taşıma cihazlarının bilişim sistemine takılmadığı sürece bilişim sisteminin bir parçası olamayacağını, bu sebeple yukarıda belirtilen görüşe katılmadığını ifade etmiştir[339].

Virüs bulaştırmak[340], şifre koymak[341], var olan şifreyi değiştirmek[342], veri taşıma aracının bozulması, verilerin silinmesi[343], başka bir yere taşınması, sistemin elektriğinin kesilmesi[344], dosya isimlerininin değiştirilmesi, dosyaların gizlenmesi, veri taşıma cihazına el konulması, elektronik postaların gizlenmesi, içerisindekileri silmek[345] bu fiile örnek olarak gösterilebilir. Bununla birlikte veriler sistem içerisinde bir sıra veya düzen içerisinde bir yazılım oluştururlar, bu düzen veya sıranın bozulması ya da yazılıma başka bir veri sokulması halinde de verilere erişilemeyecektir[346].

Bu suç uygulamada en çok karşılaşılan suçlardan birisidir. Bu suç, daha çok başkalarının şifrelerinin değiştirilmesi suretiyle işlenmektedir. Nitekim Yargıtay ve BAM ceza dairelerinin vermiş olduğu bir çok kararda, mağdurun e-posta şifresini, facebook şifresini, MSN şifresini değiştiren failin bu fıkra kapsamında cezalandırılması gerektiğine hükmetmiştir[347]. Ankara BAM 8 CD. vermiş olduğu bir kararda, sanığın beş yıl arkadaşlık yaptığı katılanın facebook şifresini değiştirmekten ilk derece mahkemesince TCK'nın 243. maddesinden verilen cezanın TCK'nın 244/2. maddesine uyduğundan bahisle bozmuş ve faile 244/2 maddesinden altı ay hapis cezası vermiştir[348]. Ancak bu konuda Yargıtayın 23. CD. diğer daireler ve BAM kararlarıyla çelişir nitelikte sanığın, katılanın facebook şifresini değiştirerek katılan

337 Akbulut, Sistemi Engelleme. s. 37.
338 Soyaslan, age.s. 703; Kızıltan, age. s. 83; Dülger, age. s. 422.
339 Erdoğan, age. s. 225.
340 Özbek, Doğan, Bacaksız, Tepe, age. s. 952; Erdoğan, age. s.225; Dülger, age. s. 422.
341 Akbulut, Sistemi Engelleme. s. 35; Koca,Üzülmez, age.s.830; Erdoğan, age. s. 225.
342 Koca,Üzülmez, age. s. 830.
343 Artuk, Gökçen,Yenidünya, Ceza Özel, s. 855; Soyaslan, age. s. 703.
344 Soyaslan, age. s. 703; Dülger, age. s. 422.
345 Akbulut, Sistemi Engelleme. s. 35.
346 Dülger, age. s. 422; Soyaslan, age. s. 704.
347 Yar. 12. CD. 02/02/2016 T, 2015/15291 E, 2016/1124 K,; 8 CD. 21/04/2014 T, 2013/13127 E, 2014/10178 K, 8 CD. 08/01/2014 T, 2012/33042 E, 2014/231 K.; 8 CD. 17/09/2014 T, 2014/14716 E, 2014/20052 K, Yar. 12 CD. 22/12/2014 T, 2014/10843E, 2014/26243 K. sayılı ilamı.
348 Bkz. Ankara BAM. 8 CD. 19/12/2017 T, 2017/1422 E, 2017/1919 K. sayılı ilamı

gibi hareket ettiği olayda, verilere yönelik herhangi bir eylemin bulunmaması sebebiyle ilk derece mahkemesince TCK'nın 244/2. maddesinden verilen hükmü bozarak 244/1 maddesinde yazılı bilişim sisteminin işleyişini engelleme suçunu oluşturduğunu belirtmiştir[349].

**2.3.1.4.2.5. Bilişim Sistemine Veri Yerleştirmek**

Sisteme veri yerleştirmeyi doktrin, sistemde bulunmayan verilerin sisteme girmek[350], bilişim sistemine veya veri depolama aracına sistem sahibinin izni olmadan dışarıdan sisteme veri kaydedilmesi, eklenilmesi veya yüklenilmesi[351], sistemde yer alan verilere herhangi bir zarar vermeden, onlara ulaşma imkanı ortadan kaldırılmadan sisteme harici veri ilave etmek[352], sistemin orijinalinde olmayan verileri sisteme dahil etmek[353] şeklinde tanımlamıştır.

Flash bellek, harici bellek, disket, CD gibi harici veri taşıyıcılarıyla sisteme veri yerleştirilebileceği gibi, klavye ile ya da internet veya diğer bilişim ağları ile de sisteme veri yerleştirilebilir[354]. Yerleştirilen bu veriler ile sisteme herhangi bir zararın verilmemesi bu maddi unsur için gereklidir[355].

Eylemin oluşabilmesi için failin söz konusu bilişim sistemine ister hukuka aykırı isterse hukuka uygun girmesinin, suçun oluşumu açısından bir önemi bulunmamaktadır. Örneğin, bedeli ödenen ve şifresi alınan bir internet sitesine, failin girmesi hukuka uygun iken, bu sisteme veri yüklemesi hukuka aykırı olacaktır. Ancak daha çok sisteme girme hakkı bulunan failin aynı zamanda sisteme veri yükleme hakkının da bulunması halinde, her iki eylemin de hukuka uygun olması nedeniyle herhangi bir suç oluşmayacaktır[356].

Bununla birlikte sisteme yerleştirilen veri ile bir belgenin içeriği değiştirilmişse fail ayrıca belgede sahtecilikten sorumlu tutulacaktır[357].

**2.3.1.4.2.6. Bilişim Sisteminde Var Olan Verileri Başka Bir Yere Göndermek**

---

349 Yar. 23 CD. 24/05/2016 T, 2015/9146 E, 2016/6542 K. sayılı ilamı

350 Hafızoğulları,Özen, age. s. 451; Tezcan,Erdem, Önok, age. s. 912; Akbulut, Sistemi Engelleme. s. 38.

351 Dülger, age. s.427; Soyaslan, age. s. 704.

352 Artuk, Gökçen, Yenidünya, Şerh. s. 6934.

353 Eker, age. s. 125.

354 Akbulut, Sistemi Engelleme. s. 38; Dülger, age. s. 427; Soyaslan, age. s. 704; Koca,Üzülmez, age. s. 830.

355 Koca,Üzülmez, age. s. 830; Artuk, Gökçen, Yenidünya, Şerh. s. 6934.

356 Dülger, age. s. 427; Kızıltan, age. s. 83.

357 Artuk, Gökçen, Yenidünya, Şerh. s. 6934.

Bilişim sistemindeki verilerin başka bir yere gönderilmesi eylemi, 15/05/2003 tarihinde TBMM'ye sunulan tasarının içerisinde yer almamaktaydı. TBMM Adalet Komisyonu tarafından ilgili madde değiştirilerek son anda maddeye eklenmiştir.

Bu konu doktrinde, sistemde bulunan verilerin yerlerinin değiştirilmesi[358], mağdura ait bir verinin bilişim sistemindeki farklı bir yere ya da farklı bir bilişim sistemine gönderilmesi[359], sistemdeki orijinal verilerin her ne suretle olursa olsun başka bir yere götürülmesi, taşınması ya da gönderilmesi[360] şeklinde ifade edilmiştir.

Dülger, soyut bir kavram olan verinin, somut bir eylemi içeren göndermek eylemiyle açıklanmasının doğru olmadığını, bu fiile kastedilenin verilerin aktarılması, kaydedilmesi veya kopyalanması olduğunu ifade etmiştir[361].

Bu halde verilerin, mağdura ait bilişim sistemi haricinde başka bir sisteme gönderilmesi şart olmayıp, kendi bilişim sisteminde farklı bir dosyaya konulması halinde de suç oluşacaktır[362].

Veriler, bir bilişim ağı vasıtasıyla başka bir yere gönderilebileceği gibi CD, flash bellek, hard disk gibi veri taşıma aracı ile de gönderilebilir. Veriler genellikle sisteme yerleştirilen key logger, truva atı veya virüsler ile başka bir yere gönderilmektedir. Bu tür yazılımlarla failler sistemdeki şifreleri, kullanıcı adlarını veya sistemdeki diğer verileri göndermektedir[363]. Örneğin, bir öğrencinin sınav sorularını kopyalaması, bilişim sistemindeki fotoğrafların, çeşitli belgelerin yazıcıdan çıktı yoluyla alınması, sistemdeki verilerin truva atı ya da virüslerle başka bir sisteme gönderilmesi, devletin önemli bilgilerinin ele geçirilmesi konuya örnek olarak verilebilir[364].

Bu halde veri aslı ortadan kaldırılmamaktadır. Veri aslının ortadan kaldırılması halinde, verinin başka bir yere gönderilmesi değil yok edilmesi eylemi oluşacaktır. Bu yüzden bu fiilde verinin kopyası başka bir yere aktarılmaktadır. Veri kopyalanması ile aynı zamanda çoğaltılmaktadır. Verinin kopyalanması ile orijinal

---

358 Tezcan, Erdem, Önok, age. s. 912.

359 Artuk, Gökçen, Yenidünya, Şerh. s. 6934, benzer nitelikte Mahmutoğlu, F. S. (2013). Türk Ceza Kanununda Yer Alan Bilişim Alanındaki Suçlar Ve Karşılaşılan Sorunların Yargı Kararları Işığında Değerlendirilmesi, İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, C.71, S.1, s.855-889, http://www.journals.istanbul.edu.tr/iuhfm/article/view /1023021510/1023020290 (Erişim tarihi: 05/04/2018)

360 Eker, age. s.125.

361 Dülger, age. s. 428.

362 Artuk, Gökçen, Yenidünya, Şerh. s. 6934; aski görüş için bkz. Yaycı, age. s. 92.

363 Akbulut, Sistemi Engelleme. s. 38; Kızıltan, age. s. 84; Yılmaz, Siber. s. 197.

364 Gürler, age. s. 122.

verinin kendisine, kullanımına ya da erişilebilirliğine müdahale edilmemektedir. Bu yüzden orijinal veriye herhangi bir zarar verilmemektedir. Oysa bu suç madde gerekçesinden de anlaşılacağı üzere, mala zarar vermenin özel bir düzenlemesidir. Bu sebeple bu iki durum birbiriyle bağdaşmamaktadır[365].

Ketizmen haricinde bu harekete bir eleştiri de Özbek-Kanbur-Doğan-Bacaksız'dan gelmiştir. Buna göre, bu eylemin muğlak olduğu, gerçek amacını ortaya koyamadığı, çünkü bir bilişim sisteminde gerçekleşecek her türlü eylem için mutlaka bir veri iletimi halinin mevcut olduğu, veri iletiminden kastın TCK 244/2'nin kabul ettiği verinin başka bir yere gönderilmesi olarak düşünülmesi gerektiği ileri sürülmektedir[366].

### 2.3.2. Manevi Unsur

Suçun manevi unsuru, kast ve taksirdir. Kast, doğrudan ve olası kast diye ikiye ayrılır. Doğrudan kast, suçu oluşturan fiilin bilerek ve istenerek işlenmesidir. Olası kast ise failin öngördüğü neticeyi kabul edip "olursa olsun" diyerek işlemesidir. Taksir de bilinçli taksir ve bilinçsiz taksir şeklinde ikiye ayrılmakta olup, bilinçli taksir, failin kendi deneyim ve tecrübelerine güvenerek yaptığı hareket ile meydana gelen neticeyi kabul etmemesi hali iken, bilinçsiz taksir, fail gerekli dikkat ve özen yükümlülüğüne uymaksızın yaptığı hareket ile suçun oluşması halidir[367].

Bu suçun karşılığı olan eski 765 sayılı kanunda suç için zarar vermek veya yarar sağlamak amacıyla yapılması gerektiği açıkça belirtilmişti. Yani eski kanunda bu suç için özel kast aranıyordu. Oysa 5237 sayılı TCK'nın 244/1. ve 2. fıkrasında yer alan suçlar için yarar sağlamak ya da zarar vermek amacıyla gibi ibarenin belirtilmemesi sebebiyle suç genel kastla işlenebilir hale gelmiştir[368].

---

365 Ketizmen'e göre bu fıkra maddeden çıkartılarak madde bütünlüğü sağlanmalı ya da 765 sayılı TCK'da olduğu gibi ayrı bir maddede ele alınması gerektiği belirtilmiştir. Ayrıntılı bilgi için bkz. age. s. 141.

366 Özbek, Doğan, Bacaksız, Tepe, age. s. 953.

367 Konu hakkında ayrıntılı bilgi için bkz. Artuk, Gökçen, Yenidünya, Ceza Genel. s. 450-518; Centel, Zafer, Çakmut, age. s. 379-404; Demirbaş, T. (2009). *Ceza Hukuku Genel Hükümler.* Ankara: Seçkin Yay. s. 341.

368 Pallı, age. s. 178.

Kast, failin suçun kanuni tanımındaki unsurları bilmesi ve istemesidir[369]. Fail, bilişim sisteminin işleyişini engellediğini, bozduğunu ya da bilişim sistemindeki veriyi bozduğunu, yok ettiğini, değiştirdiğini, erişilmez kıldığını, verilere başka bir yere gönderdiğini bilmelidir. Failin hangi saikle hareket ettiğinin bir önemi yoktur. Doğrudan kasta ilişkin herhangi bir düzenleme olmaması sebebiyle, suç olası kastla da işlenilebilir[370]

Kanunda suçun taksirle işlenebileceğinin öngörülmemesi sebebiyle, suç taksirle işlenemez, işlenmesi halinde ceza verilemez. Bununla birlikte bilişim sistemlerinin hayatımızda önemli bir yere sahip olması sebebiyle taksirli halinin en azından şikayete tabi suç olarak düzenlenmesi gerektiği doktrinde ileri sürülmüştür[371].

Failin yetkili olmadığı halde kendisini yetkili sanarak belli bir davranışı yapması halinde, fail hata yapmış sayılır. Bu tür hatalar failin lehine olarak değerlendirilecektir[372].

### 2.3.3. Hukuka Aykırılık Unsuru

5237 sayılı TCK hukuka uygunluk nedenlerini, 24/1. maddesinde kanunun hükmünü yerine getirme, 25/1. maddesinde meşru savunma, 26/1. maddesinde hakkın kullanılması, 26/2. maddesinde de ilgilinin rızası olacak şekilde dört ana grupta toplamıştır[373].

Bu suç açısından en önemli hukuka uygunluk nedeni, ilgilinin rızasıdır. İlgilinin rızası yapılan eylemi suç olmaktan çıkartır. Bu rızanın suçun işlendiği anda mevcut olması gerekir. Rızanın açık veya zımni olmasının ise bir önemi yoktur.

Bir bilişim sisteminin teknik sorumlusuna, bilişim sistemiyle ilgili gerekli izinler verilmiştir. Bu çerçevede sisteme yapılacak saldırılardan korunmak için sisteme yüklenilen virüs programları ve bu programların kullanılması eylemi hukuka uygun sayılacaktır[374]. Aynı doğrultuda, bilişim sistemini onarmak ve sistemdeki verileri kurtarabilmek için teknisyenin bazı dosyaları silmesi hukuka uygun sayılacaktır[375]**.** Fakat bu izinler verilerin bilerek ve istenerek zarar verilmesi ya da

---

369 Demirbaş, T. (2009). age. s. 341; Hakeri, H. (2009). *Ceza Hukuku Genel Hükümler*. Ankara: Seçkin Yay. s. 177.

370 Erdoğan, age. s. 230; Koca,Üzülmez, age.s.831; Dülger, age. s. 435.

371 Erdoğan, age. s. 230; Kurt. age. s. 169; Taşkın, age. s. 53.

372 Hafızoğulları, Özen, age. s. 450, 452.

373 Özgenç, İ. (2011).*Türk Ceza Hukuku Genel Hükümler*. Ankara: Seçkin Yay. s. 278.

374 Hafızoğulları, Özen, age. s. 449.

375 Pallı, age. s. 171.

yok edilmesini içermez. Bu şekilde yetkisini kötüye kullanan fail kendisine verilen rızanın sınırlarını aşmış olacak ve yaptığı eylemden sorumlu tutulacaktır. Failin bilmeden bir zarar vermesi halinde yukarı da belirtildiği üzere suçun taksirli hali suç oluşturmayacağı için kendisine herhangi bir ceza verilmeyecektir[376] .

Bu konuda rızanın kim tarafından verileceği önemli olup suç açısından tespiti gerekmektedir. Bir bilişim sistemi sahibinin rızası, eylemi her zaman hukuka uygun hale getirmez. Kimi zaman bu bilişim sistemi sahibi bilişim sistemini kullanmak üzere yetkilerini başkasına devretmiş olabilir. Bu halde rızanın, devralan kişi tarafından verilmesi gerekecektir. Aynı doğrultuda bir bilişim sistemiyle beraber içerisindeki programlar yani donanımlar da devralınabilir. Bu halde de rıza devralan kişi tarafından verilmelidir. Bilişim sistemi sahibi, bilişim sistemini ve donanımını bir başkasına kiralayıp, kiralayanın bu kullanım yetkisini aşacak şekilde bilişim sistemini kullanması halinde ya da içerisindeki verilere kullanamayacak şekilde zarar vermesi halinde artık kiralayan kendisine verilen rızanın sınırlarını aşmış olacağı için TCK'nın 244/2 maddesinden sorumlu tutulacaktır[377].

Suç için bir başka hukuka uygunluk nedeni de kanunun verdiği emir ve görevin ifasıdır. Örneğin, 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanunda, belirli durumlarda suç içeren bir internet sitesine erişimin engellenebileceği hüküm altına alınmıştır. Bu sebeple yetkililerce suç içeren bir internet sitesinin kapatılması halinde eylem suç oluşturmayacaktır[378]. Yine vergi borçlarının silinmesi yolunda karar alınması halinde bu çerçevede vergi borçlarını silen kişiye herhangi bir ceza verilmeyecektir[379]. Aynı şekilde hakim kararına istinaden sanığın bilişim sistemlerinde yapılan arama ve verilerin kopyalanması, hakim kararına istinaden iletişimin denetlenmesi ve sanığın elektronik postalarının kopyalanması hukuka uygun sayılacaktır[380].

Bu suç için doktrinde bir kısım yazarlar tarafından ilgilinin rızası ve kanun hükmünü icra etmek haricinde başka bir hukuka uygunluk nedeni olmadığı belirtilmiş ise de[381], Pallı ve Avşar/Öngören, bu suç açısından meşru müdafaanın da

376 Soyaslan ,age. s. 706.
377 Akbulut, Sistemi Engelleme. s. 21.
378 Özbek, Doğan, Bacaksız, Tepe, age. s. 959; Tezcan, Erdem, Önok, age. s. 913.
379 Akbulut, Sistemi Engelleme. s. 40.
380 Koca, Üzülmez, age.s.831.
381 Özbek, Doğan, Bacaksız, Tepe, age. s. 961.

hukuka uygunluk nedeni olduğu ifade edilmiştir. Avşar/Öngören'e göre bir web sitesinden başkalarına sürekli hakaret edilmesi sebebiyle bu sitenin fiziken engellenmesi halinde yapılan eylemin hukuka uygun bir eylem olacağı ifade edilmiştir[382]. Meşru müdafaa TCK'nın 25/1. maddesinde düzenlenmiştir. Buna göre, gerek kendisine gerekse bir başkasına ait bir hakka yönelmiş, gerçekleşen, gerçekleşmesi veya tekrarı muhakkak olan haksız bir saldırıyı o anda hal ve koşullara göre saldırı ile orantılı biçimde defetmek zorunluluğu ile işlenen fiillerden dolayı faile ceza verilemeyecektir. Bize göre de bir bilişim sistemine karşı yapılan haksız bir saldırıyı orantılı biçimde defetmek isteyen kişiye meşru müdafaadan dolayı ceza verilmemesi gerekmektedir.

### 2.4. Suçun Özel Görünüş Biçimleri

#### 2.4.1. Teşebbüs

Bu suça teşebbüs mümkündür. Failin icra hareketlerine başlamasından sonra bu icra hareketleri yarıda kalabileceği gibi, suçun icra hareketleri tamamlandıktan sonra fakat neticenin meydana gelmeden failin elinde olmayan nedenlerle suçu gerçekleştirememesi şeklinde de olabilir[383].

Bir bilişim sistemindeki verilere zarar vermek isteyen bir kişi sisteme virüs gönderdikten sonra bu virüs bilişim sistemi sahibi tarafından tespit edilip etkisiz hale getirilmesi halinde eylem teşebbüs aşamasında kalacaktır. Benzer durum mantık bombası veya DoS saldırıları içinde geçerli olacaktır[384]. Aynı doğrultuda bir bilişim sistemine giren failin, sistemin işleyişini bozmak isterken birden sistem elektriğinin kesilmesi halinde de eylemi teşebbüs aşamasında kalacaktır[385].

Seçimlik hareketlerden herhangi birisinin yapılması suç için yeterli olacaktır. Bu seçimlik hareketlerden birisinin tamamlanması, diğer hareketlerden herhangi birisinin ise teşebbüs aşamasında kalmış olması halinde, faile tamamlanmış suçtan dolayı ceza verilmesi gerekecektir. Örneğin, failin verilerin tamamını silmek isterken bir kısım verileri silmesi halinde, verilerin değiştirilmesi suçu tamamlanmış olacak ve faile bu suçtan ceza verilecektir[386].

---

382 Avşar, Öngören, age. s. 138; Pallı, age. s. 171; aksi görüş için bkz. Erdoğan, age. s. 201.

383 Dülger, age. s. 436.

384 Dülger, age. s. 436; Erdoğan, age. s.232; Yılmaz, Siber. s. 200; Akbulut, Sistemi Engelleme. s. 43

385 Özbek, Doğan, Bacaksız, Tepe, age. s. 961; Erdoğan, age. s. 233.

386 Artuk, Gökçen, Yenidünya, Ceza Özel. s. 851; Akbulut, Sistemi Engelleme. s. 44; Dülger, age. s. 436.

Fail, bilişim sistemine müdahale ettikten sonra fakat netice meydana gelmeden önce eylemine kendi çabasıyla son verirse gönüllü vazgeçme gündeme gelecek ve faile bu suçtan dolayı ceza verilmeyecektir. Ancak failin bu aşamaya kadar yaptığı, yani bilişim sistemine girme eylemi tamamlanmış olacak, TCK'nın 243. maddesinde yazılı bilişim sistemine girmekten dolayı kendisine ceza verilecektir.

Failin verileri değiştirdikten sonra pişmanlık duyarak bu verileri eski hale getirmesi halinde gönüllü vazgeçmeden yararlandırılması gerektiği doktrinde ileri sürülmüş ise de[387]; gönüllü vazgeçme, failin kendi çabalarıyla suçun tamamlanmasını veya neticenin gerçekleşmesini önlemesi halidir. Oysa etkin pişmanlık suçun tüm unsurlarıyla tamamlanmasından sonra failin pişmanlık göstermesi halidir[388]. Yukarıda bahsedilen olayda fail verileri değiştirdiği an suç tüm unsurlarıyla gerçekleşmiş sayılacaktır. Artık bu aşamada gönüllü vazgeçme değil, etkin pişmanlık hükümlerinin uygulanması gerekecektir. TCK"nın 244. maddesi etkin pişmanlık hükümlerine yer vermediği için fail bu durumdan istifade edemeyecektir. Hakim TCK'nın 61. maddesi doğrultusunda cezayı belirlerken failin bu durumunu göz önünde bulunduracak ve takdiri indirim nedeni olarak değerlendirecektir.

### 2.4.2. İştirak

5237 Sayılı TCK'nın 244. maddesinde yer alan suçlarda faille ilgili özel bir belirleme yapılmamıştır. İştirak açısından TCK'nın 37, 38, 39 ve 40. maddelerinde yazılı iştirake ilişkin genel kurallar bu suç açısından da geçerlidir  Dolayısıyla bu suç için iştirak şekillerinin gerçekleşmesi mümkündür.

### 2.4.3. İçtima

#### 2.4.3.1. Genel Olarak

TCK'nın 43/1. maddesinde, bir suç işleme kararının icrası kapsamında aynı suçun bir kişiye karşı farklı zamanlarda işlenmesi halinde faile tek ceza verileceği belirtilmiştir. TCK'nın 244. maddesinde yazılı suçların zincirleme şekilde işlenmesi mümkündür. Örneğin, failin bilişim sistemine farklı zaman aralıklarında birden çok veri yerleştirmesi halinde eylemi tek sayılacak fakat kanunun öngördüğü miktarda arttırım yoluna gidilecektir. Nitekim Yargıtay vermiş olduğu bir kararında şüphelilerin çok sayıda saldırı iletisi göndererek siteye başkalarının erişimini

387 Kurt, age. s. 265, 266.

388 Centel, Zafer, Çakmut, age. 464, 470.

engellediğinin belirtilmesi karşısında sanığa TCK 244/1 ve 43/1 maddeleri gereği ek savunma hakkı verilmesi[389], sanığın MSN ile facebook hesaplarının şifrelerinin değiştirilmesi iki farklı bilişim sistemi olmasından dolayı bir suç işleme kararının icrası kapsamında değişik zamanlarda her bir mağdura karşı aynı eylemi birden fazla işleyen sanık hakkında TCK'nın 43/1. madde ve fıkrasında düzenlenen zincirleme suç hükmünün uygulanması gerektiği şeklinde zincirleme suç hükümlerinin uygulanmasının gerekeceğini ifade etmiştir[390]. Aynı doğrultuda sanığın değişik tarihlerde dört kez, dört farklı ders notunu değiştirmesi halinde de TCK'nın 43/1. maddesinin tatbik edilmesi gerekecektir[391].

TCK'nın 43/2. maddesinde aynı neviden fikri içtima düzenlenmiştir. Buna göre, aynı suçun birden fazla kişiye tek bir fiille işlenmesi halinde yine faile tek cezanın verileceği belirtilmiştir. TCK'nın 244. maddesinde yazılı suç açısından da bu hüküm uygulanabilir. Örneğin, failin aynı virüsü tek bir hareketle (e-posta ile) birden fazla kişiye göndermesi halinde ya da bir internet sitesine gönderilen virüs ile çok sayıda kişinin bu virüsü bilişim sistemine indirmesi ve bilişim sistemlerinin zarar görmesi halinde, aynı neviden fikri içtima kuralları uygulanarak mağdur sayısı kadar suç değil, tek suç üzerinden ceza verilecek fakat verilecek ceza belli oranlarda arttırılacaktır[392].

Bu suçlar kesintisiz (mütemadi) olarak da işlenilebilir. Örneğin, bilişim sisteminin engellenmesi ani olarak değil, belli bir süre devam eden harekettir. Bu eylemde suç kesintinin gerçekleştiği anda tamamlanmış olacaktır. Aynı zamanda zamanaşımı süresi de bu tarihte başlayacaktır[393].

TCK'nın 44. maddesi, bir fiille birde fazla suçun oluşması halinde faile en ağır olan cezadan hüküm kurulmasını yani farklı neviden fikri içtima kuralını düzenlemiştir. Failin bir bilişim sistemine veri yükleyerek bu verinin başka bir suçta mağdur aleyhine delil olarak kullanılması halinde, fail hem TCK'nın 244/2 maddesinde yazılı suçtan hem de TCK'nın 271. maddesinde yazılı suç uydurma ya da 267. maddesinde yazılı iftira suçundan cezalandırılacaktır. Aynı doğrultuda fail sahte belge düzenleyerek sistemdeki verileri değiştirebilir. Bu halde hem belgede sahtecilik hem de verileri değiştirme suçunu işlemiş olacaktır. Her iki halde de fail

389 Yar. 8 CD. 29/02/2016T, 2015/14793E, 2016/2407 K. sayılı ilamı
390 Yar. 12 CD. 11/10/2017 T. 2016/10818E, 2017/7390 K. sayılı ilamı
391 Yar. 8. CD. 08/01/2014 T., 2012/33044 E., 2014/236 K. sayılı ilamı
392 Dülger, age. s. 437.
393 Dülger, age. s. 427.

tek bir hareketle birden fazla farklı suçu işlemiş olması sebebiyle hakkında TCK'nın 44. maddesi uygulanacak ve en ağır olan suçtan cezalandırılma yoluna gidilecektir[394]. Benzer durum TCK'nın 244/1 ve 2. fıkraları için de geçerli olacaktır. Fail bilişim sistemindeki verileri değiştirirken aynı zamanda o bilişim sistemini bozabilir. Yani TCK'nın hem 244/2 hem de 244/1. maddesinde yazılı suçları işlemiş olabilir. Bu halde de fikri içtima kuralları geçerli olacak ve faile en ağır olan suçtan ceza verilecektir[395].

TCK'nın 244. maddesi ile 243. maddesi arasındaki ilişki, doktrinde bir grup yazara göre, TCK'nın 243. maddesinde yazılı bilişim sistemine girme suçu inceleme konusu suç tipi açısından bir geçit suçu oluşturmayacağı, TCK'nın 244. maddesindeki yazılı suçların işlenebilmesi için mutlaka TCK'nın 243. maddesindeki yazılı suçun da işlenmesinin gerekmeyeceği ifade edilerek bilişim sisteminin çekiçle kırılması ya da suya atılması halinde TCK'nın 243. maddesi işlenmeden 244. maddesinin işlenmiş olacağı ifade edilmiştir. Dolayısıyla fail TCK'nın 244. maddesindeki yazılı suçları işlemek için TCK'nın 243. maddesindeki suçu da işlemesi halinde her suçtan ayrı ayrı ceza verilmesi gerekeceği belirtilmiştir[396]. Bizim de katıldığımız çoğunluk görüşü ise, TCK'nın 244/1. ve 2. fıkralarında yazılı suçların işlenebilmesi için genellikle failin TCK'nın 243. maddesinde yazılı bilişim sistemine girme suçunu da işlemiş olacağını düşünmektedir. Bu halde TCK'nın 243. maddesinde yazılı suç tipi geçitli suç kabul edilecek ve faile sadece TCK'nın 244. maddesinde yazılı suçtan dolayı ceza verilecektir. Gerçekten de bir bilişim sistemindeki verileri değiştirmek isteyen failin, bu suçu gerçekleştirebilmek için aynı zamanda bilişim sistemine de girmesi gerekecektir. Bu halde TCK'nın hem 243. maddesi hem de 244. maddesi oluşmuş olacaktır. Fakat failin TCK'nın 44. maddesinde yazılı fikri içtima kuralları gereği en ağır olandan cezalandırılması gerekecektir[397].

TCK'nın 244. maddesi ile 243. maddesindeki bir diğer sorun hangi kanun maddesinin tatbik edilmesi gerekeceği noktasında çıkmaktadır. TCK'nın 243/3. maddesinde bilişim sistemine girmenin nitelikli hali düzenlenmiştir. Buna göre fail

---

394 Dülger, age. s. 428; Akbulut, Sistemi Engelleme. s. 46.

395 Akbulut, Sistemi Engelleme. s. 44; Dülger, age. s. 437.

396 Dülger, age. s. 438.

397 Artuk, Gökçen, Yenidünya, Ceza Özel, s. 851; Koca, Üzülmez, age. s. 833; Soyaslan, age. s. 707; Erdoğan, age. s. 236; Apaydın, C. (2016). Bilişim Sistemine Girme Suçu. TAAD. Y.7, S.24. s. 292.

hem bilişim sistemine girer hem de verileri yok eder ya da değiştirirse altı aydan iki yıla kadar hapis cezası ile cezalandırılacaktır. Bu fıkra bir nevi verilerin yok edilmesini düzenlemektedir. TCK'nın 244/2. maddesi de verilerin yok edilmesini içermektedir. Failin yaptığı eylem hangi kanun maddesine girdiğinin tespiti bu sebeple zor olmaktadır. Hangi kanun maddesinin uygulanması gerekeceğinin tespitini failin kastı belirler. Bunun için failin kastı açıkça tespit edilmelidir. TCK'nın 243/3. maddesinin uygulanabilmesi için failin verileri yok etme veya değiştirme kastının bulunmaması gerekir[398]. Aynı zamanda bilişim sistemine giren failin verilerin yok edilmesinden sorumlu tutulabilmesi için TCK'nın 23. maddesi gereğince en azından taksirle bu zarara sebebiyet vermesi gerekecektir. Eğer failin kastı verileri yok etmek ise yukarıda da belirtildiği üzere TCK'nın 243. maddesi geçitli suç olacak ve fail sadece TCK'nın 244 .maddesinden sorumlu tutulacaktır[399]. Bununla birlikte failin saikinin açıkça tespit edilemediği hallerde, failin daha lehine olan TCK'nın 243. maddesinden hüküm kurulması gerekecektir. Nitekim bu konuda bir çok Yargıtay kararında sistemi ya da veriyi bozduğu tespit edilemeyen sanıklar hakkında TCK'nın 243. maddesinde yazılı suçtan cezalandırılma yolu tercih edilmiştir[400].

Fail TCK'nın 244/1 ve 2. fıkralarındaki suçları işlerken aynı zamanda TCK'nın 244/4. maddesinde yazılı haksız yarar sağlama suçunu da işlemiş olabilir. Bu halde fail iki suçtan cezalandırılmayacaktır. Çünkü TCK'nın 244/4. maddesinde yazılı suçun oluşabilmesi için failin 244/1 veya 2. maddede yazan suçları işlemesi gerekmektedir. Bu durum kanun maddesinde "*yukarıdaki fıkralarda tanımlanan fiillerin işlenmesi suretiyle*" şeklinde açıkça belirtilmiştir. Dolayısıyla 4. fıkradaki suçun işlenmesiyle 1. ve 2. fıkradaki suçlar eriyecek bir bütün halinde 4. fıkrada belirtilen suçu oluşturacaktır. Yani 1. ve 2. fıkradaki suç 4. fıkrada yazılı suçun unsuru niteliğinde olup, bileşik suç sayılacak ve fail sadece 4. fıkradan cezalandırılacak, 1. ve 2. fıkradan ceza verilmeyecektir[401].

---

398 Karakehya, H. (2009). Türk Ceza Kanunu'nda Bilişim Sistemine Girme Suçu. TBB Dergisi. S:81. Y:2009.s. 18.

399 Apaydın, age. s. 273; Gürocak, İ.Bilişim Sistemine Girme. http://www.ismailgurocak.av.tr/makale/B%C4%B0L%C4%B0%C5%9E%C4%B0M%20S%C4%B0STEM%C4%B0NE%20G%C4%B0RME%20SU%C3%87U-%C4%B0SMA%C4%B0L%20G%C3%9CROCAK.pdf (erişim tarihi 16/04/2018)

400 Bkz.Yar. 8 CD. 27/09/2017 T, 2016/11236 E, 2017/10500K; 8. Cd. 03/05/2017 T, 2016/12634E,2017/4967 K. sayılı ilamı.

401 Özbek, Doğan, Bacaksız, Tepe, age. s. 961; Koca, Üzülmez, age. s. 833.

Bununla birlikte fail bazen birden fazla farklı suçu fikri içtima kapsamı dışında kalacak şekilde işlemiş olabilir. Bu gibi hallerde failin her iki suç açısından ayrı ayrı cezalandırılması yoluna gidilecektir. Nitekim yargıtay vermiş olduğu bir kararda sanığın, katılanın cep telefonunu katılandan habersiz kendi kullandığı bilgisayara bağlayarak içerisinde bulunan rehber ve media dosyalarının tamamını ele geçirdiği ve cep telefonundaki kayıtları sildiği iddia ve kabul edilen olayda, sanığın sübut bulan eylemleri nedeniyle TCK'nın 244/2. maddesinde düzenlenen sistemi engelleme, bozma, verileri yok etme veya değiştirme, aynı Kanunun 134/1 maddesinde düzenlenen özel hayatın gizliliğini ihlal ve 136/1 maddesinde düzenlenen verileri hukuka aykırı olarak verme veya ele geçirme suçlarını oluşturduğu gözetilmeden sadece TCK'nın 136/1. maddesinde düzenlen verileri hukuka aykırı olarak verme veya ele geçirme suçundan sanığın mahkumiyete karar verilmesini hukuka aykırı bularak yerel mahkeme kararını bozmuştur[402]. Aynı doğrultuda oluşa ve dosya kapsamına göre, sanık Oktay'ın, kız arkadaşı olan mağdur Sevil ile aralarındaki arkadaşlık ilişkisi sona erdikten sonra, mağdura ait facebook hesabının önceden bildiği internet şifresini, onun bilgisi ve rızası dışında değiştirerek, hakkı bulunmadığı halde giriş yaptığı ve mağdurun facebook hesabında beraber oldukları dönemde mağdurun bilgisi dahilinde kaydettiği cinsel içerikli görüntülerini yayımlayıp, mağdurun facebook hesabına erişimini engellemesi biçiminde sübut bulan eylemlerinin TCK'nın 244/2. maddesindeki sistemi engelleme, bozma, verileri yok etme veya değiştirme ve aynı Kanun'un 134/2. maddesinde yazılı özel hayatın gizliliğini ihlal suçlarını oluşturduğu ifade edilmiştir[403].

#### 2.4.3.2. Mala Zarar Verme Suçu Açısından

TCK'nın 151. maddesinde yer alan mala zarar verme suçu ile TCK'nın 244. maddesinde yazılı suç arasındaki ilişki doktrinde tartışmalıdır. Özgenç'e göre, sistemin somut unsurlarına verilen zararların mala zarar verme suçunu oluşturacağını, sistemin fiziki varlığına zarar vermeksizin elektronik ortamda verilen zararların ise bilişim suçunu oluşturacağını ifade ederek bu ayrımın her iki suçu oluşturan malvarlığı değerlerinden kaynaklandığını ifade etmiştir[404].

Kurt ve Artuk/Gökçen/Yenidünya bozmak eylemi ile mala zarar verme suçunun oluşacağını, bununla birlikte bilgisayarın kırılmasıyla hem mala zarar verme

402 Yar. 12 CD. 18/10/2017 T. 2016/10576E, 2017/7642K. sayılı ilamı.
403 Yar. 12 CD.24/05/2017 T, 2015/13308 E, 2017/4272 K. sayılı ilamı.
404 Özgenç, İ. (2005). *Türk Ceza Kanunu*. Ankara: Seçkin Yay. Gazi Şerhi. s. 989.

hem de bilişim sisteminin işleyişinin bozulacağı, tek bir fiil ile birden fazla hükmün ihlali nedeniyle fikri içtima kuralı gereği en ağır olan cezadan hüküm kurulması gerektiğini ifade etmiştir[405].

Dülger ise mala zarar verme suçunun konusunu taşınır veya taşınmaz malların oluşturduğunu, bilişim alanındaki suçun ise bilişim sistemi yanında verilerin oluşturduğunu, buradaki bilişim sisteminden kastın duran eşya değil, bilişim sistemi olarak kullanılan, işlerliği olan ve fayda sağlayan araç durumunda bulunduğunu, dolayısıyla her iki hükmün birbirinden farklı nitelikte olduğunu ve farklı hukuksal değerleri koruduğunu, her iki suç tipi arasında özel-genel hüküm ilişkisi olmadığını, bu yüzden sırf mala zarar vermek kastıyla yapılan eylemlerde TCK'nın 244. maddesinin uygulanamayacağını ifade etmiştir[406].

Erdoğan, Yazıcıoğlu gibi TCK'nın 151. maddesinin oluşabilmesi için ortada bir "mal" olmasının gerekeceğini, verilerin mal olarak değerlendirilemeyeceğini, bu durumda suçta ve cezada kanunilik ve kıyas yasağı gereği TCK'nın 151. maddesinin tatbik edilmesinin gerekeceğini ifade etmiştir[407].

Bize göre daha önce de belirttiğimiz üzere, hangi kanun maddesinin tatbik edilmesi gerektiği failin kastına göre belirlenmelidir. Failin, bilişim sistemi içerisinde bulunan bir veriye zarar vermek kastıyla hareket etmesi halinde TCK'nın 244. maddesi; sırf mala zarar vermek amacıyla hareket etmesi halinde ise mala zarar verme suçunun tatbik edilmesi gerekecektir. Gerçekten de vitrinde sergilenen bir bilgisayara karşı işlenen suç mala zarar verme niteliğinde iken, bir akademisyenin sistemindeki bilgilerini bozmak, ya da devamsızlıklarını ortadan kaldırmak isteyen bu doğrultuda bilgisayara zarar veren failin TCK'nın 244. maddesinden cezalandırılması gerekecektir. Aynı doğrultuda bir bilgisayarın kasasına sprey boyayla yazı yazan failin, bilişim sistemine yönelik bir kastının olmaması sebebiyle, sadece mala zarar verme suçundan cezalandırılması gerekecektir.

### 2.5. Suçun Nitelikli Halleri

#### 2.5.1. Daha Az Cezayı Gerektiren Haller

Hem Eski 765 sayılı Kanunda hem de Yeni 5237 sayılı Kanunda bu suç için herhangi bir özel hafifletici neden kanunda belirtilmemiştir. Hakim cezayı

405 Kurt, age. s. 165; Artuk, Gökçen Yenidünya, Ceza Özel, s. 851.
406 Dülger, age. s. 438.
407 Erdoğan, age. s. 237; Yazıcıoğlu, TCK 244/4 üzerine düşünceler, s. 6.

belirlerken sadece TCK'nın 62. maddesinde yazılı takdiri indirim nedenlerini uygulayabilir.

### 2.5.2. Daha Fazla Cezayı Gerektiren Haller

TCK'nın 244/3. maddesi "*bir banka veya kredi kurumuna veya kamu kurum veya kuruluşuna ait bilişim sistemi üzerinde işlenmesi*" şeklinde düzenleme ile suçun nitelikli halini yaptırım altına almış ve faile verilecek olan cezanın yarısı oranında artırılması gerektiğini belirtmiştir.

Bakıldığı zaman, bu nitelikli hal ile herkes tarafından zarar görülme olasılığı bir hayli yüksektir. Örneğin Adalet Bakanlığına ait UYAP sisteminin engellenmesi halinde tüm adalet hizmetleri zarar görecektir. Aynı doğrultuda Nüfus müdürlüklerine ait bir sistemin çökertilmesi, bir bankanın bilgisayar sisteminin çökertilmesi hallerinde de olduğu gibi nüfustan veya bankadan hizmet almak isteyen tüm kişilerin bu suçtan zarar görecek olmaları sebebiyle, yasa koyucu konuyu nitelikli hal olarak düzenleme yoluna gitmiştir[408].

Bu nitelikli halde, tüm kamu kurum ve kuruluşları, devletin merkez ve taşra teşkilatı ile yerel yönetimler, KİT'ler yani geniş anlamda devletin anlaşılması gerekecektir. Banka ya da kredi kurumu niteliğinde olmayan özel kurumlar, şirketler ile vakıflar ve derneklere ait bilişim sistemleri üzerinden işlenmesi halinde nitelikli halin uygulanması, özel ceza içeren yasalarda yorum yapılamayacak olması sebebiyle mümkün olmayacaktır. Doktrinde bu fıkra, kredi kurumu veya kamu kurum ve kuruluşlarıyla sınırlı tutulması sebebiyle eleştirilmektedir[409]. Nitekim yargıtay vermiş olduğu bir kararında "*Sanıkların İl Emniyet Müdürlüğüne ait internet sitesine izinsiz olarak girerek işleyişini engelleyip bozmaktan ibaret eylemlerinin TCK.nun 244/1-3 maddelerine uyan suçu oluşturduğu gözetilmeden aynı Yasanın 244/2-3. maddesiyle uygulama yapılması aleyhe temyiz olmadığından bozma nedeni yapılmamıştır"* şeklinde yerel mahkeme kararına eleştiri konusu yapmıştır[410]. Aynı doğrultuda sanıkların okul ders notlarını ve devamsızlık durumlarını değiştirmek için Milli Eğitim Bakanlığına bağlı e-okul bilişim sistemini değiştirmekten ibaret eylemlerinde TCK'nın 244/3'ü uygulama konusu yapmayan yerel mahkeme kararını bozmuştur[411].

---

408 Koca, Üzülmez, age. s. 832.
409 Akbulut, Sistemi Engelleme. s. 41; Erdoğan, age. s. 197; Dülger, age. s. 433.
410 Yar. 8 CD. 15/05/2014 T. 2013/4359 E, 2014/12455K. sayılı ilamı.
411 Yar. 8. CD. 15/02/2017 T, 2016/3794 E, 2017/1405 K. sayılı ilamı.

Bilişim alanında işlenen suçların, suç işlemek için kurulmuş bir terör örgütü faaliyetleri çerçevesinde işlenmesi halinde cezanın yarı oranında artırılması gerekeceği 3713 sayılı Terörler Mücadele Kanunu'nun 5. maddesinde belirtilmiştir. Ancak bu hal çocuklar hakkında uygulanamayacaktır. Yani bilişim alanında yer alan suçları yetişkin bir kişi tarafından terör amacıyla işlenmesi halinde 3713 sayılı TMK'nın 4 ile 5. maddeleri gereğince verilecek olan ceza yarı oranında artırılacaktır[412]. Nitekim sanığın olay tarihinde Etimesgut İlköğretim Okuluna ait etimesgutilkögretim.meb.k12.tr uzantılı web adresine girdiği, kürdistan ve bölücübaşı Abdullah Öcalan lehine propaganda yaparak hacklendiği iddia edilen eylemde mahkemece sanığa 244/1. maddesinden uygulama yapılmış yargıtay 16 CD. suçun silahlı terör örgütü faaliyeti çerçevesinde işlenmesi sebebiyle verilen cezada arttırım yapılması gerekirken yapılmadığını belirtmiştir[413].

Doktrinde görev yaptıkları yer ve konumları gereği kamu görevlilerin veya banka görevlilerinin bu suçları işlemesi hallerinde cezayı artıran nitelikli hal olarak düzenlenmesinin gerektiği, bu kişilerin konumları gereği dışarıdan müdahalede bulunmak isteyen kişilere göre sistemlere çok daha kolay zarar verebileceklerini, bu yüzden konunun düzenlenmesi gerektiği ileri sürülmüştür[414]. Kanaatimizce, böyle bir düzenleme yersiz olacaktır. Çünkü kanun cezanın alt ve üst sınırlarını çizmiştir. Basit bir eylemle suçu işleyen kişiye alt sınır olan 1 yıl gibi bir ceza verilebilecekken, somut olaya göre bir kamu görevlisinin suçu işlemesi halinde 5 yıla kadar ceza verilebilmesi mümkündür. Kamu görevlilerine duyulan güven ya da onların diğer kişilere nazaran suçları daha kolay işleyebilmesi bir çok kanun maddesi için de geçerlidir. Örneğin, bir kamu görevlisi ile normal bir kişinin kamu binasında hırsızlık yapması ya da bir uyuşturucu maddeyi normal bir kişi yerine Cumhuriyet Savcısının nakletmesi örnek olarak verilebilir. Her iki suçun da kamu görevlileri tarafından işlenmesi diğer kişilere nazaran daha kolay olacaktır.

### 2.6. Yaptırım

Eski 765 sayılı kanunun 525/b-1 maddesinde bu suç için hem hürriyeti bağlayıcı ceza hem de para cezası öngörülmüştü. 5237 sayılı TCK ile para cezası kaldırılmış yalnızca hapis cezasına yer verilmiştir.

412 Dülger, age. s. 380.
413 Yar. 16 CD. 26/04/2016 T, 2016/1813 E, 2016/2611 K sayılı ilamı.
414 Erdoğan, age. s. 197; Dülger, age. s. 434; Pallı, age. s. 166.

Buna göre TCK'nın 244/1. maddesinde yazılı bilişim sistemlerinin işleyişini engelleyen ya da bozan kişinin 1 yıldan 5 yıla kadar hapis; 244/2. maddesinde yazılı suçun işlenmesi halinde ise 6 aydan 3 yıla kadar hapis cezası öngörülmektedir. Ceza belirlenirken hakim TCK'nın 61. maddesi gereği takdir yetkisi kullanarak bu sınırlar arasında bir ceza tayin edecektir.

Hakimin faile iki yıldan az bir ceza vermesi halinde CMK'nın 231. maddesinde yazılı hükmün açıklanmasının geri bırakmasına (HAGB) diğer şartları da taşıyorsa karar verebilir. HAGB'ye karar verilmezse TCK'nın 51. maddesinde yazılı diğer şartları da taşıması halinde erteleme kararı verebilir. Failin 1 yıldan az ceza alması halinde yine hakim HAGB ve erteleme kararı verebileceği gibi cezasını TCK'nın 50. maddesinde yazılı seçenek yaptırımlardan birisine ya da birkaçına da çevirebilir.

TCK'nın 60. maddesinde tüzel kişiler hakkında yaptırım müessesi düzenlenmiştir. aynı maddenin 4. fıkrasında "*bu madde hükümleri kanunun ayrıca belirttiği hallerde uygulanır"* şeklindedir. dolayısıyla suç içeren bir ceza normunda tüzel kişiler hakkında yaptırımdan bahsedilmezse bu maddenin uygulanma olasılığı olmayacaktır.

TCK'nın bilişim alanındaki suçları düzenleyen 10. bölümün son maddesinde yani 246. maddesinde "*bu bölümde yer alan suçların işlenmesi suretiyle yararına haksız menfaat sağlanan tüzel kişiler hakkında bunlara özgü güvenlik tedbirine hükmolunur*" hükmü yer almaktadır. TCK'nın 244. maddesinde yazılı suçların bir tüzel kişi lehine işlenmesi halinde ilgili tüzel kişi hakkında TCK'nın 60. maddesi uygulama alanı bulacak ve bu tüzel kişiye iznin iptali ya da müsadere kararı verilebilecektir. Ancak işlenen fiile nazaran daha ağır sonuçların çıkması halinde hakimin bu tedbirlere hükmetmeyebileceği TCK'nın 60/3. maddesinde ayrıca belirtilmiştir.

Bununla birlikte diğer şartların da oluşması halinde TCK'nın 54 ve 55. maddelerinde yazılı eşya ve kazanç müsaderesinin de uygulanması mümkündür.

Doktrinde, bu suç için öngörülen ceza miktarları suçun niteliği, takibi, suçları işleyen kişilerin çoğu zaman uzman kişilerden olması ve bunların tespitinin zor olması, farklı ülkelerden işlenebilir olması sebebiyle eleştirilmektedir[415]. 3 aydan 2 yıla kadar hapis cezası öngören hakaret fiiline kıyasen işlenmesi daha çok teknik

[415] Koca, Üzülmez, age. s. 833; Akbulut, Sistemi Engelleme. s. 47.

bilgi ve beceri isteyen (hacker) bilişim suçlarının cezası 6 aydan ya da 1 yıldan başlaması caydırıcılık açısından çok etkili olamayacağı için bize göre de ceza miktarları bir hayli düşük kalmıştır.

### 2.7. Soruşturma ve Kovuşturma

Kanun maddesinde şikayetle ilgili herhangi bir düzenleme bulunmaması sebebiyle, suç re'sen dikkate alınıp re'sen soruşturulan suçlardandır. Bununla birlikte TCK'nın 11. maddesinde bir Türk vatandaşının yabancı ülkede işlediği bir suçta, failin Türkiye'de olması ve suçun aşağı sınırı olarak bir yıldan az hapis cezasının öngörülmesi halinde suç, takibi şikayete bağlı hale gelecek ve re'sen soruşturma ve kovuşturma yapılamayacaktır[416].

5235 sayılı Adli Yargı İlk Derece Mahkemeleri ile Bölge Adliye Mahkemelerinin Kuruluş, Görev ve Yetkileri Hakkında Kanun'un 10, 11 ile 12. maddelerine göre bu suç için görevli mahkeme Asliye Ceza Mahkemeleridir. Uygulamada bu suçlar genellikle TCK'nın 158/1-f maddesinde yazılı bilişim sistemleri kullanılmak suretiyle dolandırıcılık suçlarıyla karıştırılmaktadır. TCK'nın 158/1-f maddesinde yazılı suçlar ağır ceza mahkemeleri tarafından kovuşturulmaktadır. Bu şekilde bir olayın meydana gelmesi halinde delillerin takdiri ve değerlendirilmesi üst dereceli ağır ceza mahkemelerince yapılmalı ve ağır ceza mahkemelerince karar verilmelidir. Nitekim Yargıtay'ın bu konuda vermiş olduğu bir çok kararı mevcuttur[417].

Suçu hangi yetkili asliye ceza mahkemesinin inceleyeceği CMK'nın 12. maddesinde belirtilmiştir. Buna göre suçun işlendiği yer mahkemesi bu suçu incelemeye yetkili yer olacaktır. Suçun bilişim sisteminin ya da verinin olduğu yerde işlenmesi halinde suç yeri için bir sorun yoktur. Ancak netice ile hareketin farklı yerlerde söz konusu olması halinde, örneğin internet üzerinden işlenen suçlarda, suçun nerede işlendiğinin tespiti zor olacaktır. Bize göre fail eylemini nerede gerçekleştirdiyse örneğin, evinde başkasının bilişim sistemine virüs göndermiş ise suç yeri hareketin icra edildiği yer olan şüphelinin ikametgahı olacaktır. Ancak failin hareketi nerede yaptığı tam olarak tespit edilemezse bu durumda neticenin gerçekleştiği yer mahkemesinin yetkili olması gerekecektir[418]. Bununla birlikte suçun

---

416 Akbulut, Sistemi Engelleme. s. 49.

417 Bkz. Yar. 8 CD: 18/12/2013 T, 2013/735 E, 2013/29491 K; 8 CD. 16/04/2014 T, 2013/2817 E, 2014/9715 K; 23 CD. 12/01/2016 T, 2015/20254 E, 2016/135 K. sayılı ilamı.

418 Özbek, Doğan, Bacaksız, Tepe, age. s. 962.

işlendiği yerin tespit edilememesi halinde CMK'nın 13. maddesi uygulanacak ve sırasıyla şüpheli ya da sanığın yakalandığı, yakalanamamışsa yerleşim yeri, yerleşim yeri yok ise Türkiye'de en son adresinin bulunduğu yer, bunun da mümkün olmaması halinde ilk usul işlemin yapıldığı yer mahkemesi yetkili olacaktır.

Unutulmaması gereken bir husus da 02.12.2016 tarihli Resmi Gazete'de yayımlanarak aynı tarihte yürürlüğe giren 6763 sayılı Kanun'un 34. maddesiyle değişik 5271 sayılı CMK.nun 253. maddesi ve maddeye eklenen fıkraya göre uzlaşma hükümleri yeniden düzenlendiği ve SSÇ'ler için TCK'nın 244/2. maddesi uzlaşma kapsamına alındığıdır. Bu kapsamda SSÇ'nin üzerine atılı suçu işlediğinin düşünülmesi halinde uzlaşma hükümlerinin uygulanması gerekecektir[419].

## 3. BİLİŞİM SİSTEMİNİ KULLANARAK HAKSIZ ÇIKAR SAĞLAMA SUÇU

### 3.1. Genel Olarak

Eski 765 sayılı TCK'nın 525/b-2 maddesinde bu suç "*bilgileri otomatik işleme tabi tutmuş bir sistemi kullanarak kendisi veya başkası lehine hukuka aykırı yarar sağlamak*" şeklinde ifade edilmişti.

Yeni TCK'nın 244. maddesinin 4. fıkrasında "*bilişim sistemi aracılığıyla hukuka aykırı yarar sağlama suçu*" düzenleme altına alınmıştır. Bu fıkra, maddenin 1. ve 2. fıkrasına atıf yapılarak düzenlenmiştir.

Bu düzenleme ASSS'nin 8. maddesinde "*sahtekarlık yoluyla kendisi veya başkasına haksız maddi menfaat sağlamak amacıyla, bilgisayar verilerine herhangi bir şekilde yeni veriler ekleme, bilgisayar verilerini herhangi bir şekilde değiştirme, silme veya erişilmez kılma*" yer alan hükme paralel olarak iç hukukumuzda yaptırım altına alınmıştır[420].

Doktrinde bir kısım yazarlar bu düzenlemeyi, 1. ve 2. fıkradaki suçun nitelikli hali olarak görse de[421] kanaatimizce bu düzenlemenin nitelikli hal olarak

---

419 Bkz. Yar. 8 CD. 28/09/2017T, 2017/1265E, 2017/10581K; 8 CD:25/09/2017 T, 2017/16011 E, 2017/10323 K. sayılı ilamı.

420 Artuk, Gökçen, Yenidünya, Ceza Özel, s. 859.

421 Özbek, Doğan, Bacaksız, Tepe, age. s. 954; Pallı, age. s. 167.

sayılmaması gerekmektedir. Çünkü öncelikle fıkra ile bir suçun tüm unsurları belirlenmiştir. Aynı zamanda diğer nitelikli hallerde de olduğu gibi, nitelikli hal olabilmesi suçun temel şeklinin belirli oranlarda ya da miktar belirtilmek suretiyle artırım öngörülmesi gerekmekteydi. Tıpkı maddenin 3. fıkrasında "*verilecek ceza yarı oranında artırılır*" şeklinde belirtildiği gibi. Fakat maddenin bu fıkrasında belirli oranlarda artırım öngörülmemiş, bu suç işleyen kişinin 2 yıldan 6 yıla kadar hapis ve beş bin güne kadar adli para cezası öngörülmüştür. Bu sebeple bu suçun, bağımsız bir suç olarak değerlendirilmesi gerekmektedir[422]. Doğan, fıkra ile eylemin başka bir suçu oluşturmaması halinde bu hükmün uygulanamayacağının açıkça belirtilmesi sebebiyle yasa koyucunun bu suçu bağımsız bir suç olarak öngördüğünü, nitekim suçun tüm unsularının maddede belirtildiğini, fıkrada artırım oranı belirlemek yerine doğrudan cezanın belirlenmiş olması sebebiyle bu suçun bağımsız bir suç olduğunu ileri sürmüştür[423]. Koca ve Üzülmez, bu fıkranın bağımsız bir suç olduğunu, bu fıkranın bileşik suç olduğunu, 1. ve 2. fıkradaki suçların bu suçun unsurunu oluşturduğunu ifade etmiştir[424]. Nitekim Yargıtay da vermiş olduğu bir kararında sanığın, katılana ait kimlik bilgilerini kullanarak sahte nüfus cüzdanı çıkardığı, bu nüfus cüzdanına kendi fotoğrafını koyduğu, bu sahte nüfus cüzdanı ile katılan adına bir hesap açtırdığı, bu hesaptan başka bir katılanın verilerini kullanarak kendi hesabına havale yaptığı ve açtırdığı sahte hesaptan yatan paraların çektiği olayda, paranın sanığın açtırdığı hesaba gelene kadar katılana yönelik herhangi bir hilenin bulunmaması nedeniyle eylemin TCK'nın 244/4. maddesinde yazan suçu oluşturduğunu belirtmiş ve bizim görüşümüze uygun olacak şekilde TCK'nın 244/4. maddesinde yazan suçun bağımsız bir suç olduğunu belirtmiştir[425]. Aynı şekilde İstanbul BAM 17 CD. vermiş olduğu bir kararında, ilk derece mahkemesince "Bilişim Sistemine Hukuka Aykırı Müdahale Suretiyle Haksız Çıkar Sağlama" şeklinde kabul edildiği halde eylemin TCK 244/4 yerine TCK 244/1 olarak gösterilmiş olmasını maddi hata olarak değerlendirilerek bu suçun bağımsız bir suç olduğunu ifade etmiştir[426].

---

422 Aynı doğrultuda bkz, Hafızoğulları, Özen, age. s. 453; Erdoğan, age. s. 246-247; Dülger, age. s. 439; Tezcan, Erdem, Önok, age. s. 913.

423 Doğan, age. s. 144.

424 Koca, Üzülmez, age. s. 834.

425 Yar. 11. CD. 22/01/2008 T. 2007/8423 E, 2008/117K sayılı ilamı.

426 İstanbul BAM. 17. CD. 2017/1073 E, 2017/2222 K sayılı ilamı.

Fıkrada suçun oluşabilmesi için başka bir suçun oluşmaması gerektiğinin belirtilmesi sebebiyle bu düzenleme tali norm niteliğindedir. Norm, tali ve asli olmak üzere ikiye ayrılır. Asli normun olduğu hallerde tali norm uygulanamaz. Dolayısıyla bu suç tali norm sayılacak, suçla aynı zamanda dolandırıcılık, hırsızlık, güveni kötüye kullanma gibi suçların işlenmesi halinde asli norm sayılan bu suçlardan fail cezalandırılacak, tali norm olması sebebiyle bu suçtan ayrıca cezalandırılma yoluna gidilemeyecektir[427].

Fıkrada "*başka bir suç oluşturmaması*" şartının öngörülmüş olması sebebiyle, bu fıkranın tatbik edilebilmesi için eylemin başka bir suçu içermemesi gerekmektedir. Eylemin aynı zamanda başka bir suçu içermesi halinde bu maddeden değil, diğer suçtan fail cezalandırılacaktır. Bu düzenleme madde gerekçesinde, "*bu fıkra hükmüne istinaden cezaya hükmedilebilmesi için, fiilin daha ağır cezayı gerektiren başka bir suç oluşturmaması gerekir. Bu bakımdan, fiilin dolandırıcılık, güveni kötüye kullanma veya zimmet suçunu oluşturması halinde, bu fıkra hükmüne istinaden cezaya hükmedilecektir*." şeklinde açıkça ifade edilmiştir.

### 3.2. Korunan Hukuki Değer

Bu konuda doktrinde görüş birliği yoktur. Artuk/Gökçen/Yenidünya, kişilerin özel hayatlarının gizliliğinden, malvarlığının korunmasına kadar geniş bir çerçevede ele alınabileceğini, bilişim sistemlerine haksız müdahalede bulunularak kişilerin maddi ve manevi haklarına yapılan saldırıların önlenmeye çalışıldığını[428], Soyaslan, suçla mağdurun maddi manevi zararlarının korunduğunu[429], Hafızoğulları/ Özen, doğrudan zarar gören kişilerle beraber, herkese bilişim güvenliğini sağlamakla yükümlü kamu idaresinin korunduğunu[430], Dülger, suçun oluşabilmesi için failin haksız bir yarar sağlamasının gerektiğini, bu yarardan kastın ne olduğu fıkrada belirtilmediğini, bir ayrım yapılmadığı için fail tarafından elde edilen tüm maddi veya manevi yarar suçla korunan hukuksal yarar olduğunu, aynı zamanda mağdur için bir zararın olduğunu, mağdurun zarar uğratılan hakkını koruduğunu[431] ifade etmiştir.

---

427 Doğan, age. s. 142-143.
428 Artuk, Gökçen, Yenidünya, şerh. s. 6937-6938.
429 Soyaslan, age. s. 708; Aynı doğrultuda Doğan, age. s. 146.
430 Hafızoğulları, Özen, age. s. 453.
431 Dülger, age. s.441.

Genel anlamda bizim de katıldığımız görüşe göre, bu suçla bir bütün halinde malvarlığı yani mülkiyet hakkı korunmaktadır [432].

### 3.3. Suçun Unsurları

Suçun unsurları tipiklik, maddi unsur, manevi unsur ve hukuka aykırılık unsuru olmak üzere dörde ayrılır[433].

#### 3.3.1. Maddi Unsur

Suçun maddi unsuru hareket, netice ve bunlar arasındaki illiyet bağı olarak üç ana başlık altında incelenmektedir. İnsandan sadır olan ve dış dünyaya yansıyan ihmali ya da icrai davranışa hareket; insanın dış dünyada meydana getirdiği değişikliğe netice; meydana gelen neticenin yapılan hareketten doğmuş olmasına da illiyet bağı denir[434].

##### 3.3.1.1. Suçun Faili

Fıkrada fail için herhangi bir sınırlama olmaması sebebiyle bu suçun faili herkes olabilir. Maddenin 1. ve 2. fıkrası hakkında belirttiğimiz hususlar burada da geçerlidir.

##### 3.3.1.2. Suçun Mağduru

Bilişim sistemi aracılığıyla haksız yarar sağlama suçunda, mağdur açısından da herhangi bir özerklik maddede belirtilmediği için bu suçun mağduru da herkes olabilir.

Eski 765 sayılı TCK döneminde bu suçun mağduru konusunda çeşitli görüşler ileri sürülmüş ve mağdurun, bilişim sisteminin maliki ya da zilyedi olduğu ileri sürülmüştü. Kanaatimizce, yeni TCK ile bu tür suçlarda mağduru bu şekilde sınırlandırmak mümkün değildir. Verinin sahibi olmadan da bu suçun mağduru olunabilir. Örneğin, bir internet sitesine üye usulü girip oradan istifade eden bir kişinin rakip internet sitesi tarafından engellenmesi halinde ya da internetten takip edilen sanal ekonomi gazetesinden istifade eden bir kişi, bu sitedeki verileri bir ticari şirket tarafından kendi lehlerine olacak şekilde değiştirilmesi halinde, o siteyi takip

---

[432] Tezcan Erdem, Önok, age. s. 911; Özbek, Doğan, Bacaksız, Tepe, age. s. 945; Koca,Üzülmez, age. s. 839.

[433] Artuk, Gökçen, Yenidünya, Ceza Genel. içindekiler kısmı; Centel, Zafer, Çakmut, age. s. içindekiler kısmı.

[434] Artuk, Gökçen, Yenidünya, Ceza Genel. s. 388; Centel, Zafer, Çakmut, age. s. 228.

eden kişinin bu habere aldanıp hisse senetleri alması ve haberdekinin aksine hisselerin düşmesi halinde, ne bilişim sistemi sahibi ne de verinin sahibi olmasına gerek olmadan siteyi takip eden herhangi biri suçtan zarar gören konumunda olacaktır[435]. Hafızoğulları/Özen, suçun mağduru bir yandan bilişim sisteminin sahibi ya da zilyedi ilen diğer yandan herkese bilişim güvenliği sağlamakla yükümlü kamu idaresinin suçun mağduru olduğunu ifade etmiştir[436]. Tezcan/Erdem/Önok'a göre de bu suçta mağdurun malvarlığı itibariyle zarara uğrayan kişi olduğu ifade edilmiştir[437].

#### 3.3.1.3. Suçun Konusu

Bu suçun konusu hukuka aykırı yarardır. Koca ve Üzülmez, ekonomik değer olarak ölçülemeyen aynı zamanda kişilerin manevi hazlarının tatmini için yaptıkları eylemlerin yani manevi yararların suça konu olamayacağını belirtmişse de[438] bize göre, bu yararın ekonomik bir değeri olabileceği gibi manevi bir değeri de olabilir. Bu husus suç açısından önemli değildir[439]. Örneğin, bir bilişim sistemine yapılan haksız bir müdahale ile kişinin işe alınması, ihaleyi kazanması, sınavdan geçmesi hallerinin de yarar kavramı içerisinde değerlendirilmesi gerekecektir[440].

#### 3.3.1.4. Fiil ve Netice

TCK'nın 244/4. maddesinde "*yukarıda tanımlanan fiillerin işlenmesi suretiyle kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlanmasının başka bir suç oluşturmaması halinde"* eylemin suç oluşturacağı hüküm altına alınmıştır. *"yukarıda tanımlanan fiiller"* den kasıt TCK'nın 244/1. maddesinde düzenlenen bir bilişim sisteminin işleyişini engellemek veya bozmak ve 244/2. maddesinde düzenlenen bir bilişim sistemindeki verileri bozmak, yok etmek, değiştirmek veya erişilmez kılmak, sisteme veri yerleştirmek, var olan verileri başka bir yere göndermek fiilleridir.

Haksız çıkar, bir kimsenin malvarlığında meydana gelen artış olabileceği gibi yukarıda belirtildiği üzere manevi çıkar da olabilir. Fail bu haksız çıkarı TCK'nın 244/1, 2 ve 3. maddelerindeki suçları işleyerek yapmalıdır. Bir kimsenin malvarlığı artarken diğer bir kimsenin malvarlığının azalması zorunlu değildir. Mağdur

---

435 Dülger, age. s. 442.
436 Hafızoğulları, Özen, age. s. 453.
437 Tezcan, Erdem, Önok, age. s. 911.
438 Koca, Üzülmez, age. s. 839-840; aynı doğrultuda Tezcan, Erdem, Önok, age. s. 913.
439 aynı görüş için bkz. Dülger, age. s. 440; Soyaslan, age. s. 709; Erdoğan, age. s. 255.
440 Koca,Üzülmez, age. s. 839.

herhangi bir zarara uğrayabileceği gibi zarara uğramayabilir de. Fakat bu hususun, suçun zarar suçu olarak nitelendirilmesine engel teşkil etmeyeceği doktrinde ileri sürülmüş ise de[441], bize göre suçun oluşumu için zararın oluşması şart değildir. Yasa koyucu haksız çıkardan bahsetmiş, herhangi bir zarardan bahsetmemiştir. Bu haksız çıkar mağdurda herhangi bir zarar oluşturabileceği gibi herhangi bir zarar oluşturmayabilir de. Bu yüzden suçun oluşabilmesi için herhangi bir zarar aranmamıştır. Dolayısıyla bu suç zarar değil tehlike suçudur[442].

Haksız yarar fail lehine olabileceği gibi üçüncü kişi lehine yani failin yakınları lehine de olabilir. Suçun oluşumu açısından bu durumun bir önemi yoktur. Hukuka aykırı yarar elde edilmesiyle suç oluşmuş olur. Ortada herhangi bir yarar bulunmaması halinde eylem TCK'nın 244/1. ve 2. maddesi kapsamında kalacaktır.

TCK'nın 244/4. maddesinde yazılı suç çok hareketli bir suçtur. Yapılan eylemle ilk önce TCK'nın 244/1 ve 2. maddesinin oluşması gerekir. İkinci olarak bu fiille failin haksız bir çıkar sağlaması gerekir. Çıkarın hangi hareketlerle sağlanmasının gerekeceği kanunda belirtilmiştir. Buna göre çıkarın, maddenin 1. ve 2. fıkralarındaki suçların işlenmesi suretiyle meydana gelmesi zorunludur. Bu sebeple suç aynı zamanda bağlı hareketli bir suçtur. Haksız çıkar failin ya da başkasının tasarruf alanına girmesiyle gerçekleşir. Örneğin paranın failin ya da üçüncü bir kişinin hesabına geçmesiyle sağlama unsuru gerçekleşmiş olur[443].

Kanun, failin yaptığı eylemle başka bir suçun oluşmaması şartını aramıştır. Kanun maddesi bu şekilde iken gerekçe "*ancak, bu fıkra hükmüne istinaden cezaya hükmedilebilmesi için, fiilin daha ağır cezayı gerektiren başka bir suç oluşturmaması gerekir*" şeklindedir. Görüldüğü üzere, madde ile gerekçe birbiriyle çelişmektedir. Madde başka bir suç demişken, gerekçe daha ağır cezayı gerektiren bir suç demiştir[444]. Doktrinde suçun tamamlayıcı hüküm olması nedeniyle gerekçede belirtilen biçimde anlaşılmasının gerekeceği ifade edilmiş ise de[445] bize göre madde metninde yazanın önemli ve geçerli olması nedeniyle fıkrada yer alan başka bir suç oluşturmaması ifadesi geçerlidir[446].

---

441 Koca, Üzülmez, age. s. 840; Soyaslan, age. s. 709.

442 Aynı doğrultuda görüşler için bkz. Dülger, age. s. 448; Doğan, age. s. 149; Erdoğan, age. s. 448.

443 Koca, Üzülmez, age. 840.

444 Karagülmez, age. s. 243; Hafızoğulları, Özen, age. s. 454.

445 Hafızoğulları, Özen, age. s. 454; aynı doğrultuda Kurt, age. s. 171.

446 benzer görüş için bkz. Karagülmez, age. s. 244; Soyaslan, age. s. 711.

Failin yaptığı eylem başka bir suçu oluşturuyorsa faile bu suçtan ceza verilecek, TCK'nın 244/4. maddesinden ceza verilmeyecektir. Örneğin Yargıtay, iki kişinin haksız bir şekilde bir firmanın internet bankacılığını ele geçirip bu hesaptan kendi lehlerine para göndermelerinde faillerin eylemini 244 değil, 142/2-e olması gerektiğine hükmetmiştir[447].

### 3.3.2. Manevi Unsur

Bu suç ancak ve ancak kasten işlenebilir. Fail suçta belirtilen tüm unsurları bilmeli ve istemelidir. Yani fail kendisine veya başkasına haksız bir yarar sağlamak adına başkasının bilişim sistemini engellediğini, bozduğunu ya da verilerini değiştirdiğini, veya başka bir yere gönderdiğini bilmelidir.

Suçun manevi unsuru noktasında doktrinde farklı görüşler ileri sürülmüştür. İlk görüş genel kastı yeterli görürken[448]; ikinci görüş, suç için failde özel kastın bulunması gerektiğini ifade etmiştir[449]. Erdoğan, suçta kastın yeterli olacağını, ayrıca özel saikin aranamayacağını, özel saik aranmış olsaydı yasa koyucu tarafından tıpkı TCK'nın 105. maddesinde düzenlenen cinsel taciz suçunda "cinsel amaçlı olarak", aynı şekilde 141. maddesinde yer alan hırsızlık suçunda "kendisine veya başkasına bir yarar sağlamak maksadıyla" şeklinde belirtildiği üzere, “amacıyla” ya da “maksadıyla” gibi ibarelere yer verebileceğini, oysa incelemekte olduğumuz maddede buna benzer bir kelimenin olmadığını, bu yüzden suç için özel saikin aranmayacağını ifade etmiştir[450]. Dülger de "kişinin kendisine veya başkasının yararına haksız çıkar sağlaması" ibaresinin neticeye yönelik bir ifade olduğunu, failin hangi amaçla hareket ettiğini önemsemediğini, fıkrada failin amacı veya saikine yönelik bir ifade yer almadığını, bu yüzden kast dışında herhangi bir amaç unsurunun aranmadığını ifade etmiştir[451].

Bize göre fıkrada yasa koyucu "kendisinin veya başkasının yararına haksız çıkar sağlamak" ifadesiyle failde özel kast aramaktadır. Failin eylemini yarar sağlamak amacıyla yapması gerekeceği için bu suçta özel kast aranmaktadır.

### 3.3.3. Hukuka Aykırılık Unsuru

---

447 YCGK 17/11/2009 tarih 2009/11-193E. 2009/268K sayılı ilamı için bkz. Hafızoğulları, Özen, age. s. 455.

448 Erdoğan, age. s. 257-258; Dülger, age. s. 450; Koca, Üzülmez, age. s. 841.

449 Karagülmez, age. s. 240; Kurt, age. s. 175; Taşkın, age. s. 59; Parlar, age. s. 43; Doğan, age. s. 149.

450 Erdoğan, age. s. 258.

451 Dülger, age. s. 450.

Fıkrada failin elde ettiği yararın haksız olması gerektiğinin açıkça belirtilmesi sebebiyle rıza ile yapılan eylemler suç oluşturmayacaktır. Dolayısıyla mağdurun rızası hukuka uygunluk nedeni olarak değerlendirilecektir. Buradaki rıza suçun oluşmasından önce verilen rızadır. Suç oluştuktan sonra gösterilen rıza, eylemi hukuka uygun hale getirmez.

Her somut olayda verilerin maliki veya ilgilisi iyi tespit edilmeli, mağdur buna göre belirlenmelidir. Buna göre bir bilişim sistemi sahibi olmayan kişiler de suçun mağduru olabilir. Örneğin, kullanıcı bilgileri ve şifre girilmek suretiyle girilen bir siteye sırf hasmına zarar vermek için kişinin sistemde bulunan verilerine zarar verilmesi halinde mağdur, veri sahibi olan ilgili olacaktır[452].

### 3.4. Suçun Özel Görünüş Biçimleri

#### 3.4.1. Teşebbüs

Her ne kadar doktrinde bu suça teşebbüsün mümkün olmadığı ifade edilmiş ise de [453] bizim de katıldığımız genel görüş bu suça teşebbüsü mümkün görmektedir. Yukarıda da belirtildiği üzere suçun oluşumu için failin haksız bir çıkar sağlaması şarttır. Haksız çıkarın sağlanması ile suç tamamlanır. Fail gerekli hareketleri yapmasına rağmen, hatta bilişim sisteminin içerisine girmesine rağmen elinde olmayan nedenlerle, örneğin bir virüs programına takılması ya da sistem elektriğinin gitmesi halinde bilişim sistemi engellemiş olacak fakat 244/4. fıkradaki suç tamamlanamamış teşebbüs aşamasında kalmış olacaktır[454].

Fail TCK'nın 244/4. maddesinde yazılı suçu yani yarar sağlamak amacıyla verileri yok etme eylemini gerçekleştirmek için bir karar verir, suça icra hareketlerine başlar fakat elinde olmayan sebeplerle verileri dahi yok edemeden yakalanır. Bu örnekte ortada suça teşebbüs söz konusudur. Fakat hangi fıkraya teşebbüs olacağının tespiti bir hayli zor olmaktadır. Bunun tespiti için failin kastının açıkça tespit edilmesi gerekecektir. Eğer fail haksız yarar elde edebilmek amacıyla eylemine başlamış ve 1. ve 2. fıkradaki eylemleri gerçekleştiremeden elinde olmayan nedenlerle eylemi gerçekleştirememişse, failin amacı doğrultusunda suç TCK'nın 244/4. maddesine teşebbüs olacaktır. Bunun haricinde failin amacı çoğu zaman tespit edilememekte bu yüzden failin lehine olan TCK'nın 244/1. ve 2. fıkralarına teşebbüs

---

452 Dülger, age. s. 451.

453 Hafızoğulları, Özen, age. s. 454.

454 Artuk, Gökçen, Yenidünya, şerh. s. 6938; Doğan, age. s.150.

olarak değerlendirilmektedir[455]. Koca/Üzülmez'e göre fail 1. ve 2. fıkradaki fiilleri işleyemeden sistemden çıkması halinde 4. fırkadaki suçun icra hareketlerine başlanılmaması sebebiyle eylemin 4. fırkaya teşebbüs olmayacağını, bu durumda filin 243. maddeden sorumlu olacağını ifade etmiştir. Nitekim Yargıtay 26/03/2009 tarihinde bir şirketin internet hesabına giren failin hesapta oynama yaparak başka bir hesaba havale yapamadığı olayda failin TCK'nın 243/1 maddesinden sorumlu tutulması gerekeceğine dair karar ile konuya örnek vermiştir[456].

### 3.4.2. İştirak

Bu suça iştirak açısından özel bir durum yoktur. Genel iştirak halleri bu suç açısından da uygulanır. Bu suçta daha çok bir bilişim uzmanını azmetme ya da teşvik etme halleri yaygın olarak görülmektedir[457].

### 3.4.3. İçtima

#### 3.4.3.1. Genel Olarak

TCK'nın 43/1. maddesinde, bir suç işleme kararının icrası kapsamında aynı suçun bir kişiye karşı farklı zamanlarda işlenmesi halinde faile tek ceza verileceği belirtilmiştir. Bu kapsamda failin, bu suçu aynı mağdura karşı farklı zamanlarda işlemesi halinde eylemi tek sayılacak, fakat verilecek olan ceza belli oranlarda arttırılacaktır.

TCK'nın 43/2. maddesinde aynı neviden fikri içtima düzenlenmiştir. Buna göre, aynı suçun birden fazla kişiye tek bir fiille işlenmesi halinde, yine faile tek cezanın verileceği belirtilmiştir. Bu düzenleme de bu suç için geçerli olacak, bu şekilde suç işleyen faile tek ceza verilecek, fakat cezası belirli oranlarda arttırılacaktır.

Bu suç kesintisiz (mütemadi) olarak da işlenilebilir. Bu eylemde suç kesintinin gerçekleştiği anda tamamlanmış olacaktır. Aynı zamanda zamanaşımı süresi de bu tarihte başlayacaktır.

Bu suçun işlenebilmesi için maddenin 1. ve 2. fıkrasındaki suçların da işlenmesi gerekeceğinden fail ayrıca 1. veya 2. fıkradaki suçlardan cezalandırılamayacaktır. 1. ve 2. fıkradaki suçlar bu suç kapsamında eriyecektir. Dolayısıyla bu fıkradaki suç TCK'nın 42. maddesinde belirtildiği üzere bileşik suç sayılacaktır.

---

455 Dülger, age. s. 451-452.

456 Koca, Üzülmez, age. s. 842.

457 Erdoğan, age. s. 262.

Bu suçun işlenebilmesi için fail aynı zamanda TCK'nın 243. maddesinde yazılı bilişim sistemine girme suçunu da işlemiş olacağından TCK'nın 44. maddesi gereği yalnızca TCK'nın 244/4. maddesinde yazılı suçtan cezalandırılacaktır[458].

**3.4.3.2. Nitelikli Hırsızlık Suçu Açıcından İçtima**

TCK'nın 142/2-e maddesi bilişim sistemleri kullanılmak suretiyle hırsızlık suçunu işleyen kişinin cezalandırılacağı belirtilmiştir. Buna göre, zilyedin rızası olmaksızın başkasına ait bir taşınır mal hakkında bilişim sistemleri kullanılmak suretiyle yarar sağlayan kişi suçun faili olacaktır. Dolayısıyla bu suçun oluşabilmesi için ortada taşınır bir malın mevcudiyeti şarttır.

Bu hüküm ile TCK'nın 244/4. maddesi arasındaki ayrım, bilişim sitemine müdahale ile yararın sağlandığı an kıstasıdır. Eğer yarar malın bulunduğu yerden alınmasından önce gerçekleşmişse yani malın elde edilmesi ikincil ise TCK'nın 244/4. maddesi uygulanması gerekecekken, sisteme müdahaleye rağmen taşınır bir mal elde edilmeden önce bir yarar sağlandığı söylenilemiyorsa orada 142/2-e maddesi uygulanması, aksi yönde düşünen[459] görüşler olmakla birlikte çoğunluk tarafından kabul görmüştür[460].

Yargıtay ilk uygulamalarında, TCK'nın 244/4. maddesinin sıkça uygulanmasına yol açacak şekilde bir yorumda bulunmuşken Yargıtay Ceza Genel Kurulunun 17/11/2009 tarihinde sanık V.E. ile firari S.T. birlikte hareket ederek, daha önceden haksız bir şekilde ele geçirdikleri katılan firmanın internet bankacılık şifresini kullanmak suretiyle ... hesaptan 10.750YTL'yi internet kanalı ile sanık V. adına açtırdıkları hesaba havale ettikleri olayda, taşınır nitelikteki parayı bilişim sistemini kullanmak suretiyle kendi banka hesaplarına geçirmeye başka bir anlatımla var olan veriyi başka bir yere göndermekten ziyade, bu verinin temsil ettiği parayı alarak mal edinmeye yönelik olduğunu, 244/4. maddesinin değil de 142/2-3 maddesinin tatbik edilmesi gerektiğini belirttiği kararından[461] sonra ilk

---

458 Koca, Üzülmez, age. s. 842; Dülger, suçun geçitli suç olmadığını, bu şekilde suç işleyen failin hem TCK'nın 243/1 maddesinden hem de 244/4'den sorumlu olacağını ve ayrı ayrı ceza alması gerektiğini ifade etmiştir. Bkz. age. s. 454.

459 Yazıcıoğlu, Taşdemir ve Özbek hırsızlık suçunun ancak taşınır bir mal üzerinde işlenebileceğini, kanunda verinin taşınır bir mal olarak tanımlanmadığını bu sebeple verinin taşınır bir mal olmadığını ifade etmişlerdir. Bkz. Yazıcıoğlu, Genel Değerlendirme. s. 398; Yazıcıoğlu, TCK 244/4 üzerine düşünceler, s. 6; Taşdemir, age. s. 276; Özbek, age, s. 1058.

460 Ketizmen, age. s. 181-182; Erdoğan, age. s. 278-280; Doğan, age. s. 154;

461 YCGK 17/11/2009 T., 2009/11-293 E., ve 2009/268 K. sayılı ilamı.

uygulamalarından dönmüş ve Ceza Genel Kurulu Kararı doğrultusunda içtihadını değiştirmiştir[462].

Ceza Genel Kurul Kararıyla uygulamada (Yargıtay ve BAM) tam bir birlik sağlanarak, sanığın hesabına internet üzerinden girerek banka hesabındaki paraları kendi hesabına aktarılması eylemlerinde haklı olarak TCK'nın 142/2-e maddesi uygulanması gerektiği yer edinmiştir[463].

**3.4.3.3. Nitelikli Dolandırıcılık Suçu Açısından İçtima**

TCK'nın 157. maddesinde yazılı dolandırıcılık suçu ile "hileli davranışlarla bir kimseyi aldatan" kişinin cezalandırılacağı hüküm altına alınmıştır. Dolandırıcılık suçunun oluşabilmesi için öncelikle ortada hileli davranışlar olmalıdır. Bu hileli davranışlarla bir kimsenin aldatılması gerekmektedir.

TCK'nın 158. maddesinde nitelikli dolandırıcılık suçları yer almaktadır. 158/1-f maddesinde de bilişim sistemlerinin araç olarak kullanılması suretiyle dolandırıcılık suçu düzenlenmiştir.

Yukarıda da açıklandığı üzere, TCK'nın 244/4. maddesindeki suçun oluşabilmesi için başka herhangi bir suçun oluşmaması gerekmektedir. Dolayısıyla bu suçun oluşabilmesi için TCK'nın 158/1-f maddesinde yazılı suçun oluşmaması gerekecektir. Dolandırıcılık suçunun oluşabilmesi için eylemin bir kişiye karşı yapılması gerekmektedir. Bilişim sistemleri kullanılmak suretiyle yapılan dolandırıcılıklarda da, eylem yine bir kişiye karşı yapılmakta fakat bilişim sistemleri sadece araç olarak kullanılmaktadır. Dolayısıyla TCK 244 ile 158/1-f maddesindeki ayrım, failin bilişim sistemine veya verilerine yaptığı müdahale ile elde ettiği yarar noktasında toplanmaktadır. Nitekim failin yaptığı eylem ile fayda kendiliğinden meydana gelmişse TCK'nın 244/4. maddesindeki suç oluşmuş, yarar eğer kendiliğinden ortaya çıkmaz gerçek bir kişinin araya girmesi ile ortaya çıkmışsa artık 158/1-f maddesi tatbik edilmesi gerekecektir[464].

Yazıcıoğlu, "*dolandırıcılık suçunun oluşabilmesi için suç mağdurunun iradesinin hile ve desise sonucu kandırılması, etkilenmesi gerekmektedir, halbuki eylem bir bilgisayara, bir bilişim sistemine karşı gerçekleştirildiğinde bilgisayarın*

---

462 04/03/2010 T., 2009/6772 E., ve 2010/2433K.,; 28/03/2011 T., 2011/696 E., ve 2011/1729K. sayılı ilamı.

463 Bkz. Yar. 2. CD. 15/11/2017 T, 2015/935 E, 2017/11819 K; 2 CD. 10/05/2017 T, 2017/2209 E,; 2017/ 5340 K; 2 CD. 25/02/2016 T, 2014/20601 E, 2016/3182 K; İstanbul BAM. 17. CD. 15/11/2017 T, 2017/1024 E, 2017/224 K. sayılı ilamı.

464 Nitekim aynı doğrultuda görüşler için bkz. Özbek, age. s. 1059; Erdoğan, age. s. 270-273.

*iradesi diye bir şey söz konusu olamayacağından yani ortada etkilenen bir irade bulunmayacağından eylem dolandırıcılık suçunu değil ve fakat bilgisayar marifetiyle haksız menfaat sağlanması suçunu oluşturacağını*" ifade etmiştir[465].

Yargıtay, sanığın şikayetçilere ait hesaplardan internet aracılığı ile kendi hesabına para aktarmaktan ibaret eyleminde gerçek kişiye yönelik hile ve desise bulunmadığı gözetilmeden 5237 Sayılı TCK. nun 244/4. maddesi yerine suç vasfında hataya düşülerek dolandırıcılık suçundan hüküm kurulması şeklindeki kararla ilk derece mahkemesince verilmiş olan kararları bozmuştur[466]. Yargıtay'ın bu konudaki görüşü istikrar kazanmış ve oturmuştur[467].

Her ne kadar doktrinde ve uygulamada yukarıda belirtilen görüş yani gerçek kişiye yönelmiş herhangi bir hileli hareketin bulunmaması halinde TCK'nın 244/4. maddesinin tatbik edilmesi, diğer hallerde TCK 158/1-f maddesinin uygulanması gerektiği görüşü yaygın olsa da Taşkın, TCK'nın 158/1-f maddesinin uygulama olanağının olmadığını, hileli davranışların TCK'nın 158/1-f maddesi çerçevesinde bir kişiye karşı yapılamayacağını, dolayısıyla bu maddenin uygulama imkanının olmadığını ifade etmiştir[468].

### 3.5. Yaptırım

Kanunda bu suç için iki yıldan altı yıla kadar hapis ve beş bin güne kadar adli para cezası öngörülmüştür. TCK'nın 244/1. ve 2. fıkrasında yalnızca hürriyeti bağlayıcı ceza öngörülmüşken bu fıkrada hem hürriyeti bağlayıcı ceza hem de adli para cezası öngörülmüştür. Yasa koyucunun her iki cezayı "ve" bağlayıcıyla ayırması sebebiyle bu iki ceza seçimlik olmayıp bağlayıcı cezadır.

TCK'nın 60. maddesinde tüzel kişiler hakkında yaptırım müessesi düzenlenmiştir. 60/4. maddesinde de "*bu madde hükümleri kanunun ayrıca belirttiği hallerde uygulanır"* şeklindedir. Dolayısıyla suç içeren bir ceza normunda tüzel

---

465 Yazıcıoğlu, Genel Değerlendirme. s. 411.

466 Yar. 11 CD. 18/09/2007 T., 2007/6963 E. ve 2007/5533 K sayılı ilamı.

467 *"Dolandırıcılık suçu, hileli davranışlarla bir kişinin aldatılıp onun veya bir başkasının zararına, failin kendisine veya bir başkasına yarar sağlanması suretiyle oluşur. Suçun maddi unsurunu oluşturan hareketlerin, ger.ek kişiye yöneltilmiş olması, onun kandırılarak çıkar sağlanması gerekir. Gerçek bir kişiyle karşı karşıya gelmeden, yüz yüze veya telefon, bilgisayar, bilgi geçer gibi bir başka vasıta kullanılarak görüşmeden, konuşmadan, hileli davranışlarla ger.ek kişiler dolandırılmadan sadece bilişim sistemi kullanılarak doğrudan doğruya çıkar sağlanması halinde TCK'nın 244/4. maddesindeki suç gerçekleşecektir*" bkz. Yar. 11 CD. 12/10/2009 T., 2008/11060E., ve 2009/11936 K. sayılı ilamı. aynı doğrultuda, yar. 11 CD. 22/01/2008 T. ve 2007/8423 E., ve 2008/117 K. sayılı ilamı.

468 Bkz. Taşkın, Uyuşmazlıklar. s. 349.

kişiler hakkında yaptırımdan bahsedilmezse bu maddenin uygulanma olanağı olmayacaktır.

TCK'nın bilişim alanındaki suçları düzenleyen bölümün son maddesinde yani 246. maddesinde "*bu bölümde yer alan suçların işlenmesi suretiyle yararına haksız menfaat sağlanan tüzel kişiler hakkında bunlara özgü güvenlik tedbirine hükmolunur*" ifadesi yer alması TCK'nın 244. maddesinde yazılı suçların bir tüzel kişi lehine işlenmesi halinde, ilgili tüzel kişi hakkında TCK'nın 60. maddesi uygulama alanı bulacak ve bu tüzel kişi hakkında iznin iptali ya da müsadereye karar verilebilecektir. Ancak işlenen fiile nazaran daha ağır sonuçların ortaya çıkması halinde hakimin bu tedbirlere hükmetmeyebileceği TCK'nın 60/3 maddesinde ayrıca belirtilmiştir.

Bununla birlikte diğer şartların da oluşması halinde TCK'nın 54 ve 55. maddelerinde yazılı eşya ve kazanç müsaderesinin de uygulanması bu suç açısından mümkündür.

**3.6. Soruşturma ve Kovuşturma**

Kanunda ayrıca belirtilmediği için suç şikayete tabi olmayıp re'sen soruşturulan suçlardandır. Buna göre herhangi bir şekilde suçun işlendiğini öğrenen Cumhuriyet Savcısı re'sen soruşturma işlemlerine başlayacaktır.

5235 sayılı Adli Yargı İlk Derece Mahkemeleri İle Bölge Adliye Mahkemesinin Kuruluş, Görev ve Yetkileri Hakkında Kanuna göre bu suçta görevli mahkeme asliye ceza mahkemeleridir.

# SONUÇ

Bilgisayarın gerçek anlamda ortaya çıkması ile beraber bu teknolojik alan akılalmaz bir ilerleme göstermiştir. Futbol sahası büyüklüğünden cebimize sığacak şekilde üretime başlanan bilgisayar herkesin kolaylıkla erişebileceği seviyeye çoktan ulaşmıştır. Bu teknolojik gelişme internetin kişisel kullanıma açılması ile beraber durdurulamayacak boyutlara ulaşmıştır. Hemen hemen herkes, bütün devlet kurumları, bankalar, ticari işletmeler bu teknolojiyi kullanmak suretiyle iş ve işlemlerini yapar hale gelmiştir. Bu bilişim sistemlerinde para dahil her türlü bilgi ve değer tek tuşla saklanabilir hale gelmiştir. Bu denli önemli bilgiler içeren bilişim sistemleri, zanlılar tarafından da hedef haline gelmiştir.

Klasik suç tiplerinden olan hırsızlık, yaralama vb. suçlara, bilişim suçları da eklenmiştir. Bu suçlar coğrafi alan sınırlaması olmaması, hızlı ve bu alanda uzmanlaşmış kişiler tarafından kolayca işlenebilir olması, çok fazla işlenme şeklinin olması ve her geçen gün bu işlenme şekillerine yenisinin eklenmesi sebebiyle zanlılar tarafından çokça tercih edilen suçlar arasında yerini almıştır.

Bu tür yıkıcı sonuçlar ortaya çıkaran bilişim suçlarını engellemek isteyen yasa koyucu, bu tür eylemleri yaptırım altına alarak suçun önüne geçmek istemiştir. Bu çerçevede 5237 sayılı TCK'da konuyu, üçüncü kısım onuncu bölüm başlığı altında ele almıştır.

Yeni bir suç tipi olması, gelişen teknolojiye paralel olarak her geçen gün yeni bir işlenme şeklinin ortaya çıkması sebebiyle uygulamada, ulusal ve uluslaraarası hukukta bu suçlar için bir takım eksiklikler mevcuttur.

Bunlardan ilki, mevuatımızda suçun alt ve üst sınırı çok düşük olmasıdır. TCK'nın 125. maddesinde düzenlenen hakaret suçunun alt sınırı üç ay; TCK'nın 86/2. maddesinde yer alan basit tıbbi müdahale ile giderilebilecek nitelikte yaralama suçunun alt sınırı dört ay, normal yaralamalarda ise bir yıl iken; şüphelilerin tespit edilmesi ve yakalanması oldukça zor olan, aynı zamanda yıkıcı sonuçları diğer suçlara nazaran bir hayli ağır olan TCK'nın 244/2. maddesinde yazan verilere müdahale suçunun alt sınırının altı ay gibi çok düşük bir ceza alt sınırı olması

eleştirilmesi gereken ilk husustur. Bu doğrultuda yasada gerekli değişiklik yapılarak suç için öngörülen alt ve üst sınırlar arttırılmalıdır.

Bir başka eleştri de TCK'nın 244. maddesinin düzenlendiği yer için geçerlidir. Her ne kadar TCK'nın 244. maddesinde yazan suçun hukuki konusu, mala zarar verme suçunun hukuki konusu ile benzer şekilde kişilerin mülkiyet haklarının korunması olduğu belirtilmiş ise de kanunun düzenleniş şekli bakımından durum çelişkilidir. TCK'nın 151. maddesinde yazılı mala zarar verme suçu, TCK'nın ikinci kısım onuncu bölümünde yer almasına rağmen TCK'nın 244. maddesinde düzenlenen suç, TCK'nın üçüncü kısım onuncu bölümünde düzenlenmektedir. Bu kapsamda mala zarar verme suçları açısından uygulama alanı bulan ve kanunun 167. maddesinde düzenlenen şahsi cezasızlık halleri ile 168. maddede düzenlenen etkin pişmanlık konusu 244. maddede öngörülmediğinden bu suçun failinin etkin pişmanlık ve şahsi cezasızlık hallerinden yararlanması mümkün olmamaktadır. Bu dorultuda, mala zarar verme suçuyla benzer hukuki değeri koruyan TCK 244. maddesine de benzer bir düzenlemenin getirilmesi ve çelişkinin giderilmesi gerekmektedir. Nitekim TCK'nın 245. maddesinde yer alan kredi kartlarının kötüye kullanılması suçunda buna benzer bir düzenleme madde içerisinde mevcuttur.

Bu suçta bir başka önemli husus uluslararası işbirliğidir. Bilişim suçları, yapısı gereği internet bulunan her yerde işlebilen suçlardandır. Coğrafi alan sınırlaması yoktur. Suç işleyen kişilerin bu suçları yaptırım altına almayan ülkelere sığınması ve suçları orada işlemeleri halinde eylemleri cezasız kalabilmektedir. Zanlılar bu ve buna benzer sebeplerle eylemlerini gelişmemiş ya da az gelişmiş ülkelerde işlemektedir. Bu çerçevede gerekli yasal düzenlemeler ile gelişmemiş ve az gelişmiş ülkelerin de bu suçları yaptırım altına almaları, başta Rusya ile Çin ve diğer ülkelerin ASSS üye olmalarının sağlanması ve ASSS'ye üye devlet sayısının artırılması gerekmektedir.

Bu suçların önlenmesinde toplumun aydınlatılması da bir o kadar önemlidir. Bu suçta yapılması gerekenleri öğrenen toplum suçun işlenmesinin önüne geçebilecek, suç işlense bile nasıl hareket etmesi gerektiğini bilecektir. Sosyal medyadaki şifresinin karmaşık kelime ve harflerden oluşması halinde şifrenin kırılmasının ve hesaplarının ele geçirilmesinin bir o kadar zor olduğunu öğrenen toplum şifresini ona göre belirleyerek suçun işlenmesinin önüne geçebilecektir.

Sonuç olarak gelişen teknolojiye ve yeni suç işlenme şekillerine paralel olarak yeni ve güncel düzenlemeler yapılması, uluslararası işbirliğinin artırılması, bu suçla mücadele için uygulamaya yönelik gerekli eğitimlerin verilmesi, vatandaşın aydınlatılması bilişim suçlarının önüne geçilmesinde etkili birer adım olacaktır.

## KAYNAKÇA


Akarslan, H. (2015). *Bilişim Suçları.* ( 2. Baskı.) Ankara: Seçkin Yayıncılık,

Akbulut, B. B. (2000). Bilişim Suçları. *Selçuk Üniversitesi Hukuk Fakültesi Dergisi*. Milenyum Armağanı, C. 8, S.1-2, (545-555)

Akbulut, B. (2016). Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme. *Selçuk Üniversitesi Hukuk Fakültesi Dergisi*, C.24. S.2. (7-55)

Apaydın, C. (2016). Bilişim Sistemine Girme. *TAAD,* S.24 (245-308)

Artuk M. E., Gökçen, A,, Yenidünya, A.C. (2013). *Ceza Hukuku Özel Hükümler*. Ankara: Adalet Yayınevi.

Artuk M. E., Gökçen, A, Yenidünya, A.C. (2007). *Ceza Hukuku Genel Hükümler.* Ankara: Turhan Kitapevi

Avşar, B. Z., Öngören, G., (2010). Bilişim Hukuku. *Türkiye Bankalar Birliği Yayını*, Yayın No: 270.

Aydın, E. D., (1992). *Bilişim Suçları ve Hukukuna Giriş.* Ankara: Doruk Yayınevi.

Boğa,U. (2011). *Bilişim Suçlarıyla Mücadele Yöntemleri*. RTÜK Yayımlanmamış Uzmanlık Tezi. Ankara

Bölükbaş C. (2014). *Yeni Nesil Teknolojik Silahlar: DoS/DDoS,* https://siberbulten.com/makale-analiz/yeni-nesil-teknolojik-silahlar-dosddos/

Çakır, H. (2013). *İnternet, Etik ve Bilişim Suçları.* http://android.eng.ankara.edu.tr/wpcontent/uploads/sites/656/2017/10/9_%C4%B0nternet-Etik-ve-Bili%C5%9Fim-Su%C3%A7lar%C4%B1_H%C3%BCseyin-%C3%87AKIR.pdf

Çakır, H., Kılıç, M. S. (2014). *Güncel Tehdit Siber Suçlar*. Ankara: Seçkin Yayıncılık.

Centel, N. Zafer, H. Çakmut, Ö. (2008). *Türk Ceza Hukukuna Giriş*. İstanbul: Beta Basım.

Demircan, M. T. (2016). *Bilişim Alanında Suçlar*: İstanbul: Legal Yayıncılık.

Demirbaş, T. (2009). *Ceza Hukuku Genel Hükümler*. Ankara: Seçkin Yayıncılık.

Doğan, R. (2014). *5237 Sayılı Türk Ceza Kanunu'nda Bilişim Suçları*. Ankara: Adalet Yayınevi.

Dülger, V. M. (2015). *Bilişim Suçları ve İnternet İletişim Hukuku.* Ankara: Seçkin Yayınevi.

Eker, Ö. U. (2006). Türk Ceza Hukuku'nda Bilişim suçları" Eski Tck Bağlamında Hukukumuzda Yer Alan İlk Düzenlemeler ve 5237 Sayılı Yeni Türk Ceza Kanunu'nun İlgili Hükümlerinin Yorumu, *TBB Dergisi,* Y. 19, S. 62. (101-131)

Erdağ, A. İ. (2010). Bilişim Alanında Suçlar (Türk ve Alman Ceza Hukukunda). *Gazi Üniversitesi Hukuk Fakültesi Dergisi*, Ankara, C. XIV, S.2, (75-303)

Erdoğan, Y. (2013). *Türk Ceza Kanunu'nda Bilişim Suçları (Avrupa Konseyi Siber Suç Sözleşmesi ve Yargıtay Kararları İle)*. İstanbul: Legal Yayıncılık.

Ersoy, Y. (1994). Genel Hukuki Koruma Çerçevesinde Bilişim Suçları. *Ankara Üniversitesi Siyasal Bilgiler Fakültesi Dergisi,* C. XLIX, S.3-4. (149-183)

Güngör N. M. (2007). "*Yeni Türk Ceza Kanunu Kapsamında Bilişim Suçları ve Emniyet Genel Müdürlüğü Uygulamaları"*. İstanbul Üniversitesi/Sosyal Bilimler Enstitüsü, Kamu Yönetimi Anabilim Dalı, Yayımlanmamış Yüksek Lisans Tezi, İstanbul.

Gürler, F. (2013). *Teknik Ve Hukuksal Yönleriyle Bilişim Alanında Suçlar*. Çankaya Üniversitesi/Sosyal Bilimler Ensitüsü. Yayımlanmamış Yüksek Lisans Tezi.

Gürocak, İ.*Bilişim Sistemine Girme*. www.ismailgurocak. av.tr/makale.doc,

Hakeri, H. (2009). *Ceza Hukuku Genel Hükümler*. Ankara: Seçkin Yayıncılık.

Hafızoğulları, Z., Özen. M. (2012). *Türk Ceza Hukuku Özel Hükümler Topluma Karşı Suçlar*. Ankara. Usa Yayıncılık.

Henkoğlu, T. (2014). *Adli Bilişim Dijital Delillerin Elde Edilmesi ve Analizi*. İstanbul: Pusula Yayıncılık.

Hekim, H. (2015). *Oltalama (Phishing) Saldırıları.* Tombul, F., Güneştaş, M., Başıbüyük, O. (Ed.). Siber Suçlar Tehditler, Farkındalık ve Mücadele. Ankara: Global Politika ve Strateji. (57-85)

Hekim, H., Başıbüyük, O. (2013). Siber Suçlar ve Türkiye'nin Siber Güvenlik Politikaları. *Uluslararası Güvenlik ve Terörizm Dergisi*. S. 4. (135-158)

Karakehya, H. (2009). *Türk* Ceza Kanunu'nda Bilişim Sistemine Girme Suçu. *TBB Dergisi*. S:81. (1-24)

Karagülmez, A. (2014). *Bilişim Suçları ve Soruşturma-Kovuşturma Evreleri*. (Genişletilmiş ve Gözden Geçirilmiş 2. Baskı), Ankara: Seçkin Yayıncılık.

Ketizman, M. (2008). *Türk Ceza Hukukunda Bilişim Suçları.* Ankara: Adalet Yayınevi.

Kızıltan M. B., (2007). *5237 sayılı Türk Ceza Kanununda Bilişim Sistemine Girme, Sistemi Engelleme ve Bozma Suçları.* İstanbul Üniversitesi/Sosyal Bilimler Enstitüsü, Kamu Hukuku Ana Bilim Dalı, Yayımlanmamış Yüksek Lisans Tezi, İstanbul.

Kurt, L. (2005). Bilişim *Suçları ve Türk Ceza Kanunundaki Uygulaması.* Ankara: Seçkin Yayıncılık.

Koca, M., Üzülmez. İ. (2017). *Türk Ceza Hukuku Özel Hükümler*. (4. Baskı), Ankara: Adalet Yayınevi.

Orta, M. (2015). *Bilişim Suçlarında Adli Analiz*, Selçuk Üniversitesi/Sosyal Bilimler Enstitüsü, Kamu Hukuku Anabilim Dalı, Yayımlanmamış Doktora Tezi.

Özbek, V. Ö., Doğan, K., Bacaksız, P.,Tepe, İ. (2016). *Türk Ceza Hukuku Özel Hükümler*. Ankara: Seçkin Yayıncılık.

Özbek, V. Ö. (2007). Banka veya Kredi kartlarının Kötüye Kullanılması Suçu (TCK m. 245), *Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi*, C. IX, Özel sayı, İzmir, (1019-1063)

Önder, A., (1994). *Şahıslara ve Mala Karşı Cürümler ve Bilişim Alanında Suçlar*. İstanbul: Filiz Kitabevi.

Özgenç, İ. (2011). *Türk Ceza Hukuku Genel Hükümler*. Ankara: Seçkin Yayıncılık.

Özen, M., Baştürk İ. (2011). *Temel Hak ve Özgürlükler Bağlamında Bilişim – İnternet ve Ceza Hukuku*, (1. Baskı), Ankara: Adalet Yayınevi.

Özmestik, F. Ü. (2015). *Bilişim Sistemleri Üzerine Arama ve El Koyma Tedbirine İlişkin Mevzuat ve Uygulamada Yaşanan Sorunlar.* (Yayımlanmamış Yüksek Lisans Tezi). İstanbul Bilgi Üniversitesi/Sosyal Bilimler Enstitüsü. İstanbul. s. 4.

Pallı, H.(2008). *Türk Hukukunda ve Mukayeseli Hukukta Bilişim Suçları.* (Yayımlanmamış yüksek lisans tezi). Erciyes Üniversitesi/Sosyal Bilimler Enstitüsü. Kayseri.

Sarı, O. (2013). *Uluslararası Hukuk ve Türk Ceza Hukuku Bağlamında Siber Güvenlik ve Bilişim Sistemine Yönelik Suçlar*. (Yayımlanmamış Yüksek Lisans Tezi). Harp Akademileri, Stratejik Araştırmalar Enstitüsü.

Soyaslan, D. (2014). *Ceza Hukuku Özel Hükümler*. Ankara: Yetkin Yayınevi.

Soysal, T. (2007). Elektonik Posta Yoluyla Kişilik Haklarına Müdahaleden Doğan Hukuki Sorumluluk. *Ankara Barosu Dergisi.* Y. 2007. S. 1. (144-167)

Taşkın, Ş. C. (2008). *Bilişim Suçları*. Bursa: Beta Yayıncılık.

Taşkın, C. (2009). Bilişim Hukuku Uluslararası Uyuşmazlıklar, *TBB Dergisi,* S. 85. (332-372)

Tezcan, D., Erdem. M. R., Önok, M. (2015). *Teorik ve Pratik Ceza Özel Hukuku*. Ankara: Seçkin Yayıncılık.

Toroslu, N. (2009). *Ceza Hukuku Özel Kısım*. Ankara: Savaş Yayıncılık.

Turhan, O. (2006). *Bilgisayar Ağları İle İlgili Suçlar (Siber Suçlar*), Başbakanlık Devlet Planlama Teşkilatı Müsteşarlığı Hukuk Müşavirliği, Uzmanlık Tezi. Ankara.

Turan, M. (2016). *Bilişim Hukuku*. Ankara: Seçkin Yayıncılık.

Tulum, İ. (2006). *Bilişim Suçları İle Mücadele*. (Yayımlanmamış Yüksek Lisans Tezi). Süleyman Demirel Üniversitesi/Sosyal Bilimler Enstitüsü.

Uçar, H. (2014). *5237 Sayılı Türk Ceza Kanunu'nda Bilişim Suçlar.* (Yayımlanmamış Yüksek Lisans Tezi). Çankaya Üniversitesi/Sosyal Bilimler Enstitüsü. Ankara.

Ünver, M., Mızaoğlu, A.G. (2011). *Yemleme ("phıshıng") Raporu,* Bilgi Tekonolijleri ve İletişimi Kurumu Dairesi Başkanlığı

Ünal, C., Şahin, İ. (2017). İstenmeyen Elektronik Postaların (SPAM) Filtrelenmesi İçin Bir Uzman Sistem Tasarımı ve Gerçekleştirilmesi. *Polieknik Dergisi*. Y.2017 S. 20. (267-274)

Ünal, A., (2015). Dağıtık Servis Dışı Bırakma (DDOS) Saldırıları: Güncel Yöntemler ve Mücadele. Tombul, F., Güneştaş, M., Başıbüyük, O. (Ed.). Siber Suçlar Tehditler, Farkındalık ve Mücadele. Ankara: *Global Politika ve Strateji*. (11-36)

Yazıcıoğlu, Y., (1997). *Bilgisayar Suçları, (Kriminolojik, Sosyolojik ve Hukuksal Boyutları ile)*, 1. Baskı, İstanbul: Alfa Yayınları.

Yazıcıoğlu, Y., (2009). 5237 s. TCK.nun 244/4 üncü Maddesinde Düzenlenen "Bilişim Sistemi Marifetiyle Haksız Çıkar Sağlanması" Suçu ile md.142/2-e ve 158/1-f Maddesinde Düzenlenen "Bilişim Sistemlerinin Kullanılması Suretiyle" "Hırsızlık" ve "Dolandırıcılık" Suçlarının İşlenmesi Sorunsalı Üzerine Düşünceler, *Suç ve Ceza,* S. 4. (1-8)

Yazıoğlu, Y.(2005). Yeni Türk Ceza Kanunundaki Bilişim Suçlarının Genel Değerlendirmesi. *YÜHFD*. C. II. S. 2.

Yaycı, E. (2007). *Bilişim Suçları.* (Yayımlanmamış Yüksek Lisans Tezi). Gazi Üniversitesi/Sosyal Bilimler Enstitüsü. Ankara.

Yenidünya, A. C., Değirmenci O., (2003). *Mukayeseli Hukukta ve Türk Hukukunda Bilişim Suçları*. (1. Baskı), İstanbul: Legal Yayıncılık

Yılmaz, S. (2011). 5237 Sayılı TCK'nın 244. Maddesinde Düzenlenen Bilişim Alanındaki Suçlar. *TBB Dergisi*. S.92. (62-100)

Yılmaz, S. (2016). *Türk Ceza Hukuku Sisteminde Siber Suçlar*. Ankara: Adalet Yayınevi.

***İnternet Kaynakları***

Bilgi İşlem Dairesi Başkanlığı, http://bidb.itu.edu.tr/eskiler/seyirdefteri/blog/2013/09/07/denial-of-service-(dos)-sald%C4%B1r%C4%B1lar%C4%B1-ve-korunma-y%C3%B6ntemleri (erişim tarihi: 15/03/2018)

Bölükbaş C. (22 Aralık 2014). Yeni Nesil Teknolojik Silahlar: DoS/DDoS. https://siberbulten.com/makale-analiz/yeni-nesil-teknolojik-silahlar-dosddos/ (erişim tarihi: 15/03/2018)

Çakır, H. (2013). İnternet, Etik ve Bilişim Suçları. http://android.eng.ankara.edu.tr/wp-content/uploads/sites/656/2017/10/9_%C4%B0nternet-Etik-ve-Bili%C5%9Fim-Su%C3%A7lar%C4%B1_H%C3%BCseyin-%C3%87AKIR.pdf (erişim tarihi: 05/02/2018)

Gürocak, İ.Bilişim Sistemine Girme. http://www.ismailgurocak.av.tr/makale/B%C4%B0L%C4%B0%C5%9E%C4%B0M%20S%C4%B0STEM%C4%B0NE%20G%C4%B0RME%20SU%C3%87U-%C4%B0SMA%C4%B0L%20G%C3%9CROCAK.pdf (erişim tarihi 16/04/2018)

Mahmutoğlu, F. S. (2013). Türk Ceza Kanununda Yer Alan Bilişim Alanındaki Suçlar Ve Karşılaşılan Sorunların Yargı Kararları Işığında Değerlendirilmesi,İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, C.71, S. 1, s.855-889, http://www.journals.istanbul.edu.tr/iuhfm/article/view/1023021510/1023020290 (Erişim tarihi: 05/04/2018)

Muğla Emniyet Müdürlüğü, http://www.mugla.pol.tr/fethiye/Sayfalar/Botnet-Nedir.aspx. (erişim tarihi: 15/03/2018)

http://www.tdk.gov.tr

http://www.bilgiler.gen.tr/ilk-bilgisayar-nasil-ortaya-cikti.html (Erişim tarihi: 02/01/2018)

http://www.milliyet.com.tr/bakin-bakalim-10-yil-sonra-neler-olacak--dijitaloyuncaklar-1390693/ (Erişim tarihi: 25/01/2018)

https://shiftdelete.net/en-tehlikeli-10-bilgisayar-virusu-28544 (erişim tarihi: 10/02/2018)

http://www.hurriyet.com.tr/bilgisayar-kullanicilari-oltaya-geliyor-21226684 (erişim tarihi: 10/02/2018)

http://www.hurriyet.com.tr/bilgisayar-kullanicilari-oltaya-geliyor-21226684 (erişim tarihi: 15/03/2018)

https://tr.wikipedia.org/wiki/Yemleme (erişim tarihi: 15/03/2018)

https://www.garanti.com.tr/tr/bireysel/subesiz/internet_bankaciligi/guvenlik/phishing.page (erişim tarihi: 15/03/2018)

http://www.hurriyet.com.tr/bilgisayar-kullanicilari-oltaya-geliyor-21226684 (erişim tarihi: 15/03/2018)

http://www.teknokulis.com/dosyalar/internet/2015/12/30/dos-ve-ddos-saldirilari-nedir-belirtiler-farklar-ve-onlemler (erişim tarihi: 15/03/2018)

https://www.tbmm.gov.tr/sirasayi/donem24/yil01/ss380.pdf (erişim tarihi: 20/03/2018)

**EK-1**

# ÖZGEÇMİŞ

## KİŞİSEL BİLGİLER

**Adı Soyadı** : Barış Emre ALP

**Uyruğu** : T.C.

**Doğum Tarihi ve Yeri** : 05.02.1991 / Yenimahalle

**Medeni Hali** : Bekar

**E-posta** : barisemrealp@gmail.com

## EĞİTİM

| DERECE | KURUM | MEZUNİYET YILI |
|---|---|---|
| Lise | Batıkent Lisesi | 2007 |
| Lisans | İzmir Üniversitesi Hukuk Fakültesi | 2013 |

## İŞ DENEYİMİ

| YIL | YER | POZİSYON |
|---|---|---|
| 2013 - 2015 | Ankara Barosu | Avukat |
| 2015 - 2016 | Adalet Bakanlığı | Hakim-Savcı Adayı |
| 2016 - 2018 | Gemerek Adliyesi | C. Savcısı |
| 2018- | Nazilli Adliyesi | C. Savcısı |