# BİLİŞİM SUÇLARI VE ÜNİVERSİTE LİSANS ÖĞRENCİLERİNİN BİLİŞİM SUÇLARINA YÖNELİK GÖRÜŞLERİ

**BURAK TUNÇ BİLEK**

**YÜKSEK LİSANS TEZİ**
**BİLGİSAYAR EĞİTİMİ ANABİLİM DALI**

**GAZİ ÜNİVERSİTESİ**
**BİLİŞİM ENSTİTÜSÜ**

**HAZİRAN 2012**
**ANKARA**

Burak Tunç BİLEK tarafından hazırlanan Bilişim Suçları ve Üniversite Lisans Öğrencilerinin Bilişim Suçlarına Yönelik Görüşleri adlı bu tezin Yüksek Lisans tezi olarak uygun olduğunu onaylarım.

Yrd. Doç Dr. Benian TEKİNDAL
Tez Yöneticisi

Bu çalışma, jürimiz tarafından oy birliği ile Bilgisayar Eğitimi Anabilim Dalında Yüksek lisans tezi olarak kabul edilmiştir.

Başkan : Doç.Dr. M. Rahmi CANAL

Üye : Yrd. Doç Dr. Benian TEKİNDAL

Üye : Yrd.Doç.Dr. Hüseyin ÇAKIR

Tarih : 28/06/2012

Bu tez, Gazi Üniversitesi Bilişim Enstitüsü tez yazım kurallarına uygundur.

Yrd.Doç.Dr.Nurettin TOPALOĞLU
ENSTİTÜ MÜDÜRÜ

## TEZ BİLDİRİMİ

Tez içindeki bütün bilgilerin etik davranış ve akademik kurallar çerçevesinde elde edilerek sunulduğunu, ayrıca tez yazım kurallarına uygun olarak hazırlanan bu çalışmada orijinal olmayan her türlü kaynağa eksiksiz atıf yapıldığını bildiririm.

Burak Tunç BİLEK

**BİLİŞİM SUÇLARI VE ÜNİVERSİTE LİSANS ÖĞRENCİLERİNİN BİLİŞİM SUÇLARINA YÖNELİK GÖRÜŞLERİ**

**(Yüksek Lisans Tezi)**

**Burak Tunç BİLEK**

**GAZİ ÜNİVERSİTESİ**

**BİLİŞİM ENSTİTÜSÜ**

**HAZİRAN 2012**

## ÖZET

**Bilişim sistemlerinin hayatımızda yaygın olarak kullanılmasıyla birçok alanda köklü değişiklikler meydana gelmiştir. Teknolojinin yaptığı değişim sosyal hayatımızı oldukça kolaylaştırmasına rağmen bir takım güvenlik sorunlarına da sebep olmuştur. Teknoloji suç işlemeyi kolaylaştırmış ve bilişim suçlarının ortaya çıkmasına sebep olmuştur. Bu çalışmada Türkiye'deki bilişim suçu istatistikleri incelenmiş, en çok işlenen suç tipleri ve bu suçların hangi yöntemlerle işlendikleri ortaya konmuştur. En çok işlenen suç olan kredi kartı ve banka kartları sahteciliği ve dolandırıcılığı suçu ayrıntılı olarak yöntemleriyle birlikte açıklanmıştır. Bilişim suçlarını gerek suçlu gerekse muhtemel hedef kitle açısından inceleyebilmek maksadıyla, bu suçlara yönelik üniversite öğrencilerinin tutumları incelenmiş ve bu suçu işleyen hükümlülerin görüşleri değerlendirilmiştir. Sonuç olarak da bilişim suçları ile mücadelede toplumsal ve kurumsal farkındalığın artırılması ile alınması gereken tedbirler hususunda öneriler getirilmiştir.**

**Bilim Kodu: 702.6.020**
**Anahtar Kelimeler: Bilim ve teknoloji, hukuk**
**Sayfa Adedi: 130**
**Tez Yöneticisi: Yrd. Doç Dr. Benian TEKİNDAL**

# CYBER CRIME AND THE ATTITUDES OF UNDERGRADUATE STUDENTS TOWARDS CYBER CRIME

**(M.Sc. Thesis)**

**Burak Tunç BİLEK**

**GAZİ UNIVERSITY**

**INFORMATICS INSTITUTE**

**JUNE 2012**

## ABSTRACT

**Lots of fundamental changes have been faced in many fields of our daily life with the widespread use of information systems. Although changes through technology have fairly simplified our social life it has also caused some security problems as well. Technology has made it easy to commit crime, and has also brought about cyber-crime. In this study, the statistical data about cyber-crimes in Turkey was analyzed; the most committed crime types and the techniques used in these crimes were defined. As the mostly committed crime types, credit card and debit card forgery and fraud are explained in detail with their crime techniques. In order to be able to analyze cyber-crimes from the views of both criminals and probable victims, the attitudes of university students towards cyber-crimes are analyzed, and the opinions of cyber criminals were studied. As a result, a few advices about the needed precautions and the ways to increase the level of social and institutional awareness in this struggle against cyber-crimes were given.**

**Science Code: 702.6.020**
**Key Words: Science and technology, law**
**Page Number: 130**
**Adviser: Assistant Prof. Dr. Benian TEKİNDAL**

# TEŞEKKÜR

Çalışmalarım boyunca değerli yardım ve katkılarıyla beni yönlendiren danışmanım ve değerli hocam Yrd. Doç. Dr. Benian TEKİNDAL'a, tez dönemim içerisinde verdiği destek ile Yrd. Doç. Dr. Alpaslan GÖZLER'e ve Agah TEKİNDAL'a, manevi destekleriyle beni hiçbir zaman yalnız bırakmayan çok değerli arkadaşlarım Raif SARICA, Eren YAŞARKURT, Günce Ali BEKTAŞ, Hasan CAN ve Özge ÇEŞMECİ'ye ayrıca araştırmam esnasında verilerin hazırlanmasında yardımları için Jandarma Genel Komutanlığına, Adalet Bakanlığı Ceza ve Tevkifevleri Genel Müdürlüğüne, İçişleri Bakanlığı Kaçakçılık İstihbarat Harekat ve Bilgi Toplama Daire Başkanlığına ve Bankalararası Kart Merkezine teşekkürü bir borç bilirim.

# İÇİNDEKİLER

**Sayfa**

# ÇİZELGELERİN LİSTESİ

**Çizelge** **Sayfa**

# ŞEKİLLERİN LİSTESİ

**Şekil** **Sayfa**

# RESİMLERİN LİSTESİ

**Resim** **Sayfa**

# SİMGELER VE KISALTMALAR

Bu çalışmada kullanılmış bazı simgeler ve kısaltmalar, açıklamaları ile birlikte aşağıda sunulmuştur.

| Kısaltmalar | Açıklama |
|---|---|
| **ABD** | Amerika Birleşik Devletler |
| **ATM** | Automatic Teller Machine |
| **ARPANET** | Advanced Research Projects Agency Network, (Amerikan Gelişmiş Savunma Araştırmaları Dairesi Ağı) |
| **APWG** | Anti-Phishing Working Group (Oltalama Karşıtı Çalışma Grubu) |
| **BSA** | Business Software Alliance |
| **BKM** | Bankalar Arası Kart Merkezi |
| **BTİK** | Bilgi Teknolojileri ve İletişim Kurumu |
| **BÖTE** | Bilgisayar ve Öğretim Teknolojileri Eğitimi |
| **DNS** | Domain Name Server |
| **EMI** | Elektromagnetic Interfrence (Elektromanyetik girişim) |
| **ENIAC** | Elektronic Numerical Integratorand Computer |
| **İTÜ** | İstanbul Teknik Üniversitesi |
| **KİHBİ** | İçişleri Bakanlığı Kaçakçılık İstihbarat Harekat ve Bilgi Toplama Daire Başkanlığı |
| **m.** | madde |
| **ODTÜ** | Orta Doğu Teknik Üniversitesi |
| **OECD** | Ekonomik Kalkınma ve İşbirliği Örgütü bazen de İktisadi İşbirliği ve Gelişme Teşkilatı |
| **POS** | Point of sale- satış noktası |
| **TCK** | Türk Ceza Kanunu |
| **TCP/IP** | Transmission Control Protocol/Internet Protocol |
| **TDK** | Türk Dil Kurumu |

| | |
|---|---|
| **TEMPEST** | Transient Electro Magnetic Pulse Emanation Standard |
| **TİB** | Telekomünikasyon İletişim Başkanlığı |
| **TUİK** | Türkiye İstatistik Kurumu |
| **UBE** | Unsolicited Bulk E-mail |
| **ULAKNET** | Ulusal Akademik Network |
| **UYAP** | Ulusal Yargı Ağı Projesi |
| **vb.** | ve benzeri |

# 1. GİRİŞ

İnternet ve bilgisayarın hayatımızda yaygın olarak kullanılmaya başlamasıyla eğitim, iş, sağlık, bankacılık ve ticaret gibi birçok alanda köklü değişiklikler meydana gelmiştir. Teknolojinin sosyal yaşantımızda yaptığı bu değişimler hayatımızı kolaylaştırmasına rağmen bir takım güvenlik sorunlarını da beraberinde getirmiştir. Teknoloji suç işlemeyi kolaylaştırmış ve bilişim suçları ortaya çıkmıştır.

Özellikle güvenlik boyutunda, bilişim sistemlerini kontrol altında bulundurmak maksadıyla, yazılımsal ve donanımsal önlemler cezai yaptırımlarla desteklenerek çepeçevre bir emniyet halkası oluşturulmaya çalışılmıştır. Vatandaşlarının huzur ve refahını sağlamakla mükellef yasa koyucu statüsündeki devlet, bilişim sistemleri aracılığıyla işlenen suçları denetim altında tutmaya çalışmıştır. Bu kapsamda, yasa koyucu cezai yaptırımlarla konuyu düzenleyerek kurumların bu alandaki denetim rolünü ortaya koymuştur. Yasa koyucu bilişim suçları konusunda ceza kanunu, fikir ve sanat eserleri kanunu, elektronik imza kanunu ve tüketicinin korunması hakkında kanun gibi yasal yaptırımlarla bu alana düzenleme getirmiştir.

Genel anlamda bilişim suçları ve bunların farklı boyutlarını inceleyen bu çalışma beş bölümden oluşmaktadır.

Birinci bölüm giriş bölümüdür. İkinci bölümde tezin kuramsal temelleri anlatılmakta ve konuyla ilgili yapılan araştırmaların verileriyle Türkiye İstatistik Kurumu (TUİK), İçişleri Bakanlığı Kaçakçılık, İstihbarat, Harekât ve Bilgi Toplama (KİHBİ) Daire Başkanlığı ve Bankalararası Kart Merkezi (BKM)'den alınan veriler ışığında bilişim suçlarına ait veriler incelenmiştir. Ayrıca bilgisayarlarla ilgili temel konularda bilgi verilecek, suç ve bilişim suçları kavramı açıklanacaktır. Bilişim suçlarının işlenme şekilleri, bilişim suçlarının tasnifi ve konuyla ilgili yasal düzenlemeler anlatılacaktır. Üçüncü bölümde çalışmadaki materyal ve metot açıklanacaktır. Dördüncü bölümde, toplumun bilişim suçları hususunda eğitim seviyesi en yüksek kişileri arasında sayılabilecek üniversitelerin Bilgisayar ve Öğretim Teknolojileri bölümü öğrencilerinin bilişim suçu hakkındaki bilgileri ve bilişim suçu mağduru olabilecekleri hakkındaki görüşleri ile bilişim suçları hakkındaki fikirleri

değerlendirilecektir. İlave olarak, bilişim suçu faillerinin, mağdurların hangi zaaflarından yararlanıp bu suçu işledikleri ceza infaz kurumlarında yapılan nitel anket çalışması ile araştırılacak, kredi kartı ve banka kartları dolandırıcılığı ve sahteciliği suçundan hükümlü bulunanların demografik özellikleri ortaya konacaktır. Beşinci bölümde ise genel bir değerlendirme yapılarak öneriler özetlenecek ve tez çalışması esnasında araştırılması önem arz eden konular belirtilecektir.

Bilişim Suçları ve Üniversite Lisans Öğrencilerinin Bilişim Suçlarına Yönelik Görüşleri konulu tezimde amacım; elde edilen veriler ışığında bilişim suçlarının istatistiklerini çıkarmak, bilişim suçlarının işlenme sebep ve yöntemleriyle, suçluların cinsiyet, yaş, iş ve medeni durumları gibi konularda hükümlülerle görüşerek araştırma yapmak ve üniversite öğrencilerinin bilişim suçlarına yönelik tutumlarını inceleyerek bilgi düzeylerini ölçmektir.

## 2. KURAMSAL TEMELLER VE KAYNAK ARAŞTIRMASI

Birçok farklı tanımla karşımıza çıkan bilişim suçları, bilgisayar suçu, internet suçları, siber suçlar, teknoloji suçları gibi adlarla anılmaktadır.

Aslında bu farklı adlandırmalar bir anlamda bilişim suçu tanımına açıklık getirmektedir. Şöyle ki, bilişim suçları bilgisayar ve internet ortamında işlenebileceği gibi teknoloji ürünü olan diğer elektronik sistem veya aletler kullanılarak da işlenebilir. Kredi kartı kopyalama ya da yasadışı CD, DVD çoğaltma gibi suçlar internet haricindeki diğer elektronik sistemlerin kullanımı yoluyla işlenmektedir.

Kayıtlara geçen ilk bilişim suçu, 18 Ekim 1966 tarihli Minneapolis Tribune gazetesinde yayımlanan "Bilgisayar uzmanı banka hesabında tahrifat yapmakla suçlanıyor" isimli makale ile kamuoyuna yansımıştır[1]. 1970'li yılların ilk yarısından itibaren hükümetler ve uluslararası kuruluşlar bilişim suçlarıyla ilgilenmeye ve bu alana düzenlemeler getirmeye başlamışlardır. Bilişim suçları ile ilgili ilk kapsamlı kanun teklifi 1977 yılında Senatör Ribikoff tarafından Amerikan Kongresi'ne sunulmuştur. Bu teklif Kongre tarafından kabul edilmemesine rağmen, bu suç grubunun dünya çapında tanınmasını sağlamıştır[2].

Avrupa Konseyi, 1970'li yıllarda elektronik bilgi bankalarında işlenen veriler dolayısıyla, bireylerin özel hayatının korunması amacına yönelik bir dizi çalışma başlatmıştır. 1973 ve 1974 yılında Avrupa Konseyi Bakanlar Komitesi, elektronik veri bankalarında uygulanacak ilkeleri kapsayan iki tavsiye kararı kabul etmiştir. Bu tavsiye kararları uyarınca başta Almanya olmak üzere Avusturya, Fransa, Danimarka, Norveç gibi ülkeler 1970'li yılların sonunda "Verilerin Korunması" konusunda özel yasaları hukuk mevzuatlarına dâhil etmişlerdir[3].

Telekomünikasyon sistemlerinde meydana gelen gelişmelere paralel olarak ülkelerarası iletilen veri miktarı ve hızı aynı oranda artmıştır. Aktarılan bu verilerin içerisinde yer alan elektronik veri bankalarındaki kişilerin özel hayatlarına ilişkin verilerin korunması önem arz etmiştir. Avrupa Konseyi üyesi ülkelerin mevzuatlarının bu verilerin güvenliğini sağlama hususunda yetersiz kalmalarından

dolayı, konuyu uluslararası boyutta ele alıp uluslararası bir sözleşme ile düzenleme gereği doğmuştur.

“Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması”na ilişkin 108 sayılı sözleşme, 28 Ocak 1981 tarihinde imzaya açılmış ve aynı tarihte Avrupa Konseyi üyesi ülkelerle birlikte Türkiye tarafından da imzalanmıştır[4].

Bilişim suçları ilgili ceza yasalarının birbirleriyle uyumlaştırma çalışmalarına 1983 yılında OECD ülkelerinde başlanmış ve “Bilgisayarla İlgili Suç: Hukuki Politikaların Analizi” raporu ile üye ülkelere birtakım gerekli düzenlemeleri yapmaları tavsiye edilmiştir[5].

Hukuk mevzuatımızda bilişim ve bilişim suçu ile ilgili ilk tanımlama 1989 tarihli Türk Ceza Kanunu Öntasarısında yer almaktadır. Müteakiben, bilişim suçu kavramı, Türk Ceza Hukukuna ilk defa 1991 yılında 3756 sayılı kanunla girmiş olup, Bilişim Alanında Suçlar başlığı 765 sayılı kanunun (mülga) 525’inci maddesinin a,b,c ve d bentleri, bilişim alanı ihlallerini bilişim suçu olarak adlandırmıştır. 765 sayılı Ceza Kanunun mülga olmasıyla birlikte

5237 sayılı Yeni Türk Ceza Kanunu yürürlüğe girmiştir. Bilişim suçları Bilişim Alanında Suçlar başlığı altında;

- m.243 hukuka aykırı olarak bilişim sistemine girme veya sistemde kalma suçu,
- m.244/1–2 bilişim sisteminin işleyişinin engellenmesi, bozulması, verilerin yok edilmesi veya değiştirilmesi suçu,
- m.244/4 bilişim sistemi aracılığıyla hukuka aykırı yarar sağlama suçu,
- m.245 banka veya kredi kartlarının kötüye kullanılması suçu olarak yasa koyucu tarafından tanımlanmıştır.

Yukarıdakilere ilave olarak, bilişim sistemleri ve teknolojileri yardımıyla işlenebilecek, fakat bilişim suçu sayılmayan suçlar da mevcuttur. Bunlar;

- Kişilere Karşı Suçlar kısmının dokuzuncu bölümünde, Özel Hayata ve Hayatın Gizli Alanına Karsı Suçlar başlığı altında m.132 haberleşmenin gizliliğini ihlal suçu,
- Kişilere Karşı Suçlar kısmının yedinci bölümü olan Hürriyete Karşı Suçlar bölümünde haberleşmenin engellenmesi suçu;
- Kişilere Karşı Suçlar kısmının sekizinci bölüm olan Şerefe Karşı Suçlar bölümünde m.125 hakaret suçu, malvarlığına karşı suçlar bölümünde m.142 fkr.2 b. 'e' nitelikli hırsızlık suçu, m.158 fkr.1 b. 'f' nitelikli dolandırıcılık suçu,
- Topluma Karşı Suçlar kısmının yedinci bölümü olan Genel Ahlaka Karşı Suçlar bölümünde m.226 müstehcenlik suçu ile m. 228 kumar oynanması için yer ve imkân sağlanması suçlarıdır.

## 2.1. Temel Bilgiler

Bu bölümde bilgisayarın tanımı, bilgisayar donanımları, bilgisayar ağları, bilişim ve internetin tarihi gelişimi hakkında temel bilgiler verilecektir.

### 2.1.1. Bilişim suçu

Bilişim suçları konusunda en geniş kabul gören tarif Avrupa Ekonomik Topluluğu Uzmanlar Komisyonu'nun Mayıs 1983 tarihinde Paris Toplantısı'nda yaptığı tanımlamadır. Bu tanımlamaya göre bilişim suçları; bilgileri otomatik işleme tabi tutan veya verilerin nakline yarayan bir sistemde gayri kanuni, gayri ahlaki veya yetki dışı gerçekleştirilen her türlü davranıştır[6]. Bilişim suçları; ileri teknoloji suçları, siber suçlar ve bilgisayar suçları gibi adlarla da anılmaktadır.

Bilişim suçları genel olarak elektronik bilgi işlem kayıtlarına yasadışı yollarla erişilmesi veya bu kayıtların yasal olmayan şekilde silinmesi, değiştirilmesi veya bu tür kayıtlara girilmesi olarak tanımlanabilir.

### 2.1.2. Bilgisayar

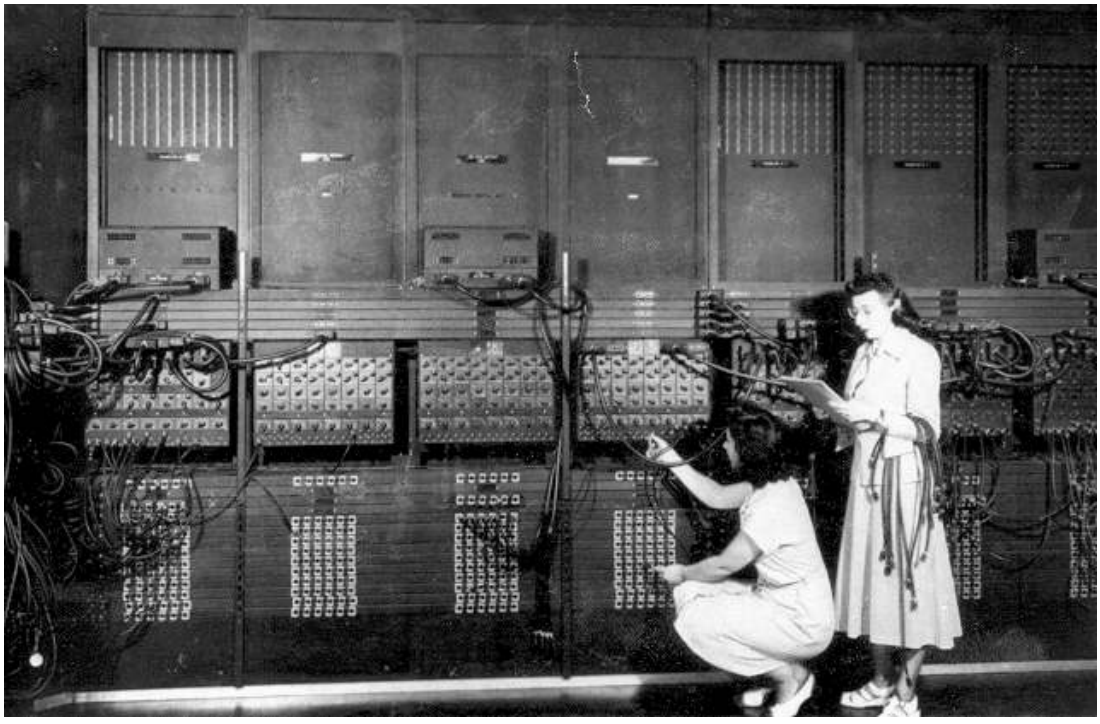
Bilgisayar terimi ülkemizde ilk olarak Prof. Dr. Aydın Köksal tarafından 1969 yılında Hacettepe Üniversitesi'nde ihtiyaç duydukları bilgisayarı kiralamak için verdikleri bir gazete ilanında kullanılmıştır.

Türk Dil Kurumu(TDK)'nun Türkçe sözlüğünde bilgisayar "Çok sayıda aritmetiksel veya mantıksal işlemlerden oluşan bir işi, önceden verilmiş bir programa göre yapıp sonuçlandıran elektronik araç, elektronik beyin." olarak ifade edilmektedir[7].

Bilgisayarlar, insanlar tarafından hazırlanıp yüklenen programlar yardımıyla bilgileri belirli bir düzende saklamak, isleyerek yeni sonuçlar üretmek, üretilen bilgileri başka yerlere iletmek, başka yerlerdeki bilgilere ulaşmak gibi amaçlarla kullanılan makinelerdir[8].

1950'li yıllarda transistörün bulunmasıyla başlayan süreç; tümleşik devreler ve lazerler, mikro işlemciler, yoğun yarı-iletken bellekler ile devam etmiş ve Bilgi Devrimini yaratmıştır[9].

Bilgi toplumunun hızlı gelişimi bilgisayar sayesinde olmuştur. Bilgisayar teknolojisi, ilk genel maksatlı elektronik bilgisayarlardan günümüze son 60 yılda inanılmaz bir gelişme göstermiştir[10]. ENIAC, 1946 yılında ABD ordusu tarafından geliştirilmiş ve ilk genel kullanım amaçlı elektronik bilgisayardır.



Resim 1.1. ENIAC - ilk genel kullanım amaçlı elektronik bilgisayar

Teknolojinin yaygınlaşması ve bilgisayara olan talep, fiyatların düşmesine sebep olmuştur. Eskiden toplu erişim yerlerinden internet ve bilgisayara ulaşılırken günümüzde ev kullanıcılarının sayısı hızla artmıştır.

TUİK'in 2010 yılında yaptığı araştırmaya göre bilgisayar kullanılan yerler; %70 ile ev, %31,3 ile işyeri, %17,5 ile internet kafe, internet kullanılan yerler ise; %62,8 ile ev, %31,6 ile işyeri, %20 ile internet kafe olarak sıralanmaktadır[11]. Araştırma, kişisel bilgisayara sahip olanların çoğunun ev kullanıcısı olduğu ve evdeki diğer aile fertlerinin de bu bilgisayar üzerinden internete eriştiğini gösteriyor. Araştırma ışığında evlerimizin dünyaya açılan kapımız haline geldiğini söylemek doğru bir tanımlama olacaktır.

Her geçen gün bilgisayarların işlev ve özelliklerinin artmasının yanı sıra, önceleri bilgisayar tanımlamasına girmeyen nesneler ve cihazlar da zamanla bilgisayar işlevleri görür hale gelmektedirler. Aslen bir iletişim aracı olmasına rağmen gelişen teknolojisi sayesinde bilgisayara dönüşmüş olan cep telefonları buna en güzel örnek olarak gösterilebilir. Zira telefon önceleri sadece kablolu iletişim aracı iken, gelişen uydu teknolojileri sayesinde kablosuz, mobil iletişim aracı haline gelmiştir. Günümüzde ise mobil telefonlar ile el bilgisayarları olan "Pocket PC" teknolojileri bütünleştirilerek geliştirilen cihazlar yaygın hale gelmiştir. Bu cihazlar minyatür bilgisayar gibi işlev görmekte, veri tutmakta, işlemektedir. Kullanıcılar internete bağlanabilmekte, elektronik posta servislerinden faydalanmakta, dosya oluşturarak iletim yapabilmekte, dijital fotoğraflar çekebilmekte ve bu fotoğrafları internet aracılığı ile 3. şahıslara ulaştırabilmektedirler[12].

Bilgisayarı kendine benzeyen diğer cihazlardan ayırt edici fonksiyonu konusunda netlik yoktur. Bilgisayarın, işlemini 4–5 temel işleme (toplama, çıkarma, çarpma, bölme, üs alma ve mantıksal karsılaştırma) dayandırarak yapması ayırt edici bir özellik olmayacağı gibi, elektronik olması veya programlanabilir olması da ayırt edici bir özellik değildir[4]. Cep telefonları, televizyonlar, hesap makineleri hatta otomobiller dahi programlanabilir. Önemli olan kullanılan bilgisayarın genel maksatlı olmasıdır[9]. Bir bilgisayar genel maksatlı olabilmesi için problem çözme yeteneğine sahip olmalıdır. Problem çözmekten kasıt, bilgisayarın kendisine

yöneltilmiş problemler ile ilgili çözümler üretmesi değil, insanlar tarafından o probleme çözüm olacak yazılım ile programlanabilmesidir. Buna ilave olarak, bilgisayarların problemleri öğrenerek benzer problemlerde benzer çözümler üretmesini sağlayan yapay zekâ programları da bulunmaktadır[12].

### 2.1.3. Donanım ve yazılım

Bilgisayarın elle tutulabilen fiziksel kısımları donanım olarak adlandırılır. Fiziksel parçaları kullanmak ve kontrol etmek için gereken programlara da yazılım denir. Yazılımlar belli bir işlemi yerine getirmek için bilgisayara kurulur. Örneğin, müzik dinlemek için medya oynatıcı programları (Windows Media Player, Winamp vb.) kullanılır.

Bilgisayarda temel olarak ana kart, merkezi işlem birimi, bellek, sabit disk ve bilgisayarda yaptığımız işlemleri ekranda görmemizi sağlayan ekran kartı bulunur. Yazılım, değişik ve çeşitli görevler yapma amaçlı tasarlanmış elektronik araçların, birbirleriyle haberleşebilmesini ve uyumunu sağlayarak, görevlerini ve kullanılabilirliklerini geliştirmeye yarayan makine komutlarıdır.

### 2.1.4. Bilişim

Bilişim sözcüğünün kaynağı, aynı kökten gelmekte olan Fransızca informatiqe sözcüğüdür. Bu sözcük Fransızca “information (bilgi)” ve “automatique (otomatik)” kelimelerinin birleşiminden türemiş olup, bilginin otomasyona tabi tutulması sonucunda işlenmesini yani verinin saklanması, organize edilmesi, değerlendirilmesi, nakledilmesi, çoğaltılması anlamlarını içermektedir[13]. Türkçeye çevrilerek “enformasyon” olarak da kullanılmıştır. Ancak sonradan bilgi vermek kökeninden gelen informatiqe sözcüğü terk edilerek Türkçe karşılığı olarak bilgi kökeninden gelen “bilişim” sözcüğü kullanılmaya başlanmıştır[14].

5237 sayılı Yeni Türk Ceza Kanununda, “bilgileri otomatik işleme tabi tutan sistem” yerine bu tür araçlarla işlenen suçları da kapsayabilmesi amacıyla “bilişim sistemi” terimi kullanılmıştır[15].

### 2.1.5. Veri

Bilişim sistemlerinin en temel birimidir. Bilişim sistemlerinde saklanan her şey bir veridir. Bilginin belirli bir formata dönüştürülmüş halidir[6]. Veri; bir yazı, bir resim ya da bir program olabilir.

Bilgi işlem sürecinin temel hammaddesi olarak çeşitli, sembol, harf, rakam ve işaretlerle temsil edilen veri; ham, işlenmeye hazır, işlenmemiş gerçekler ya da izlenimleridir[16].

### 2.1.6. İnternet ve internetin tarihi gelişimi

İnternet, dünya genelindeki bilgisayar ağlarını ve kurumsal bilgisayar sistemlerini birbirine bağlayan elektronik iletişim ağıdır[17].

İnternet, çok protokollü bir ağ olup birbirine bağlı bilgisayar ağlarının tümü olarak da tanımlanabilir. Binlerce akademik, ticari, devlet ve serbest bilgisayar ağlarının birbirine bağlanmasıyla oluşmuştur. Bilgisayarlar arasında bilgi çeşitli protokollere göre paketler halinde transfer edilir. İnternet üzerinde elektronik posta ve birbirine bağlı sayfalar gibi çok çeşitli bilgiler ve hizmetler vardır. İnternet üzerinden oyunlar da oynanabilir.

Internet, dünya kapsamında birçok bilgisayar sistemini TCP/IP protokolü ile birbirine bağlayan ve gittikçe büyüyen bir iletişim ağıdır. TCP/IP(Transmission Control Protocol/Internet Protocol), bilgisayarlar ile veri iletme/alma birimleri arasında organizasyonu sağlayan, böylece bir yerden diğerine veri iletişimini olanaklı kılan pek çok veri iletişim protokolüne verilen genel addır[18].

İnternetin ortaya çıkışı Amerikan Federal Hükümeti Savunma Bakanlığı'nın araştırma ve geliştirme kolu olan 'Savunma İleri Düzey Araştırma Projeleri Kurumu'na (DARPA- Defence Advanced Research Project Agency) dayanır.1969 yılında çeşitli bilgisayar bilimleri ve askeri araştırma projelerini desteklemek için Savunma Bakanlığı ARPANET adında Paket Anahtarlamalı Ağı oluşturmaya başladı. Bu ağ, ABD'deki üniversite ve araştırma kuruluşlarının değişik tipteki

bilgisayarlarını da içine alarak büyüdü. 1973 yılında, ağ için bir protokol seti geliştirmek amacıyla Stanford Üniversitesi'nde daha sonra University College London'ın da dâhil olduğu bir proje başlatıldı. 1978 yılına kadar İletim Kontrol Protokolü'nün (TCP - Transmission Control Protocol) dört uyarlaması geliştirildi ve denendi. 1983 yılında tüm ARPANET kullanıcıları İletim Kontrol Protokolü/Internet Protokolü (TCP/IP Transmission Control Protocol/Internet Protocol) olarak bilinen yeni protokole geçiş yaptılar. O yıl TCP/IP, ARPANET'i de içeren Savunma Bakanlığı internetinde kullanılmak üzere standartlaştırıldı. ARPANET Haziran 1990'da kullanımdan kaldırıldı[19]. ARPANET'in kaldırılmasına rağmen, TCP/IP protokolü kullanılmaya devam etti.

1991 yılında World Wide Web (dünya çapında ağ) geliştirilmiş ve bundan sonra yasal ve yasal olmayan pek çok ticari işte internet büyük bir hızla kullanılmaya başlanmıştır.[20].

Türkiye İnternete Nisan 1993'ten beri bağlıdır. İlk bağlantı ODTÜ'den gerçekleştirilmiştir. 64 kbit/san hızında olan bu hat, çok uzun bir süre, tüm ülkenin tek çıkışı olmuş ve Internet'i tüm Türkiye'de (öncelikle akademik ortamlarda) yaygınlaştırma çalışmaları yapılmıştır. Ege Üniversitesi'nden olan bağlantı ise, 1994 başlarında, 64kbit/san. hızı ile gerçekleştirilmiştir. Ardından sırayla, Bilkent Üniversitesi (Ekim 1995), Boğaziçi Üniversitesi (Kasım 1995) ve İTÜ (Şubat 1996) bağlantıları gerçekleşmiştir.

1996 yılı Ağustos ayında da TURNET çalışmaya başlamıştır. 1997 yılına gelindiğinde, akademik kuruluşların internet bağlantısını sağlayan ULAKNET çalışmaya başlamış ve üniversiteler nispeten hızlı bir omurga yapısıyla birbirlerine bağlanmış ve internet kullanır hale gelmişlerdir. 1999 yılı içerisinde, ticari ağ altyapısında büyük değişiklikler olmuş ve TURNET'in yerini TTNET adında yeni bir oluşum almıştır.

2000'lerin başında; ticari kullanıcılar TTNET omurgası üzerinden; akademik kuruluşlar ve ilgili birimler de ULAKNET omurgası üzerinden internet erişimine

sahip olmuşlardır. Ayrıca bu iki omurga arasında yüksek hızlı bağlantı mevcuttur[21].

Artan bağlantı hızları, kablosuz bağlantının yaygınlaşması ve ucuza erişilebilinen teknoloji sayesinde İnternet yaygınlaşmasına hızla devam etmektedir. TTNET 2012 yılı itibariyle ev kullanıcılarına 100 kbit/san hızında kadar bağlantı sağlayabilmektedir.

### 2.1.7. Kartlı ödeme sistemleri

Nakit kullanımı gerekmeksizin mal ve hizmet alımı veya nakit çekme olanağı sağlayan basılı kartı veya fizikî varlığı bulunmayan kart numarasına kredi kartı denir. Mevduat hesabı veya özel carî hesapların kullanımı dâhil bankacılık hizmetlerinden yararlanmayı sağlayan kartta ise banka kartı denir.

1990 yılında 13 kamu ve özel Türk bankasının ortaklığıyla, kartlı ödeme sistemi içerisinde bankalar arası yetkilendirme ve takası gerçekleştirmek, ortak sorunlara çözüm bulmak, kartlı ödeme sistemleri konusunda ülke çapında stratejik çalışmalar yapmak, yurtiçi kredi kartları kural ve standartlarını geliştirmek amacıyla Bankalar Arası Kart Merkezi (BKM) kurulmuştur. Türkiye, 31 Mart 2006 tarihinde kredi kartlarında şifreli döneme geçmiştir.2008 yılında BKM ve Turkcell tarafından dünyada ilk olarak 3D Secure ve Turkcell mobil imzanın entegrasyonu ile mobil imza bankacılık işlemlerinden sonra dünyada ilk kez, kredi kartı ile yapılacak alışverişlerde de kullanılmaya başlanmıştır.

## 2.2. Suç Kavramı

Suç, topluma zarar verdiği ya da tehlikeli olduğu kanun koyucu tarafından kabul edilen ve belirtilen eylem, davranış, tavır ve harekettir[22]. Suç devletin hukuk nizamı içinde kendisine netice ve müeyyide olarak ceza konulmuş olan fiildir[23]. Sonuç olarak suç haksız bir davranıştır ve suçun mağduru olan kişiye maddi ve manevi zararlar verir.

### 2.2.1. Suçun maddi unsuru

Bir suçun söz konusu olabilmesi için, kanuni tarifine uygun bir fiilin bulunması şartı, maddi unsuru ihtiva eder[24].Suçun maddi unsuru fiilidir. Ceza hukukunda fiil denilince hareketle netice arasında bulunması gereken nedensellik bağı anlaşılır[25].

### 2.2.2. Suçun manevi unsuru

Manevi unsur, işlenen fiil ile kişi arasındaki manevi bağı ifade etmektedir. Bu bağ tesis edilmeden, gerçekleştirilen davranış fiil niteliği taşımaz ve dolayısıyla, bir suçun varlığından söz edilemez[26].Suçun manevi unsurunu kusurluluk oluşturur. Kusurluluktan kasıt ise fiilin kusurlu olmasıdır.

### 2.2.3. Hukuka aykırılık unsuru

Bir fiilin suç sayılması için kanunda gösterilmiş olması ve karşısında bir ceza bulunması lazımdır[23]. Bir suçun varlığı için, suçta kanunilik prensibinin zorunlu bir sonucu olarak, işlenen fiilin kanunda gösterilen tarife uygun olması gerekir[24].

## 2.3. Türk Hukukunda Bilişim Suçları

### 2.3.1. 5237 sayılı Türk Ceza Kanununda bilişim suçlarıyla ilgili düzenlemeler

Madde 243. bilişim sistemine girme

Bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak giren ve orada kalmaya devam eden kimseye bir yıla kadar hapis veya adlî para cezası verilir. Yukarıdaki fıkrada tanımlanan fiillerin bedeli karşılığı yararlanılabilen sistemler hakkında işlenmesi halinde, verilecek ceza yarı oranına kadar indirilir.

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

Madde 244. sistemi engelleme, bozma, verileri yok etme veya değiştirme

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

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

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

Yukarıdaki fıkralarda tanımlanan fiillerin işlenmesi suretiyle kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlamasının başka bir suç oluşturmaması halinde, iki yıldan altı yıla kadar hapis ve beş bin güne kadar adlî para cezasına hükmolunur.

Madde 245. banka veya kredi kartlarının kötüye kullanılması

Başkasına ait bir banka veya kredi kartını, her ne suretle olursa olsun ele geçiren veya elinde bulunduran kimse, kart sahibinin veya kartın kendisine verilmesi gereken kişinin rızası olmaksızın bunu kullanarak veya kullandırtarak kendisine veya başkasına yarar sağlarsa, üç yıldan altı yıla kadar hapis ve beş bin güne kadar adlî para cezası ile cezalandırılır.

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

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

Birinci fıkrada yer alan suçun; haklarında ayrılık kararı verilmemiş eşlerden birinin, üstsoy veya altsoyunun veya bu derecede kayın hısımlarından birinin veya evlat edinen veya evlâtlığın, aynı konutta yaşayan kardeşlerden birinin zararına ait olarak işlenmesi hâlinde, ilgili akraba hakkında cezaya hükmolunmaz.

Birinci fıkra kapsamına giren fiillerle ilgili olarak bu Kanunun malvarlığına karşı suçlara ilişkin etkin pişmanlık hükümleri uygulanır.

Madde 142/2-e. nitelikli hırsızlık

Hırsızlık suçunun bilişim sistemlerinin kullanılması suretiyle işlenmesi hâlinde, üç yıldan yedi yıla kadar hapis cezasına hükmolunur.

Madde 158/1-f. nitelikli dolandırıcılık

Dolandırıcılık suçunun bilişim sistemlerinin, banka veya kredi kurumlarının araç olarak kullanılması suretiyle işlenmesi hâlinde, iki yıldan yedi yıla kadar hapis ve beş bin güne kadar adlî para cezasına hükmolunur. Ancak, TCK 158'nci maddenin 1'nci fıkrasında yer alan (e), (f) ve (j) bentlerinde sayılan hâllerde hapis cezasının alt sınırı üç yıldan, adlî para cezasının miktarı suçtan elde edilen menfaatin iki katından az olamaz.

Madde 226/5. müstehcenlik

Çocukların kullanıldığı müstehcen görüntü, yazı veya sözleri içeren ürünlerin içeriğini basın ve yayın yolu ile yayınlayan veya yayınlanmasına aracılık eden ya da çocukların görmesini, dinlemesini veya okumasını sağlayan kişi, altı yıldan on yıla kadar hapis ve beş bin güne kadar adlî para cezası ile cezalandırılır.

### 2.3.2. 5846 sayılı Fikir ve Sanat Eserleri Kanununa muhalefet

Madde 72. koruyucu programları etkisiz kılmaya yönelik hazırlık hareketleri

Bir bilgisayar programının hukuka aykırı olarak çoğaltılmasının önüne geçmek amacıyla oluşturulmuş ilave programları etkisiz kılmaya yönelik program veya

teknik donanımları üreten, satışa arz eden, satan veya kişisel kullanım amacı dışında elinde bulunduran kişi altı aydan iki yıla kadar hapis cezasıyla cezalandırılır.

### 2.3.3. Elektronik İmza Kanuna muhalefet

Madde 16. imza oluşturma verilerinin izinsiz kullanımı

Elektronik imza oluşturma amacı ile ilgili kişinin rızası dışında; imza oluşturma verisi veya imza oluşturma aracını elde eden, veren, kopyalayan ve bu araçları yeniden oluşturanlar ile izinsiz elde edilen imza oluşturma araçlarını kullanarak izinsiz elektronik imza oluşturanlar bir yıldan üç yıla kadar hapis ve beş yüz milyon liradan aşağı olmamak üzere ağır para cezasıyla cezalandırılırlar.

Yukarıdaki fıkrada işlenen suçlar elektronik sertifika hizmet sağlayıcısı çalışanları tarafından işlenirse bu cezalar yarısına kadar artırılır. Bu maddedeki suçlar nedeniyle oluşan zarar ayrıca tazmin ettirilir.

Madde 17. elektronik sertifikalarda sahtekârlık

Tamamen veya kısmen sahte elektronik sertifika oluşturanlar veya geçerli olarak oluşturulan elektronik sertifikaları taklit veya tahrif edenler ile yetkisi olmadan elektronik sertifika oluşturanlar veya bu elektronik sertifikaları bilerek kullananlar, fiilleri başka bir suç oluştursa bile ayrıca, iki yıldan beş yıla kadar hapis ve bir milyar liradan aşağı olmamak üzere ağır para cezasıyla cezalandırılırlar.

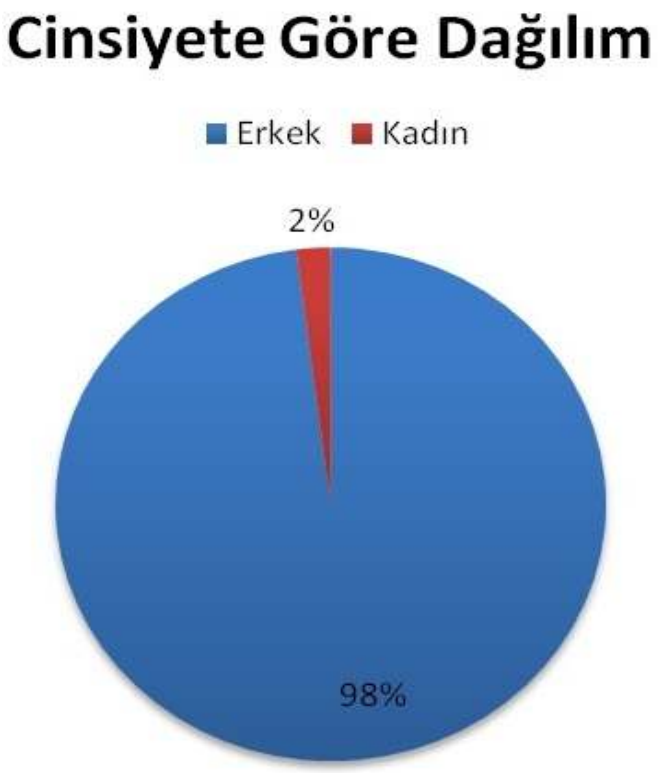
Yukarıdaki fıkrada işlenen suçlar elektronik sertifika hizmet sağlayıcısı çalışanları tarafından işlenirse bu cezalar yarısına kadar artırılır.Bu maddedeki suçlar nedeniyle oluşan zarar ayrıca tazmin ettirilir.

## 2.4. Türkiye'deki 2006–2010 Yılları Arasındaki Bilişim Suçları Verileri

### 2.4.1. 2006–2009 yıllarında ilgili Türk Ceza Kanunu maddelerinden hükümlü olanların bazı niteliklere göre dağılımı

Türk Ceza Kanununun(TCK) 2005 yılında değişmesiyle birlikte Yeni Türk Ceza Kanununda Bilişim Alanında Suçlar bölümünde düzenleme yapılmıştır.

Bilişim suçlarından hükümlü olanların cinsiyet, yaş, tahsil durumu, yapılan iş ve medeni durum gibi kıstaslara göre dağılımları Türkiye İstatistik Kurumu verileri ışığında aşağıda açıklanacaktır.




Şekil 2.1. 2006, 2007, 2008 yıllarında ilgili TCK maddelerinden hükümlü olanların cinsiyete göre dağılımı

2006–2008 yılları arasında işlenen bilişim suçu olaylarına bakıldığında toplam 199 kişi bilişim suçlarından mahkûm olmuştur. Suç işleyenlerin 195'i (%98) erkek, 4'ü (%2) kadındır.

Çizelge 2.1 2006, 2007, 2008 yıllarında ilgili TCK maddelerinden hükümlü olanların yaş-ilgili kanun maddesine göre dağılımı

| YAŞ | TCK 132 | TCK 133 | TCK 134 | TCK 135 | TCK 136 | TCK 243 | TCK 244 | TCK 245 | TOPLAM |
|---|---|---|---|---|---|---|---|---|---|
| **18-24** | 1 | - | 1 | - | - | 8 | 4 | 34 | **48** |
| **25-34** | 1 | 2 | 2 | - | 1 | 21 | 6 | 73 | **106** |
| **35-44** | - | - | - | 1 | - | 4 | 3 | 18 | **26** |
| **45-54** | - | - | - | - | - | 2 | - | 14 | **16** |
| **55-64** | - | - | - | - | - | - | - | 2 | **2** |
| **65+** | - | - | - | - | - | - | - | 1 | **1** |
| | **2** | **2** | **3** | **1** | **1** | **35** | **13** | **142** | **199** |

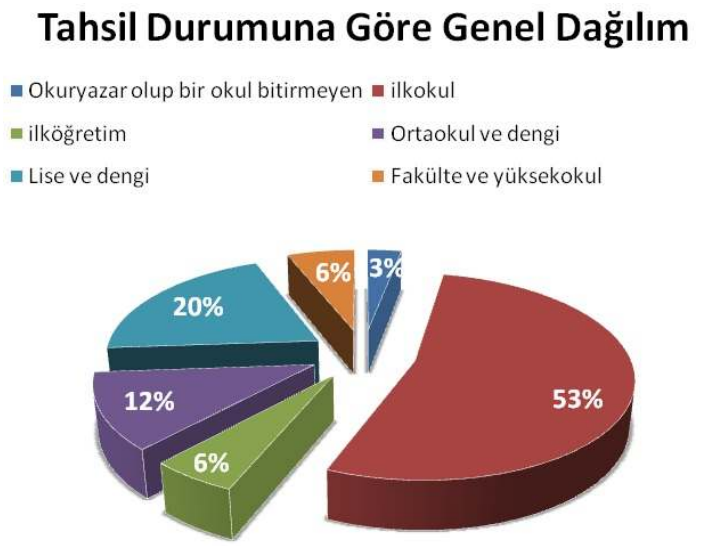
Çizelge 2.1'e bakıldığında TCK'nın 132, 133, 134, 135 ve 136'ıncı maddelerden dikkate değer bir hükümlü sayısı bulunmazken (9 kişi) 243, 244 ve 245'inci maddelerden toplam 190 hükümlü bulunmaktadır. En çok hükümlü sayısı 142 kişi ile 245'inci maddeden olmuştur.


Şekil 2.2. 2006, 2007, 2008 yıllarında ilgili TCK maddelerinden hükümlü olanların yaşa göre dağılımı

Suç işleyenlerin yaş ortalamalarına bakıldığında toplam 106 hükümlü(%53) ile 25–34, 48 hükümlü (%24) 18–24 ve 26 hükümlü (%13) 35–44 yaş aralığındadır.

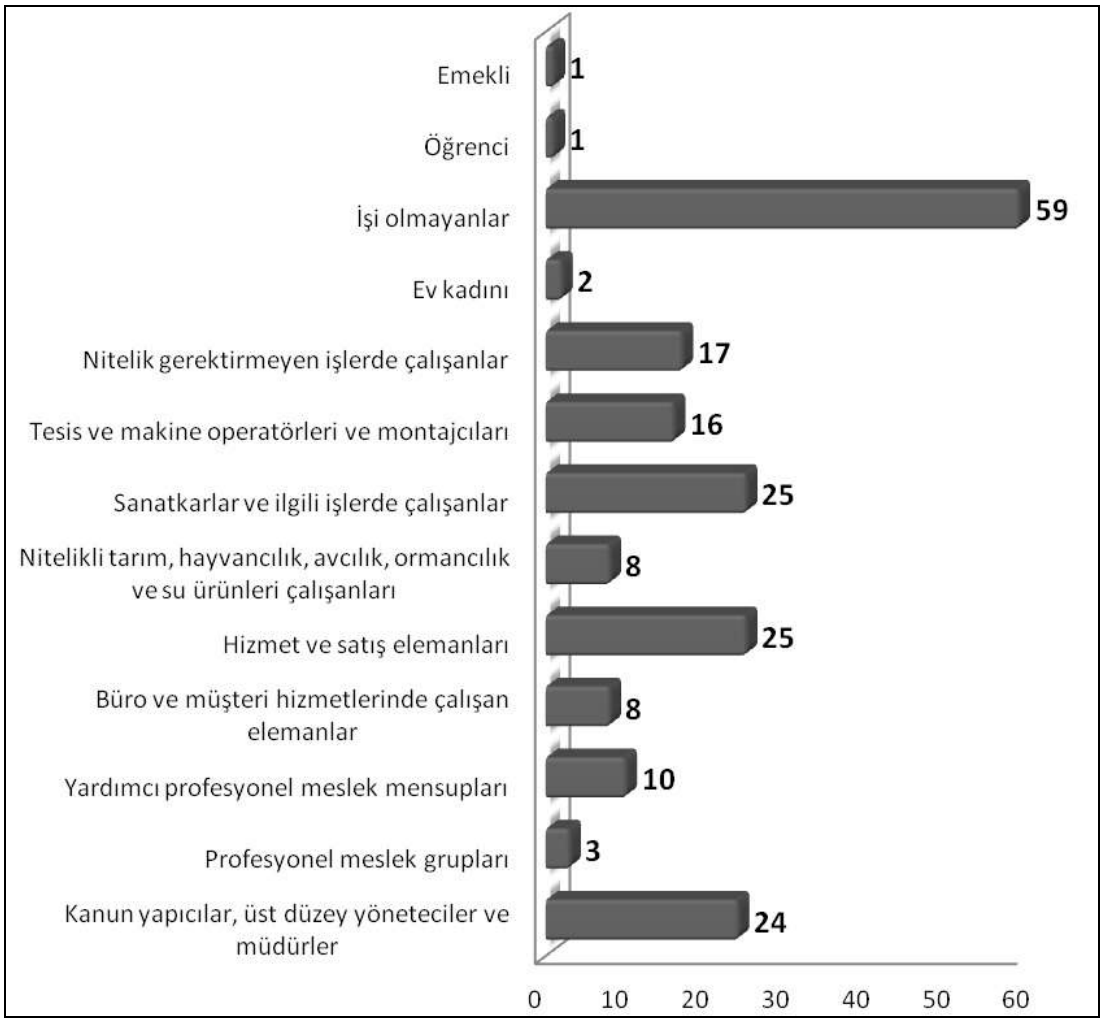
Çizelge 2.2. 2006, 2007, 2008 yıllarında ilgili TCK maddelerinden hükümlü olanların ilgili kanun maddesi-tahsil durumuna göre dağılımı

| TAHSIL DURUMU | TCK 132 | TCK 133 | TCK 134 | TCK 135 | TCK 136 | TCK 243 | TCK 244 | TCK 245 |
|---|---|---|---|---|---|---|---|---|
| **Okuryazar olup bir okul bitirmeyen** | - | 1 | - | - | - | - | 1 | 4 |
| **İlkokul** | 1 | 1 | 1 | 1 | 1 | 22 | 7 | 72 |
| **İlköğretim** | - | - | 1 | - | - | 1 | - | 9 |
| **Ortaokul ve dengi** | - | - | 1 | - | - | 3 | 2 | 18 |
| **Lise ve dengi** | 1 | - | - | - | - | 7 | 2 | 30 |
| **Fakülte ve yüksekokul** | - | - | - | - | - | 2 | 1 | 9 |
| **TOPLAM** | **2** | **2** | **3** | **1** | **1** | **35** | **13** | **142** |




Şekil 2.3. 2006, 2007, 2008 yıllarında ilgili TCK maddelerinden hükümlü olanların tahsil durumuna göre dağılımı

Çizelge 2.2.'ye bakıldığında en çok hükümlü sayısının 245'inci maddeden ve çoğunluğunun ilkokul mezunu olduğu görülmüştür. Kredi ve banka kartı dolandırıcılığının teknik bilgi ve bir takım teknolojik aletler gerektirdiği unutulmamalıdır. %53 oranla ilkokul mezunu olanların teknik bilgiye sahip olup olmadıkları veya bu suçları klasik yöntemlerle mi işledikleri konusunda veri bulunmamaktadır. Bu istatistiklere bakıldığında iyi eğitim ve teknik bilgi sahibi kişilerin bilişim suçlarını işleyebileceği yönündeki genel inanç yıkılmış olduğu gözükmektedir. TCK'de yer alan bilişim suçları sadece bilişim sistemine girme gibi yüksek bilgisayar bilgisi gerektirmez; kredi ve banka kartlarının kötüye kullanılması gibi dolandırıcılık suçları da bu suçlar kapsamındadır.



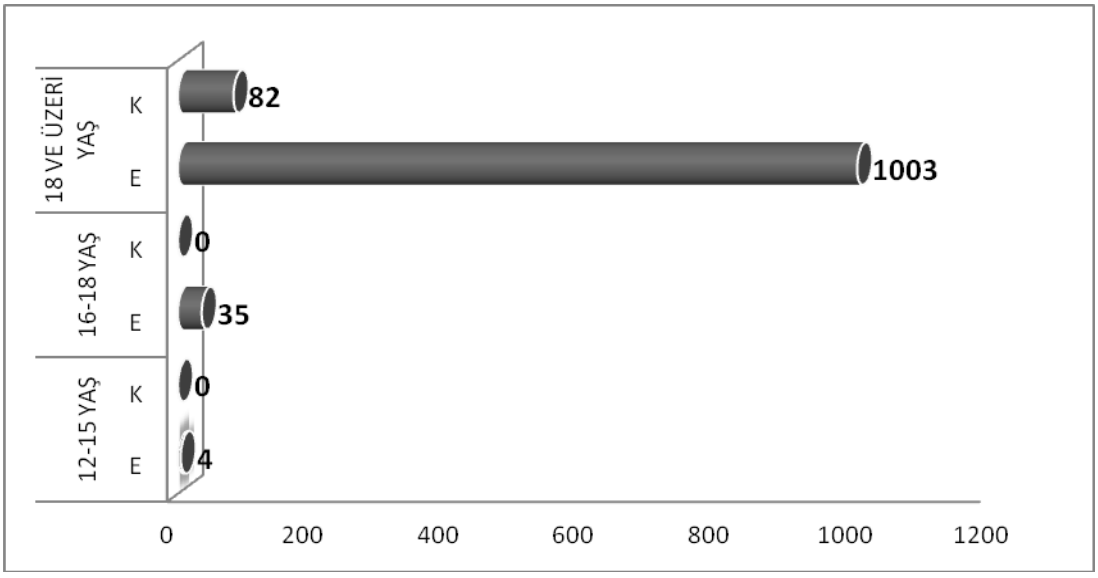

Şekil 2.4. 2006, 2007, 2008 yıllarında ilgili TCK maddelerinden hükümlü olanların iş durumuna göre dağılımı

Bilişim suçlarının büyük bir bölümünün işi olmayanlar tarafından işlendiği görülmüştür. Bu işsizliğin doğal bir sonucudur fakat geçim sıkıntısı olan insanların suç işlemeye meyilli olduğunu düşünmek yanlıştır. Dolandırıcılığı meslek olarak edinen insanların da olduğu unutulmamalıdır.

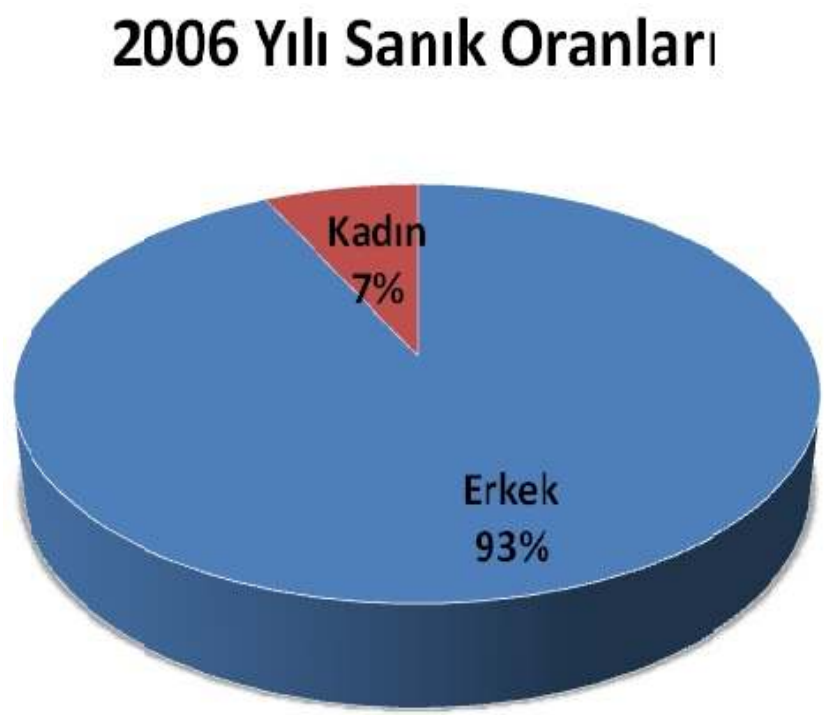
### 2.4.2. Ceza mahkemelerinde bilişim suçları ile ilgili açılan davalarda sanık ve mağdur sayılarının ile karar türlerinin suç türüne göre dağılımı

Adalet Bakanlığının 2000 yılında başlattığı Ulusal Yargı Ağı Projesinin devreye girmesiyle adli ve idari yargı birimleri, adli tıp ve ceza tevkif evleri işlemlerini bilgi sistemleri üzerinden yapmaya başladı. Bu sayede mağdur, hükümlü ve sanık sayılarının, davaların karar türlerinin ve hükümlülerin yaş, memleket gibi demografik özelliklerinin istatistikleri tutulmaya başlandı. Adalet Bakanlığı Adli Sicil ve İstatistik Genel Müdürlüğünün 2006–2010 yılları arasındaki bilişim suçları verilerinin çeşitli değişkenlere göre dağılımı şekillerde gösterildiği gibidir.

**01/01/2006 - 31/12/2006**

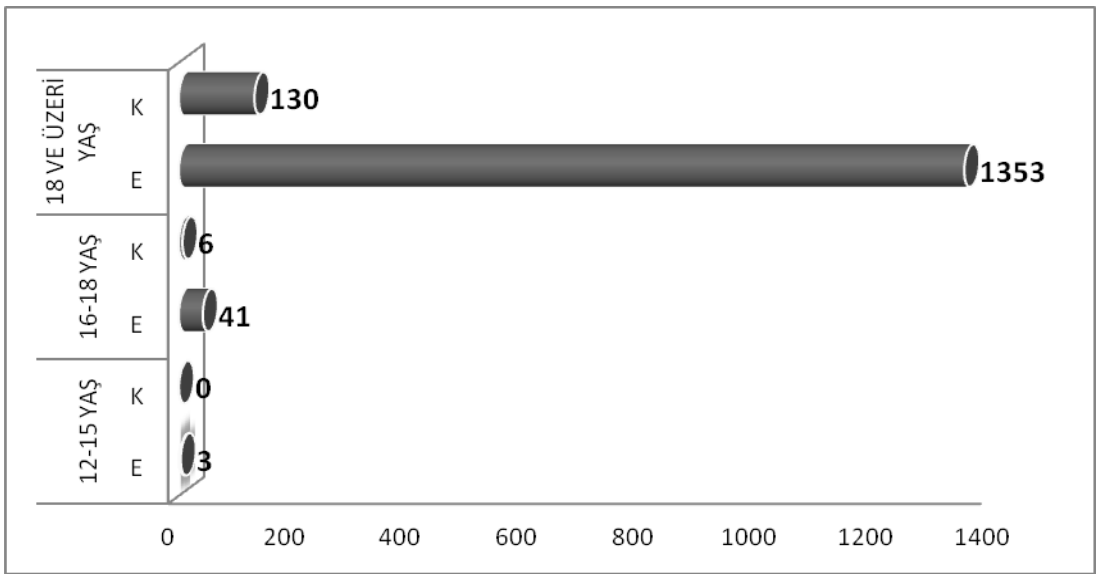



Şekil 2.5. 2006 yılı bilişim suçlarından sanık olanların yaş ve cinsiyete göre dağılımı.

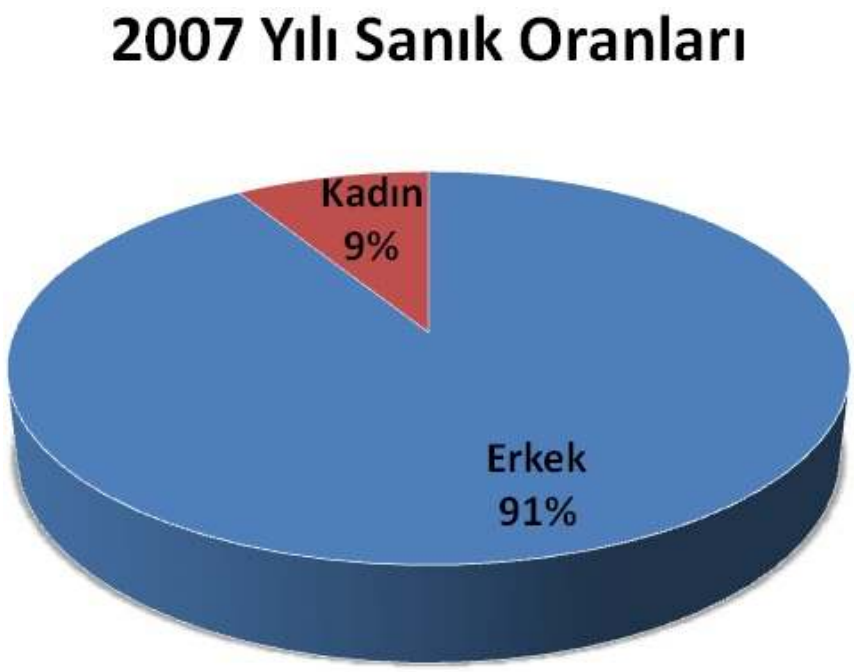



Şekil 2.6. 2006 yılı bilişim suçlarından sanık olanların cinsiyete göre dağılımı.

**01/01/2007 - 31/12/2007**

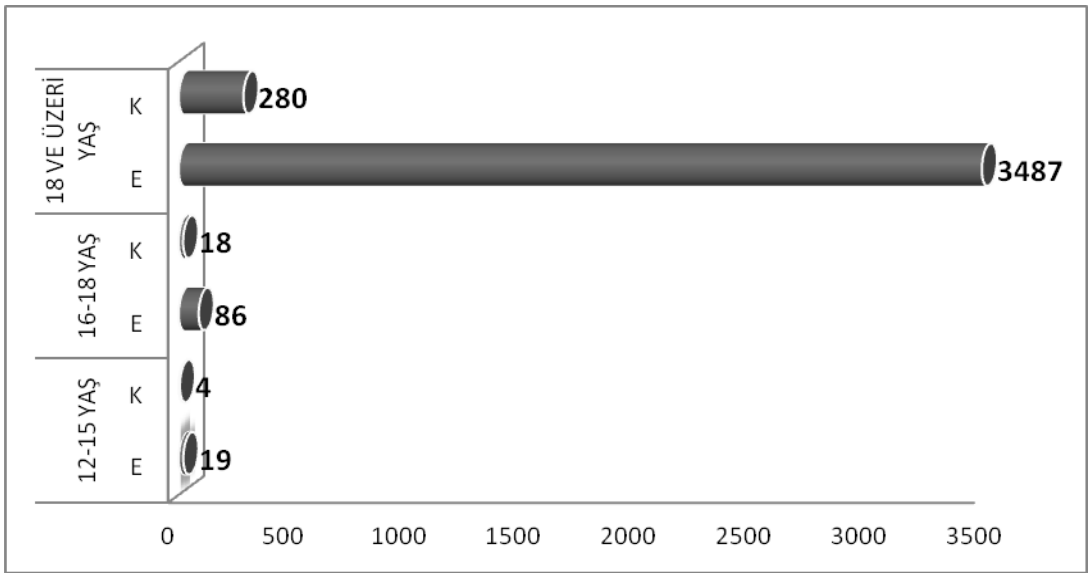



Şekil 2.7. 2007 yılı bilişim suçlarından sanık olanların yaş ve cinsiyete göre dağılımı

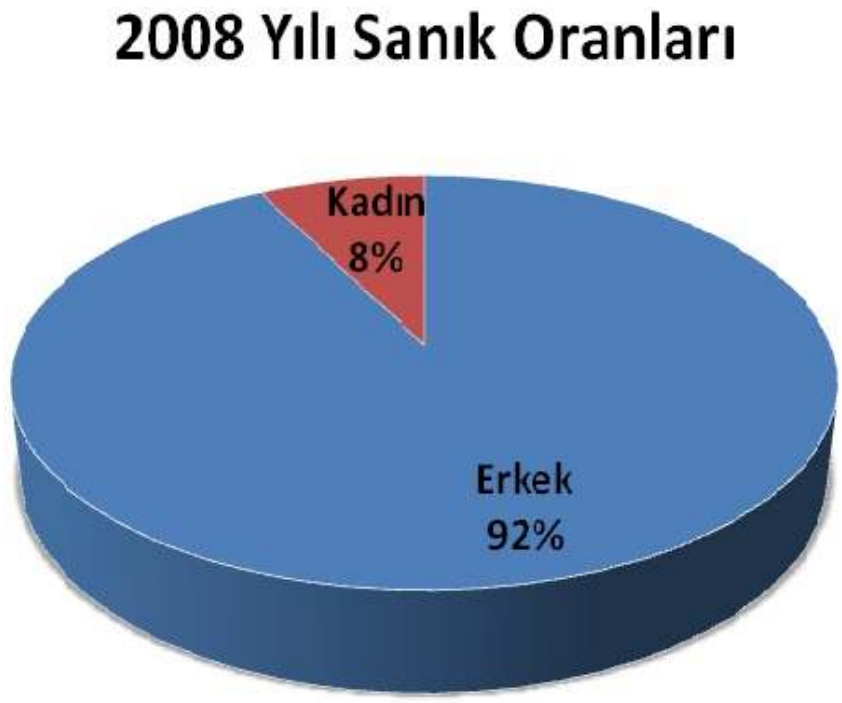



Şekil 2.8. 2007 yılı bilişim suçlarından sanık olanların cinsiyete göre dağılımı

**01/01/2008 - 31/12/2008**

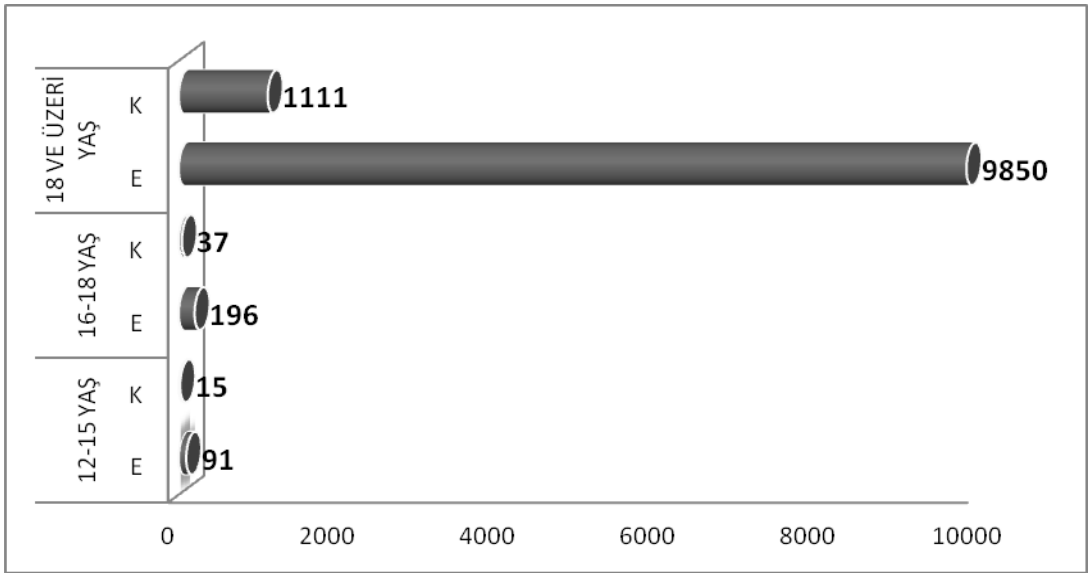



Şekil 2.9. 2008 yılı bilişim suçlarından sanık olanların yaş ve cinsiyete göre dağılımı




Şekil 2.10. 2008 yılı bilişim suçlarından sanık olanların cinsiyete göre dağılımı

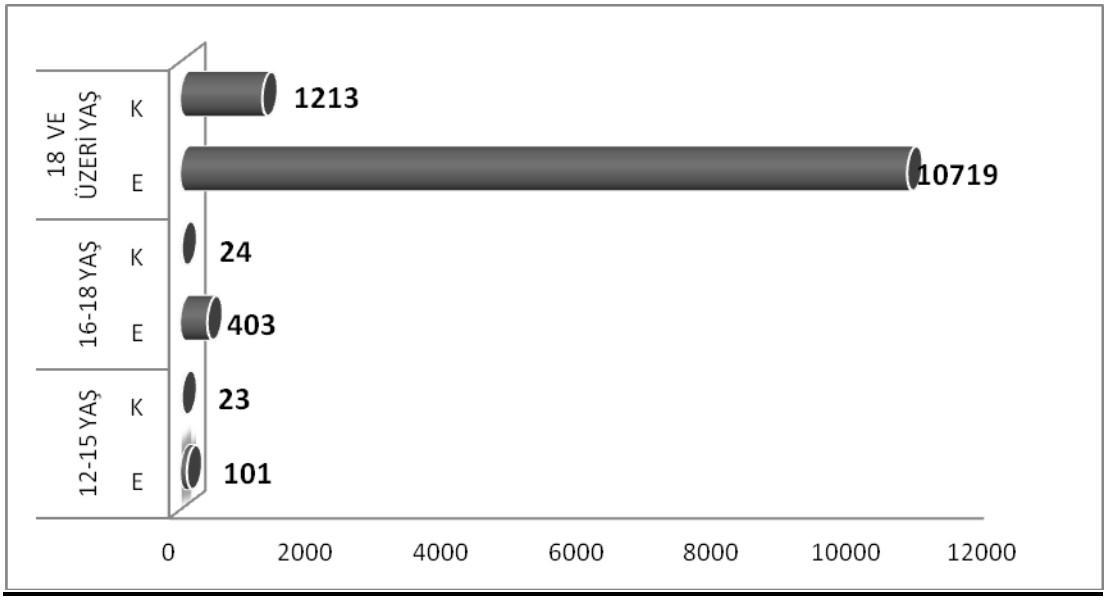
**01/01/2009 - 31/12/2009**



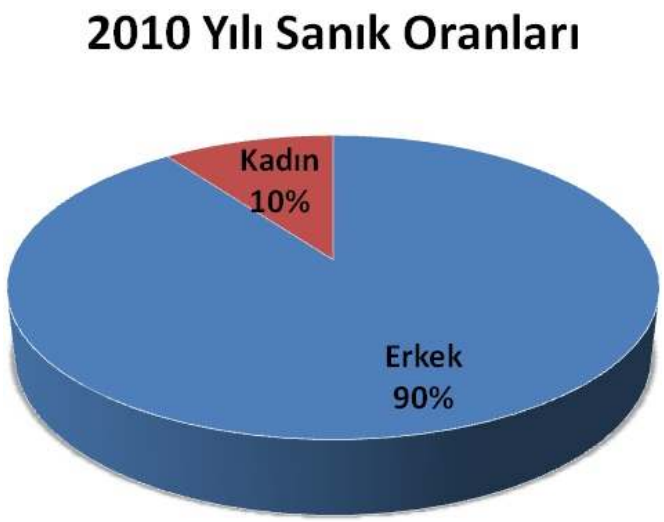

Şekil 2.11. 2009 yılı bilişim suçlarından sanık olanların yaş ve cinsiyete göre dağılımı


Şekil 2.12. 2009 yılı bilişim suçlarından sanık olanların cinsiyete göre dağılımı

**01/01/2010 - 31/12/2010**

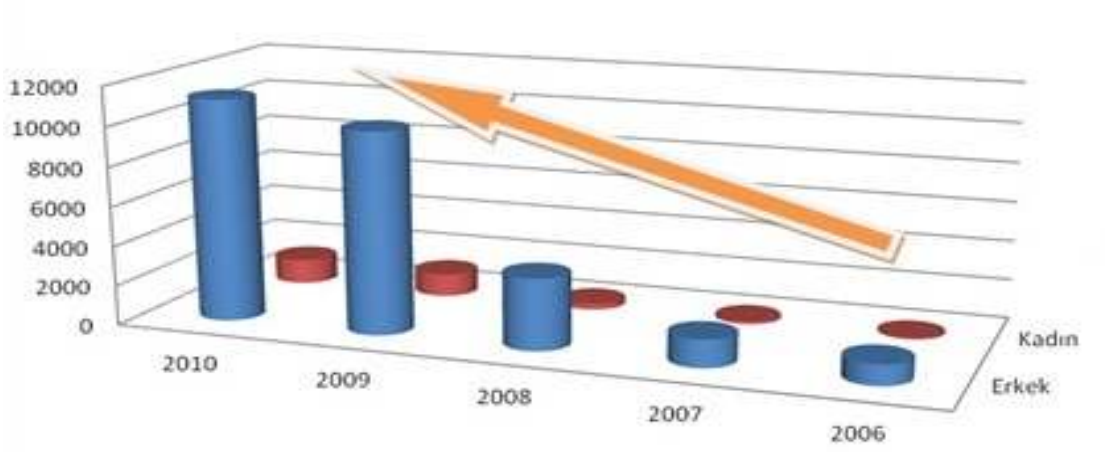



Şekil 2.13. 2010 yılı bilişim suçlarından sanık olanların yaş ve cinsiyete göre dağılımı




Şekil 2.14. 2010 yılı bilişim suçlarından sanık olanların cinsiyete göre dağılımı

## 2006-2010 Yılları Sanıkların Cinsiyete Göre Dağılımı

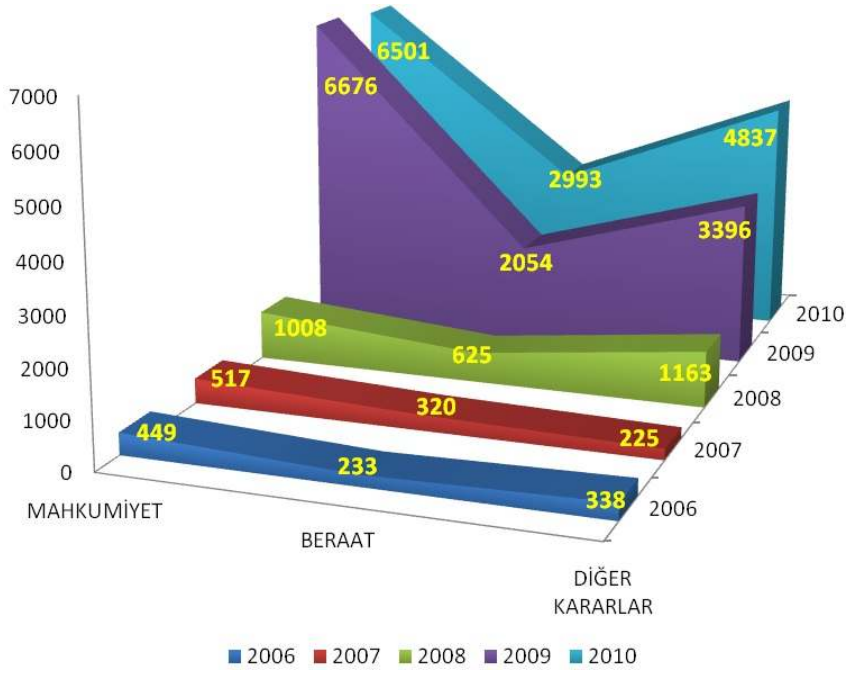



| | 2010 | 2009 | 2008 | 2007 | 2006 |
|---|---|---|---|---|---|
| Erkek | 11223 | 10137 | 3592 | 1397 | 1042 |
| Kadın | 1260 | 1163 | 302 | 136 | 82 |

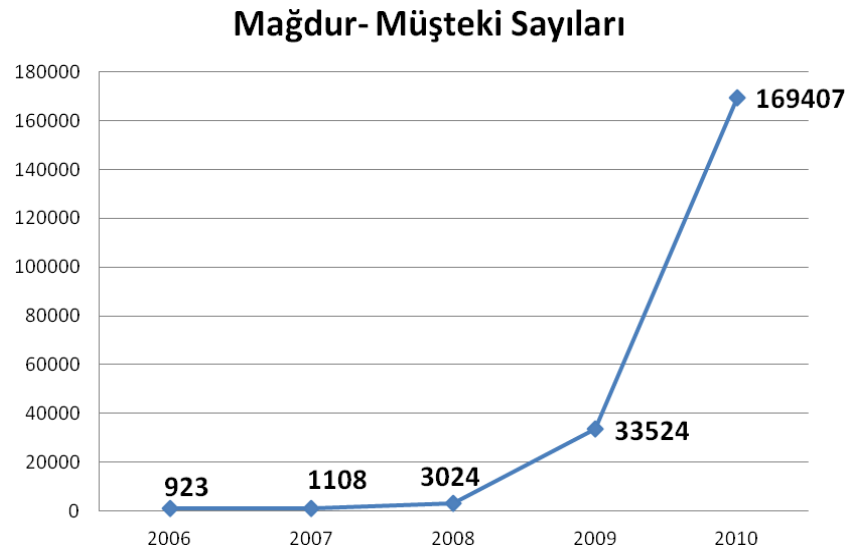
Şekil 2.15. Bilişim suçlarından sanık olanların cinsiyet ve yıllara göre dağılımı

2006 ile 2010 yılları arasındaki Adalet Bakanlığının verilerine bakıldığında her geçen yıl suç oranlarında artış olduğu görülmektedir. (Bknz. Şekil 2.15) Teknolojinin gelişmesiyle birlikte suç tekniklerini öğrenme ve suç argümanlarını elde etmedeki kolaylık, bu suç türünün artmasına sebep olmuştur. Fakat bu suç türünden sanık

olanların hepsinin suçlu olduğu kanısına varılmamalıdır. Mahkemelerin verdiği kararlar aşağıda gösterildiği gibidir.




Şekil 2.16. Ceza mahkemelerinde TCK uyarınca karara bağlanan davaların sanıkları hakkında verilen kararların ve suç türüne göre dağılımı




Şekil 2.17. 2006–2010 yılları arasındaki mağdur-müşteki sayıları

2006-2010 yılları arasındaki mağdur sayılarına baktığımızda özellikle 2010 yılında artışın fazla olduğu görülmektedir. Mağdur sayısındaki artış bilişim suçlarının artık daha geniş kitlere yönelik tehdit oluşturmaya başlamasından kaynaklanmaktadır. Bilişim suçları konusunda kendimize fazla güvenmemiz konusunda Kevin Mitnick[1]'in dediği gibi "Güvenlik zincirindeki en zayıf halka insandır[27]." Bilişim suçları günümüze küresel boyutlara ulaşmıştır. Örneğin Çinli bir bilgisayar korsanı, internet üzerinden Rusya'daki bilgisayarları kontrol edip Türkiye'deki internet kullanıcılarına spam gönderiyorsa, bu suç birçok ülkeyi kapsayan uluslar arası bir boyuta ulaşmış demektir. Bu şekilde işlenen suçlar sonucu ortaya çıkan dünyanın çeşitli yerlerindeki mağdurlar hangi mahkemelerde haklarını arayacaktır? Ülkemizde bilişim suçu mağdurlarının bu konuda nasıl müracaatta bulunacaklarını ve hangi kanunlarla korunduklarını bilemediklerinden kendi yöntemleri ile mağduriyetlerini gidermeye çalışmaktadırlar. Bütün bunlar bilişim suçları konusunda çözülmeyi bekleyen sorunlardır

## 2.5. Bilişim Suçlarının Tasnifi

### 2.5.1. Bilgisayar sistemlerine ve servislerine yetkisiz erişim

Yetkisiz erişim bir bilgisayar sistemine ya da bilgisayar ağına yetkisi olmaksızın erişmektir. Saldırganın hedefi bir bilgisayar sistemi ya da ağıdır. Saldırgan sistemin bir kısmına ya da bütününe, programlara veya içerdiği verilere ulaşma çabasındadır. İletişim metodu önemli değildir. Saldırgan bilgisayara direkt olarak yakın bir yerden erişebileceği gibi, uzak bir mesafeden örneğin bir modem hattı ya da başka bir bilgisayar sisteminden de erişebilir.

Hizmete ilişkin gizlilik dereceli bilgi ve belgelerin şirket ve kurumların bilgisayar sistemlerinde muhafaza edildiğini düşündüğümüzde, bilgisayar sistemlerine erişen kişilerin bu kuruluşlara ciddi zararlar verebileceği aşikârdır.

[1]İlk bilgisayar korsanlarından olup en meşhurudur. 15 Şubat 1995'te FBI tarafından yakalanmıştır. Fujitsu, Motorola, Nokia ve Sun Microsystems gibi şirketlerin bilgisayar ağlarına izinsiz girmekten suçlu bulunarak 5 yıl hapis cezası almıştır. Cezası 21 Ocak 2000'de, bilgisayarlara yaklaşma yasağı 21 Ocak 2003'te bitmiştir. Günümüzde, beyaz şapkalı bir bilgisayar korsanı olarak güvenlik danışmanlığı yapmakta ve dünya çapında kongrelere katılmaktadır.

### 2.5.2. Bilgisayar sabotajı

Yetkisiz erişimin eyleme geçmiş hali olarak nitelendirilen Bilgisayar Sabotajı, sisteme yetkisiz erişimle birlikte, aynı zamanda eriştiği sistemin içerdiği bilgileri silme veya değiştirme olarak ifade edilmektedir. Bir bilgisayara veyahut sisteme yetkisiz erişim sağlayanlar; sadece eriştiği bilgileri incelemekle ve kopyalamakla kalmamakta, bu bilgileri değiştirebilmekte, silebilmekte ya da bu bilgileri kanun dışı kullanmak isteyenlere satabilmektedirler.

Bilgisayar sabotajı mantıksal ve fiziksel olmak üzere iki şekilde yapılabilir. Fiziksel bilgisayar sabotajı, fiziki şiddet uygulayarak sistemin zarar görmesi ve bilgilerin silinmesidir. Bunu yaparken amaç maddi zarara yol açmak değil sistemin çalışmasını engellemektir. Mantıksal sabotajda ise bilgisayar sistemleri aracılığıyla hedef sisteme ulaşarak, sistemi kullanılmaz hale getirmek amaçlanmaktadır.

### 2.5.3. Bilgisayar yoluyla dolandırıcılık

Bilişim sistemlerindeki verilerin ve programların değiştirilmesi, sahte veriler girilmesi, mevcut verilerde tahribat yapılması gibi birtakım hileli hareketler sonucu haksız çıkar elde etmeğe yönelik eylemler, bilişim sistemlerinin aracı olarak kullanıldığı dolandırıcılık eylemleridir.

Bilgisayar dolandırıcılığındaki amaç suçluya veya bir başkasına mali kazanç sağlamak ya da mağdura ciddi kayıplar verdirmektir. Bilgisayar dolandırıcılığı suçlarının, suç işleme teknikleri açısından klasik dolandırıcılık tekniklerinden farklılıkları vardır.

Bu suçlara örnek olarak sahte isimlerle e-postalar gönderilip cazip komisyonlar ve bedeller teklif edilerek, insanların tuzağa düşürülmesi gösterilebilir. Bu tekliflerle ilgilendiğiniz zaman sizden para sızdırma yoluna gidilmektedir. Haziran 2011'de İstanbul İl Jandarma Komutanlığı yaptığı operasyonda, suç şebekenin sanal alışveriş yapılan web sitelerinin benzerlerini yaparak, mağdurların bu sitelere giriş yapmasını sağladıkları, daha sonra da dolandırdıklarını belirledi. Kendisinin gerçek sitede olduğunu zanneden kişilerin, bilgisayar üzerinden girdikleri kredi kartı bilgilerini

alan zanlıların, bu bilgilerle başka sitelerde alışveriş yaptığı ve bu yöntemle şu ana kadar 872 kişiyi kandırarak 840 bin TL dolandırıcılık yaptıkları ortaya çıkarıldı.

### 2.5.4. Bilgisayar yoluyla sahtecilik

Bilişim sistemleri kullanılarak gerçekleştirilen sahteciliği iki ayrı türde anlamamız gerekmektedir. Birincisi, klasik olarak bilinen sahtecilik suçunun bir bilişim cihazı aracılığıyla işlenmesidir. Yani sanal değil, günlük hayatta kullanılacak, çoğunlukla matbu olan unsurun hazırlanması halidir. İkincisi tamamıyla sanal ortamda gerçekleştirilen sahtekârlıklardır. Bu durum hem sanal ortamda mevcut olan verilerin değiştirilmesi hem de sahtelerinin hazırlanması şeklinde gerçekleşebilir[28].

Dijital ortamda tutulan bilgilerin üzerinde değişiklik yapmak sahteciliktir. Baskı teknolojilerinin gelişmesiyle birlikte evrak sahteciliğinde artış olmuştur. Yakalan zanlıların üzerinde çıkan sahte kimlikler alışılmış bir durumdur. Günümüzde başkalarının adına e-posta göndererek ticari ve özel ilişkilerin zedelenmesine neden olmak; başkalarının adına web sitesi hazırlamak ve bu web sitesinin tanıtım amacıyla başka kişilere e-posta gönderip ve bu e-postada mağdur olan şahsın telefonları verilerek suç işlenmektedir. Ayrıca resmi evraklar üzerinde yapılan değişikliklerle söz konusu evrakları bir suç nesnesi haline dönüştürerek bu evrakı çıkarmaya yetkili devlet memurları suçlu duruma düşürülmektedir. Adli bilişim safhasında yapılan incelemeler bu suç türünün aydınlatılmasına yeterince olanak vermemektedir.

### 2.5.5. Bilgisayar yazılımının izinsiz kullanımı

Fikir ve Sanat Eserleri Kanunu'nda 'eser' olarak kabul edilen bilgisayar yazılımlarının lisans haklarına aykırı olarak kullanılması halinde izinsiz kullanım gerçekleşmiş olur. Bilgisayar yazılımları satın alınırken üzerinde gelen lisans sözleşmelerinde; bir yazılımın bir adet kopyasının, ancak onu satın alan kişi tarafından yapılabileceği ve bu yazılımın başka bir kişi tarafından kopyalanamayacağı ve kiralanamayacağı belirtilmektedir[29].

Korsan yazılımın ülkemizde gelişim göstermesinin sebebi orijinal yazılımların pahalılığı ve özellikle ticari amaçla kullanılan Office yazılımları ile görüntü ve grafik

işleme yazılımları konusunda, işletmelerin istihdam girdi maliyetini düşürme çabasından kaynaklanmaktadır. Korsan yazılımların rahatlıkla elde edilebilir olması, her türlü yazılım ve materyalin tüketicilere ucuz ve kolay bir şekilde ulaşmasını sağlarken, her alanda yetkin ve kendini yetiştirmiş nitelikli elemanların ortaya çıkması ve yazılım alanında daha fazla sayıda insanın yasal olamayan bu tip kaynaklara erişebilmesi imkânını doğurmuştur.

Türkiye'de de faaliyet gösteren Business Software Alliance (BSA) tarafından hazırlanan 2010 raporu, lisanslı yazılımların toplumdaki kabulünün korsan yazılıma göre daha yaygın olduğunu göstermektedir. Türklerin % 60'ı lisanslı yazılımın daha iyi olduğuna inanırken, % 40'lık bir kesim ise korsan yazılımın iyi olduğunu düşünüyor. Dünya ortalamasına bakıldığında kullanıcıların % 88'i için teknik destek önemli iken % 72'si için işlevsellik ön plana çıkıyor. Bilgisayar kullanıcılarının bir kısmında oluşan sorun ise, lisanslı yazılım alıp çoklu bilgisayarlara yüklemek veya ağ bağlantılarından aktarım yapmak gibi yazılım edinmenin yasal olmadığının bilinmemesidir[30].

Aynı araştırmaya göre Türkiye'nin de yer aldığı Ortadoğu ve Afrika bölgesindeki ülkelerde korsan yazılım kullanma oranı % 58'dir.

Korsan yazılım kullanılmasının neden olduğu vergi kayıpları, virüs ve solucanların yayılmasından ortaya çıkan güvenlik sorunları, yasal süreçleri uygulayan firmaların korsan yazılım kullanan firmalarla rekabet edememesi ve bilginin değersizleşip ucuzlaşması ve önemsizleşmesi kültürünün ortaya çıkmasına sebep olmaktadır.

### 2.5.6. Verilere yönelik suçlar

Türkiye'nin de taraf olduğu Avrupa Konseyi Siber Suçlar Sözleşmesinin 2'nci Maddesine göre devletler verilerin güvenliğini korumaya yönelik tedbirler almak zorundadır. Verilere yönelik suçlar verilerin çalınması, durdurulması, değiştirilmesi ve silinmesine yönelik olabilir. Bilişim sistemleri üzerinden yapılan bu suçlar mağdurun kişisel verilerinin elde edilip kötüye kullanılması ve maddi kazanç elde edilmesi şeklinde olur.

İnternet ortamında kullanıcılar hakkında veri toplamaya veri korsanlığı denir. Bu uygulama reklam ve istatistik amacıyla yapılmakta çoğunlukla kişisel bilgisayarlarda ve internet servis sağlayıcılarında bulunan veriler kredi kartı ve hesap hırsızlığı amacıyla kullanılmaktadır[31].

### 2.5.7. Yasadışı yayınlar

Yasadışı olarak kabul edilen materyallerin bilgisayar sistemleri aracılığıyla yayınlanması ve dağıtılması olarak ifade edilmektedir. Kanunun yasaklamış olduğu bu materyaller; internet siteleri, e-postalar, iletişim sağlayan her türlü araç, optik araçlar tarafından kayıt yapan tüm sistemler olarak kabul edilmektedir.

Yasadışı yayınlar vatanın bölünmez bütünlüğüne aykırı olarak hazırlanmış terör içerikli internet siteleri ile belirli bir kişi veya zümreyi hedef alan ve hakaret niteliği taşıyan internet siteleri ve elektronik dokümanlar olabilir. Bu tür siteleri hazırlayanların asıl amacı sansür konulmuş Anayasaya aykırı fikirlerini, interneti kullanarak yaymaktır.

### 2.5.8. Terörist faaliyetler

Bilgi sistemleri doğrultusunda, elektronik araçların, bilgisayar programlarının ya da diğer elektronik iletişim biçimlerinin kullanılması aracılığıyla, ulusal denge ve çıkarların tahrip edilmesini amaçlayan, kişisel ve politik olarak motive olmuş, amaçlı eylem ve etkinliklerdir[32].

Ülkemizde internet üzerinden yapılan terörist faaliyetler kullanıcının tespiti zor olduğu için internet kafeler üzerinden yapılmaktadır. Aynı şekilde hakaret ve şantaj içerikli e-postalar ve sahte ihbarlar yine internet kafeler üzerinden yapılmakta, oturum ve kullanıcı takibi yapmayan ve güvenlik kamerası olmayan denetimsiz yerlerden yapılan bu saldırılarda failin tespiti güçleşmektedir.

### 2.5.9. Çocuk pornografisi (Paedophilia)

İnternetin ve gün geçtikçe gelişen dijital teknolojinin, müstehcen içerikli görsellerin üretimini ve dağıtımını kolay ve ucuz hale getirdiği artık bilinen bir gerçektir. Teknolojideki bu değişim internetin zararlı yönlerinden biri olan pornonun hazırlanmasına ve dağıtımına katkıda bulunmuştur. Bu istenmeyen gelişme toplumların ahlaki değerlerine yönelik önemli bir tehdittir.

Çocuk pornografisi, genel anlamda 15 yaş altındaki çocukların cinsel istismarını içeren filmler ve resimlerden oluşan, uluslararası olarak da yasaklanmış pornografi türüdür. Bu tür filmlerin çekilmesi, üretilmesi, indirilmesi, dağıtılması, paylaşılması suçtur.

Bu sitelerin çoğunluğu ABD'de yapılmaktadır. Çocuk pornografisi ile ilgili koleksiyon yapan bağımlıların tespiti ile yakalanması yoluna gidilmektedir. 'Child porn (çocuk pornosu)' cümleciğini aratma konusunda Pakistan dünyada birinci sırada yer almaktadır[33].

### 2.5.10. Kartlı ödeme sistemlerinde sahtecilik ve dolandırıcılık teknikleri ve kullanılan aletler

Birinci bölümdeki istatistiklerin de gösterdiği gibi ülkemizde en çok işlenen bilişim suçu türü kredi kartı ve banka kartları sahteciliği ve dolandırıcılığıdır. (Bknz. Şekil 2.4) Kredi ve banka kartları dolandırıcılığı interaktif yöntemlerle yapılabileceği gibi bilgisayar sitemleri ile klasik dolandırıcılık yöntemlerinin birleştirilmesi suretiyle de yapılabilir. Bu suç türünün işleniş biçimi incelendiğinde, sahte kimlik ve belgelerle başkasının hesabından para çekilmesi, banka ve diğer kredi kuruluşlarından verilmemesi gereken bir kredinin sahte evrak kullanılarak veya başka yöntemlerle alınması şeklinde ortaya çıkabilmektedir. Bahsi geçen diğer yöntemler, o çıkar amaçlı suç organizasyonunun etkinliği ölçüsünde değişmektedir[34].

2008 ve 2009 yıllarında 1679 adet banka kartları dolandırıcılığı vakası meydana gelmiştir. 2010 yılı BKM raporuna göre Türkiye'de 47 milyon kredi kartı, 1,82 milyon POS terminali, 27 bin ATM ve 70 milyon banka kartı bulunmaktadır. 2010

yılı kredi kartı cirosu 236 milyar TL'dir[35].Bu rakamlara bakıldığında kredi kartı kullanımı ve güvenliği konusuna özellikle değinmek gerekir.

Bu suç kart hamiline ulaşmayan ve kayıp/çalıntı kartlar, sahte belgelerle hesap açılması veya kart hamilinin hesap bilgilerinin ele geçirilip hesabın devredilmesi şeklinde işlenir.

Dolandırıcılar, sahte alış veriş siteleri, bahis siteleri ve cep telefonlarına gelen mesajlar aracılığıyla kart hamillerinin kredi kartı bilgilerini modern tekniklerle ele geçirip banka hesaplarındaki paraları boşaltabilirler. Ayrıca birçok hesaptan düşük meblağlarda para çekip mağdurun bilgisi dahi olmadan haksız kazanç elde etmeye devam edebilirler. Bu dolandırıcılık şekli birtakım klasik dolandırırlık metotlarını da ihtiva ettiğinden diğer bilişim suçlarına göre farklılık göstermektedir. Saldırganların ileri teknoloji gerektiren metotları ve organize bir şekilde hareket etmeleri gerçek suçlulardan ziyade suça iştirak eden basit dolandırıcıların yakalanmasına olanak vermektedir.

### 2.5.11. Ortam dinlemesi ve cep telefonu güvenliği

Haberleşmenin Gizliliği Anayasa'nın 22'nci maddesi ile güvence altına alınmış olup, kişiler arasındaki haberleşmeye müdahale edilebilmesi ancak Anayasa'nın ilgili hükmü çerçevesinde, kanunla düzenlenen şartlarla ve yetkili mahkeme kararı ile mümkündür.

Bilgi Teknolojileri ve İletişim Kurumuna (BTİK) bağlı olarak faaliyet gösteren Telekomünikasyon İletişim Başkanlığı (TİB), telekomünikasyon yoluyla yapılan iletişimin tespiti, dinlenmesi, sinyal bilgilerinin değerlendirilmesi ve kayda alınmasından sorumludur. Ayrıca elde edilen verileri ve bilgileri ilgisine göre Millî İstihbarat Teşkilatı Müsteşarlığına, Emniyet Genel Müdürlüğüne ve Jandarma Genel Komutanlığına, talep etmeleri halinde mahkemeye ve Cumhuriyet Başsavcılıklarına iletmekle görevlidir[36].

Bu görev ve yetkilerin kanunlarla belirlenmesine karşın, yapılan cep ve uydu telefonu gibi mobil haberleşme vasıtalarıyla yapılan görüşmelerin ifşa edilip

haberleşme gizliliğine müdahale edilmesi günümüzün en önemli sorunlarından biridir.

Yasadışı yollarla elde edilen bu görüşmeleri ifşa etmek suçtur ve hukuka aykırı olarak elde edilmiş olan deliller, mahkeme tarafından bir vakıanın ispatında dikkate alınamaz[1].

Ortam dinlemesi ise konuşma yapılan yerde ses kayıt cihazları vasıtasıyla veya ileri teknoloji gerektiren lazerli dinleme ve yönlendirilmiş antenlerle olabilmektedir. Teknolojinin hızla ilerlemesi güvenlik ihlallerine ve bilgi güvenliğine büyük bir etki bırakmıştır. Bu etki ancak güvenlik prensiplerine tam ve kayıtsız bir şekilde uygulamakla bertaraf edilebilir. Ortam dinlemesi gizlilik dereceli bilgiye sahip olan devlet adamlarının en büyük paranoyası haline gelmiştir.

Mobil ve kablosuz teknolojiler kullanıcılara çok farklı hizmeti kolaylıkla sunarken, pek çok tehlikeyi de beraberinde getirmektedir. Bu da mobil ortam güvenliğini sağlamak için yüksek seviyede bir güvenlik altyapısı geliştirmeyi, çeşitli güvenlik politika ve stratejileri belirlemeyi ve uygulamayı zorunlu kılmaktadır[37].

Cep telefonu ve ortam dinlemelerinin kanun koyucu tarafından cezai müeyyideleri belirtilmesine rağmen, söz konusu suçu işlemeye yarayan casus yazılım ve donanımların satışı kolaylıkla yapılabilmektedir. Ayrıca cep telefonu operatörleri müşterilerinin yaş, cinsiyet ve alışveriş eğilimlerini müşterilerinin günlük konum bilgileri ile birleştirerek bu istatistikleri şirketlere satmaktadırlar.

### 2.5.12. Dijital aktivizm

Dijital aktivizm bireylerin sosyal medya ve internet aracılığıyla sosyal veya politik konularda kamuoyu oluşturarak eylemler tasarlayabilmek ve bu eylemlerle düşünce ve/veya siyaseti tasarlayabilmektir. Bu tanım ile masum bir amaca hizmet etse de otorite aleyhinde eylem yapmak, devleti yönetimini şeffaflaşmayı sağlamak için

[1] 6100 Sayılı Hukuk Muhakemeleri Kanunu madde 189

yasadışı yollarla devletin gizli bilgilerini ele geçirip internet ağları üzerinden yaymak suç oluşturmaktadır.

Sansürden uzak ve özgür bir iletişim ideal olarak kabul edilse de özel hayatının gizliliğini ihlal eden ve ülkenin milli güvenliği ile uluslararası platformda saygınlığını sarsacak olan her türlü eylem engellenmelidir.

Amerika Birleşik Devletleri'nde diplomatik belge sızıntısı olarak kabul edilen Wikileaks[1] olayı uzun süre dünya gündemini meşgul etmiştir. 25 Temmuz 2010'da Ocak 2004 ve Aralık 2009 tarihleri arasındaki Afganistan'daki savaşı anlatan 77 bin savaş günlüğü WikiLeaks.org tarafından açıklanmış ve birçok fikir ayrılığı ve tartışmaya yol açmıştır[38].Bu olay ülkelerin diplomatik yazışmalarına kadar da kolayca erişilip yayılabileceğini tüm dünyaya göstermiştir.Ayrıca sosyal medya Mısır, Tunus ve Libya gibi ülkelerde her türlü sansür ve engellemelere karşın internet üzerinden iletişimi sürdürmüş. Facebook[2] üzerinde oluşturulan gruplarla birleşen insanlar sokaklara dökülmüş ve bu ülkelerde çok da barışçıl olmayan metotlarda sergilenerek ülke yönetiminde değişikliklere gidilmiştir.

## 2.6. Bilişim Suçlarının İşlenme Şekilleri

### 2.6.1. Bilişim korsanlığı (Hacking)

Hack, izinsiz olarak sisteme girilerek sistemin işleyişini kontrol etme ve sistemdeki verilerden bilgi sahibi olma ve sistemin işleyişini durdurma ve/veya yönlendirmedir.

Bu izinsiz giriş genellikle işletim yazılımı yazan kişilerin gerektiğinde sistemi korumak amacıyla bıraktıkları arka kapıları bularak buradan sızma yoluyla gerçekleştirilir[39].Bilişim korsanı (hacker) olacak kadar bilgiye sahip kullanıcılar, bu bilgilerini en kısa zamanda paraya dönüştürmeye çalışmakta ve bunun içinde önceliğin isimlerini duyurmak olduklarına inanmaktadırlar.

---

[1]WikiLeaks 26 Temmuz 2010'da Amerikan ordusunun 2004-2009 yılları arasında Afganistan Savaşı'nda tutmuş olduğu 92.000 belgeyi The Guardian, The New York Times ve Der Spiegel gazeteleriyle birlikte açıklamıştır. Bireysel olayları da kapsayan günlükler, sivil kayıplar hakkında ayrıntılı bilgiler içermektedir. Belgeleri sızdıran er BradleyManning görev yaptığı Kuveyt'teki CampArfijan üssünde tutuklanmıştır

[2]Sosyal Paylaşım Platformu internet: http://www.facebook.com

Saldırı (hack) teknikleri konusunda yeterince bilgi sahibi olmayıp nasıl bilişim korsanlığı yapılacağını internet veya yazılı dokümanlardan öğrenerek saldırılarda bulunan kişilere de LAMER denir. Lamerlerin alt seviye programlama bilgisi olmayıp genellikle HTML kodlamasını öğrenip web sitelerine ve ya internet kullanıcılarına saldırıda bulunurlar. Web ve e-posta saldırıları dışında saldırı yöntemlerini kullanamazlar.

Phreaker (phonehacker) telefon ağları üzerinde çalışan, telefon sistemlerine saldırarak ücretsiz görüşme yapmaya çalışan kişilerdir. Geçmişte bu kişiler çeşitli elektronik devreler hazırlayarak telefon hattına özel sinyaller göndermekteydiler. Bunun ilk örneği 1971 yılında John T. Draper'in BlueBox (mavi kutu) adlı telefon şebekesine sinyal göndererek hattı aldatan sistemdi. Telefon ağlarının modernleşmesiyle birlikte phreakerlar VoIP servislerine ve GSM operatörlerine saldırmaya başlamışlardır.

Saldırıları 5 aşamada gerçekleştirilir. Birinci aşama saldırılacak sistem hakkında bilgi toplama aşamasıdır. Bu aşamada karşıdaki sistemin portları, işletim sistemi ve sistemde çalışan servisler gibi bilgiler incelenir. İkinci aşama sistemin taranmasıdır. Bu aşamada port tarayıcılar ile sistem taranarak sistemin ağ haritası oluşturulur. Bu aşamada sistemdeki açık saptanır. Üçüncü aşama erişimdir. Bu aşamada zararlı yazılımlar kullanarak hedefe erişim sağlanır. Dördüncü aşama bu erişimden yaralanma yani bilgi elde etme aşamasıdır. Bu aşamada saldırgan sistemdeki bilgiye erişebilir, kopyalayabilir ve silebilir. Sisteme tekrar erişebilmek için sisteme Truva Atı yerleştirebilir. Son aşama izini kaybettirme yani delilleri yok etme aşamasıdır. Bu aşama da saldırgan eriştiği sisteme bir daha erişebilmek ve suç unsurunu yok etmek maksadıyla sistemin kayıtlarında (log) değişiklik yaparak izini kaybetmeye çalışır.

### 2.6.2. Gizli kapılar (Trap doors)

Gizli kapılar işletim sistemleri ve ya çok işlevli kullanıcı sistemleri hazırlayan bilgisayar programcılarının bunları meydana getirirken ileride ortaya çıkabilecek durumlara göre sistem şifrelerinde, değişiklik yapabilmeyi veya yeni şifreler girebilmeyi sağlamak üzere sisteme bıraktıkları çeşitli giriş olanaklarıdır[6]. Gizli

kapılar işletim sistemi tamamlandığında ortadan kaldırılmazsa kötü niyetli kişiler tarafından tespit edilmesi halinde kullanıcıya ve sisteme ciddi zararlar verebilirler.

### 2.6.3. Truva atı

Truva atı, legal bir program içindeki illegal talimatlar ya da bir iş yapıyormuş gibi görünüp kullanıcıdan habersiz işlemler yapan bir programdır[39]. Kullanıcıdan habersiz arka planda işlem yapan bu programlar sistem internete bağlıyken dışarıya veri aktarımı yaparlar. Truva atları, virüs ve solucanlardan farklı olarak yayılmazlar.

Truva atları genellikle internetten indirilen müzik, dosya ve programlara iliştirilmiş olarak bilgisayarlarımıza yüklenmekte veya e-posta aracılığıyla kullanıcılara ulaşmaktadır.

Truva atı sunucu ve istemci kısmı olarak iki kısımdan oluşur. Sunucu kısmı hedefteki bilgisayar yukarıda bahsedilen şekilde yüklenmiş olan program, istemci kısmı ise bu yazılımı kullanarak hedefe erişen kullanıcın bilgisayarına kurulan karşı taraftaki bilgileri çekmeye ve hedef bilgisayara komut vermeye yarayan programdır.

### 2.6.4. Ağ solucanları ve virüs

Ağ solucanları, kullanıcının bilgisi olmadan ve komutsuz çalışabilen ve bir kopyasını iletişim vasıtalarını kullanıp diğer sisteme yayarak çoğalabilen yazılımlardır. Sisteme yüklenen ağ solucanı virüs gibi sisteme zarar verebileceği gibi Truva Atı bırakarak da sisteme zarar verebilir. Solucanların temel çalışma prensibi kendilerini kopyalayarak çoğalmak olduğundan kısa süre içerisinde çok sayıda sisteme yayılarak ağları ve bilgisayarları kullanılmaz hale getirirler. Solucanlar sistemin bellek veya ağ bant genişliklerini tükettiklerinden ağ / bilgisayar kullanılmaz hele gelir ve çöker.

Ağ solucanları güvenlik duvarlarını geçip sisteme sızarak sisteme zarar verebilirler. Ağ solucanlarının en büyük özellikleri yazılımdan yazılıma, dosyadan dosyaya, sistemden sisteme kolaylıkla kopyalanabilmeleridir. Bu kopyalama işlemine “virüs bulaşması” da denilmektedir[40].

Bilgisayar virüsü kullanıcısının izni ya da bilgisi dâhilinde olmadan bilgisayarın çalışma şeklini değiştiren ve kendini dosyaların içinde gizlemeye çalışan aslında bir tür bilgisayar programıdır. Virüs terimi kötücül yazılım (malware) denilen geniş bir alanı ifade etmek için kullanılsa da gerçek bir virüs kendini çoğaltmalı ve kendini çalıştırmalıdır.

Bilişim virüsleri özellikle internet vasıtasıyla çok hızlı yayılmaktadır. 2001 yılında Filipinli bir öğrenci tarafından yazılan LoveBug isimli virüs, yayılmaya başladıktan 18 saat içinde 100 milyon bilgisayara bulaşmıştır[41].

2011 yılı Nisan ayında gerçekleştirilen TUİK'in Hane Halkı Bilişim Teknolojileri Kullanım Araştırması sonuçlarına göre Türkiye genelinde hanelerin %42,9'u İnternet erişim imkânına sahiptir[42]. İnternetin bu kadar yaygın olması her yaş ve kesimden insanın kolaylıkla erişebilmesi, eğer güvenlik önlemleri almazlarsa zararlı yazılımlara (malicious code) maruz kalabilecekleri anlamına gelmektedir.

Symantec şirketinin 2010 yılı internet tehditleri raporuna göre Truva atı, solucan ve virüslerin %49'u yetişkinlere yönelik eğlence sitelerinden yayılmaktadır[43]. Ağ solucanları ve virüslerin bulaştıkları sistemler virüs temizleme ve koruma yazılımları ile temizlenmelidir, aksi halde dosyalar silinse dahi virüsler sistemde kalmaya devam ederler.

### 2.6.5. İstem dışı elektronik postalar (Spam)

İnternet üzerinde aynı mesajın yüksek sayıdaki kopyasının, bu tip bir mesajı alma talebinde bulunmamış kişilere, zorlayıcı nitelikte gönderilmesi spam olarak adlandırılır. Spam çoğunlukla ticari reklam niteliğinde olup, bu reklamlar sıklıkla güvenilmeyen ürünlerin, çabuk zengin olma kampanyalarının, yarı yasal servislerin duyurulması amacına yöneliktir. Internet kullanıcıları üzerindeki etkileri incelendiğinde iki tip spam vardır. E-posta aracılığıyla gönderilen spam doğrudan gönderilen mesajlarla bireysel kullanıcıları hedef alır. E-posta spam listeleri genellikle

Google[1] sayfalarının taranması, tartışma gruplarının üye listelerinin çalınması veya web üzerinden adres aramalarıyla oluşturulur.

İkinci spam türü ise, içeriğinin mutlaka ticari olması gerekmeyen UBE (Unsolicited Bulk e-mail - Talep Edilmemiş Kitlesel e-posta), aynı anda yüz binlerce e-posta hesabına gönderilen e-posta iletileridir. Bu iletiler ticari içerikli olabileceği gibi politik bir görüşün propagandasını yapmak ya da bir konu hakkında kamuoyu oluşturmak amacı ile gönderilen e-posta iletileri de olabilir.

2007 Aralık ayında Barracuda Network isimli internet üzerinden mail ve web güvenliği üzerine faaliyet gösteren firmanın yayımlamış olduğu rapora göre; analiz kapsamında 50000'den fazla kullanıcıya gönderilen bir milyardan fazla elektronik posta incelenmiştir. Raporda 2007 yılında internet üzerinden gönderilen tüm e-postaların yaklaşık %95'inin reklam amacı taşıyan ve istenmeyen elektronik posta olduğu açıklanmıştır. Raporda ayrıca spam e-postaların 2006 yılında yapılan tahminlere oranla daha fazla gerçekleştiği de ifade edilmiştir[44].

İstenmeyen e-postalardan uzak durmanın en iyi yolu e-posta filtresi kullanmaktır. Filtreler, istenmeyen mesajları kullanıcıları ulaştırmadan doğrudan mesajları siler veya yığın posta kutusuna gönderirler.

### 2.6.6. Mantık bombaları

Mantık bombaları, bilişim sistemlerinde veya ağlarında, daha önceden belirlenmiş özel durumların gerçekleşmesi durumunda zarar verici sonuçlar yaratan programlardır.

Mantık bombaları aktif durumda değilken Truva Atı gibi davranır. Fakat aktif hale gelince sisteme zararlı etki bırakır. Her yıl 26 Nisan tarihinde aktif olan Chernobil virüsü (win95.CIH) mantık bombalarının en ünlüsüdür.

Mantık bombası gibi hareket edip sistemde kendisini kopyalayarak kolonileşen ve bilişim sistemine gereksiz komutlar vererek yavaşlatan saldırı türüne de tavşan denir.

[1] Google: arama motoru

Tavşanlara örnek olarak büyük bir şirketten atıldığı için sinirlenen bir programcı giderken şirketin bilgisayarına 400 Byte'lık, tek işlevi kendinin bir kopyasını yapmak olan "Sarmaşık" adında bir program bırakır. Program işten çıkarılan programcının işten çıkmasından 24 saat sonra aktif olur. 20 gün sonra şirket bilgisayarı işlev yapamaz hale gelir. Çünkü sistemin belleği 16384 kopya almış ve sistemde 6,5 milyon Byte'lık bir çöplük bırakmıştır[45].

### 2.6.7. Phishing (Password hacking- şifre saldırısı)

Phishing, sosyal mühendislik teknikleri kullanılarak, kurbanın şifreleri, banka hesap numaraları, kredi kartı bilgileri gibi özel ve yüksek güvenlik isteyen bilgilerini, kurbanı aldatarak elde etme yöntemi olarak tanımlanabilir. Phishing kelimesi İngilizce fishing (balık tutma) kelimesinden türetilmiş bir kelimedir. Bu anlamda kurbanlara phish (fish–balık) denilmektedir.

Bu yöntemde dolandırıcı hazırlamış olduğu e-postaları elinde hazır bulunan posta listelerine spam olarak yollar.

Bu postalarda banka/finans kuruluşunun sisteminde güncelleme yapılmakta olduğu ve sistemde eksik bilgilerin tamamlanması isteği belirtilir ve altına dolandırıcının daha önceden hazırladığı sitenin adresi belirli gizleme yöntemleri ile kurban aldatılacak şekilde konulur. Bu e-postaya inanan kullanıcı kendi elleri ile dolandırıcıya önemli kişisel bilgilerini verir. Bundan sonra, dolandırıcıya sadece gelen bilgileri toplayıp bu bilgilerle maddi çıkar sağlamak kalmaktadır. En yalın anlatımıyla bu şekilde işleyen Phishing sistemi son birkaç yılda çok geniş bir kitleyi etkilemekte ve her geçen gün kendisini geliştirip yenilemektedir.

Sahte web siteleri oluşturarak da phishing saldırı yapılabilir. (Bknz. Resim 2.1.) Bu sitelere kredi kartı bilgilerini hiç tereddüt etmeden veren kurbanlar suçluların tuzağına düşmektedir.


Resim 2.1. Sahte kredi kartı borç sorgulama sitesi

Kısaca Phishing tekniği bir tür sosyal mühendislik tekniği olarak insanların kavramadaki yanılmalarından ve algısal zaaflarından faydalanarak insanlardan çıkar sağlamak olarak tanımlanabilir.

### 2.6.8. Sniffer (Koklayıcı)

Sniffer koklayıcı anlamına gelen bir kelimedir. Yerel ağdan geçen paketlerin kopyalanması ile şifrelenmemiş olarak geçen bilgilerin elde edilmesinde kullanılırlar. Eğer ağda bir sniffer varsa web sayfası üzerinden şifre girişi yapıldıysa şifrenin saldırganın eline geçmesi çok kolaydır.

### 2.6.9. Tuş kaydediciler (Keylogger)

Keyloger internet üzerinde resim veya programların içerisine saklanarak kullanıcı bilgisayarına kullanıcının bilgisi dışında yüklenen programlardır. Program kullanıcının bilgisayarında aktif hale geldiği andan itibaren klavye ile yazılan bütün bilgiler ve hatta fare ile tıklanan bölgelerin resimleri kaydedilerek rapor haline getirilir ve bu rapor bahse konu zararlı yazılımı derleyen veya yazan kişilere internet aracılığı ile gönderilir. Bu sayede söz konusu yazılımı kullanıcının bilgisayarlarına bulaştırmak üzere yayan kişiler kullanıcının bilgisayarından yapılan bütün e-posta, bankacılık ve finans şifrelerini ele geçirebilmektedirler.

Kullanıcının bilgisi olmadan Android işletim sistemini kullanan mobil platformlarda fabrikasyon ayarlarında yüklü olarak son kullanıcıya sunulan bir keylogger benzeri programı olduğu bilinmektedir. Bu program kullanıcıdan habersiz SMS, e-posta içeriklerini, basılan tuşları ve konum bilgisini kaydetmektedir. Cep telefonu üreticileri CarrierIQ adı verilen bu uygulamasının sadece konuşma süresi, ses ve sinyal kalitesi gibi verilerin toplanması için varsayılan olarak yüklendiğini belirtseler de CarrierIQ, basılan her tuşu, girilen her internet sitesini, atılan her mesajı kaydetmektedir.

### 2.6.10. ARP (Adres çözümleme protokolü) zehirleme

Saldırgan sistemin yerel ağda istediği şekilde yayın yapmasına ARP (Address Resolution Protocole- Adres Çözümleme Protokolü) zehirleme denir. Örneğin sistemleri yanıltarak modemden geçmesi gereken yerel ağ trafiğini kendi sisteminden geçirerek ağdaki veri trafiğini kontrol eder. Bu saldırı metodunun diğer adı Man In The Middle (aradaki adam) saldırısıdır.

### 2.6.11. DNS (Alan adı sunucusu) aldatmacası

Hedef bilgisayarın DNS sorgularının cevabı değiştirilerek istenilen sahte bir adrese yönlendirme yapılabilir. Bu saldırı yöntemi ARP zehirleme ile birlikte kullanılır.

### 2.6.12. DoS ( Hizmet engelleme saldırısı) saldırısı

Sistemleri çalışamaz hale getirmek için yapılan saldırı tipidir. DDOS (Distrubuted Denial of Service ) ise DOS saldırısının yüzlerce, binlerce farklı sistemden yapılması şeklinde gerçekleşir. Genellikle taklit edilmiş (spoof) edilmiş IP adresleri ve köle bilgisayarlar kullanılır. Sistemde güvenlik açığı bulunamazsa zarar verme amaçlı politik sebeplerden ve ticari sebeplerle yapılabilir.

### 2.6.13. XSS ve XSRF

XSS (Cross Site Scripting) , HTML kodlarının arasına istemci tabanlı kod gömülmesi yoluyla kullanıcının tarayıcısında istenen istemci tabanlı kodun çalıştırılabilmesidir. Genelde XSS açıkları, saldırganın sistemi deneme yanılma yaparak bulması ile ortaya çıkmaktadır. Açığın bulunması ile saldırgan, başka bir alan adından, açığın bulunduğu alan adı ve sayfanın bilgilerini, oturum ayrıntılarını ve diğer nesne değerlerini çalabilmektedir.

XSRF(Cross-Site Request Forgery)'nin saldırganın, bir web sitesine, sitenin güvendiği bir kullanıcıdan yetkisiz komutlar göndermesidir. Bu tip saldırılara genelde "session riding" veya "hostile linking" saldırıları adı verilir. XSRF saldırı için web tarayıcısını kullanır ve kullanıcının yeni kullanmış olduğu varsayılan bir siteye bağlantı kuran bir kod dizini (script) veya bağlantı (link) içerir. Sonrasında kod dizini görünüşte yetkili fakat kötü amaçlı işlemleri kullanıcı adına gerçekleştirir.

### 2.6.14. İnternet bankacılığı dolandırıcılığı

İnternet bankacılığında kullanılan kullanıcı kodu ve şifrelerin bilgisayar korsanları tarafından zararlı programlar vasıtasıyla ele geçirilerek hesaplardaki paranın ele geçirilmesidir.

Bilgisayar korsanının banka müşterilerine ait internet banka hesap bilgilerini casus yazılımlar kullanarak ele geçirir ve bu hesapları örgüt elemanları adına açılan veya çeşitli yollarla elde ettikleri hesaplara havale/eft yaparak boşaltma yoluna giderler.

### 2.6.15. Kredi ve banka kartlarını sahteciliği

2011 rakamlarıyla 47 milyon kredi ve banka kartı kullanıcısı olduğundan günümüzde bu dolandırıcılığın rakamsal boyutu gittikçe yükselmektedir.

Suçlular kart kopyalamasını birtakım tekniklerle yaparlar. Döviz büroları ve lokantalar başta olmak üzere çeşitli işyerlerinde özellikle turistlere ait kredi kartlarını kart kopyalama cihazları kullanarak kopyalarlar.

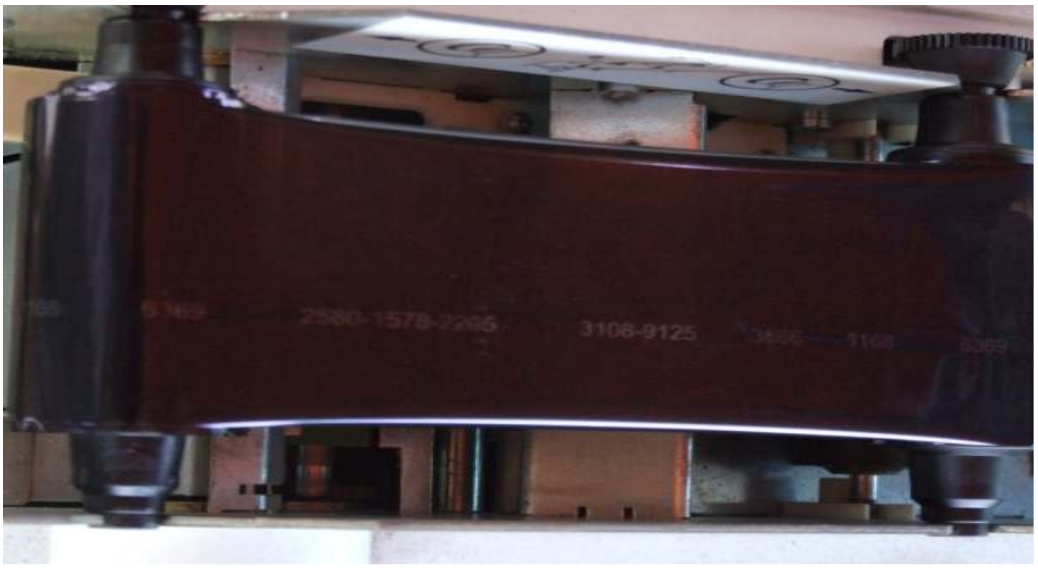
Resim 2.2. Kart kopyalama cihazı

Resim 2.3.a. ATM kart kopyalama düzeneği- üst panel

Aynı yolla yurt dışında faaliyet gösteren dolandırıcıların elde ettikleri kart bilgilerini internet ortamında satın alarak da sahte kart oluşturabilirler. ATM'lerin ön paneline yerleştirdikleri kart kopyalama düzeneği ile işlem yapan müşterilerin kart bilgilerini kopyalayabilirler.


Resim 2.3.b. ATM kart kopyalama düzeneği- tuş takımı

Elde ettikleri kart bilgilerini kart kodlama, renkli kart baskı, kabartma baskı ve hologram baskı cihazları kullanarak, oluşturdukları sahte kartların manyetik şeritlerine kodlarlar.




Resim 2.4. Kart baskı cihazı


Resim 2.5. Dijital baskı makinesi

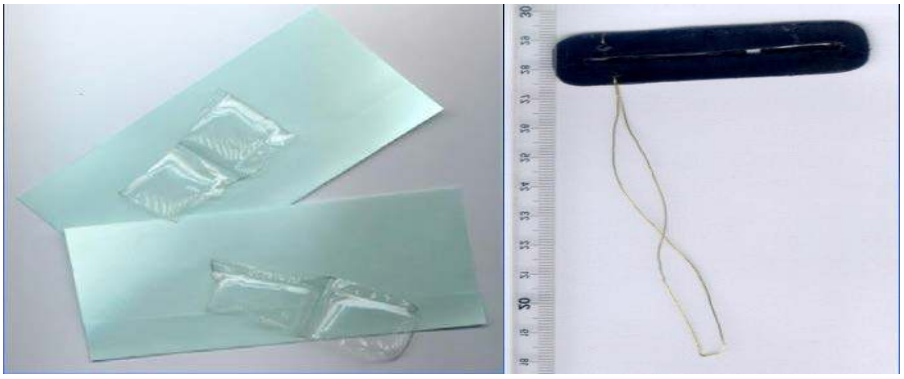
Resim 2.6. Kabartma baskı makinası

Sahte olarak oluşturdukları kartları özellikle kuyumcularda, petrol istasyonlarında, elektronik malzeme satan büyük mağazalarda kullanarak, haksız kazanç elde ederler. Çip uygulaması sayesinde dolandırıcılar artık eskisi gibi kolay olarak kartları kullanamadıklarından hem kartı kopyalamaya hem de şifreyi öğrenme metodunu izlemektedirler.


Resim 2.7. Sahte kartlar

Saldırganlar ATM'lere yerleştirdikleri düzeneklerle kredi kartınızı bankamatiğe sıkıştırmakta bu esnada sahte olarak düzeneğini hazırladıkları ve ATM'nin yanına yerleştirdikleri müşteri hizmetleri hattı ile kart kullanıcısının şifresini öğrenerek kazanç elde etmektedirler.

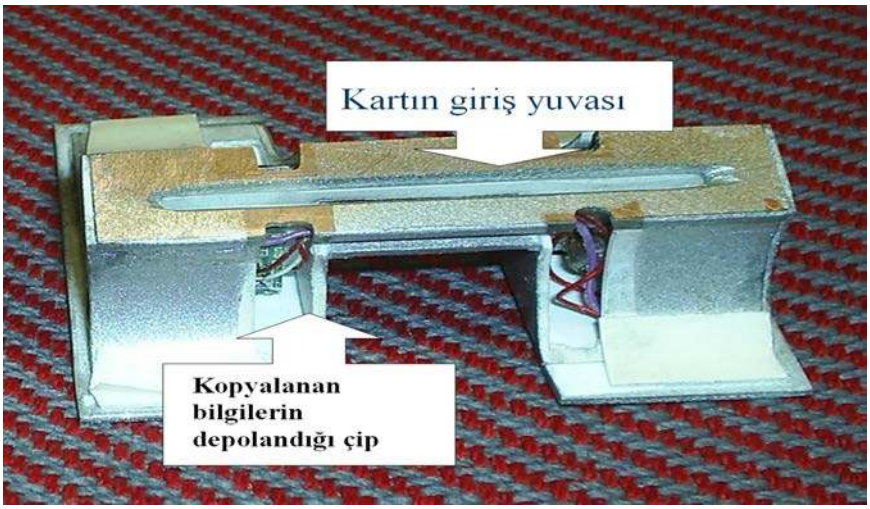
Resim 2.8. Sahte müşteri hizmetleri hattı



Resim 2.9. Kart sıkıştırma aparatları

Ayrıca saldırganlar ATM'lere yerleştirdikleri kameralarla kullanıcının bastığı tuşları görerek şifre bilgilerini öğrenmekte, bu esnada ATM'nin kart yerleştirme yuvasına taktıkları kart kopyalama cihazı ile kart bilgilerini elde etmektedirler. ATM'leri termal kameralarla görüntüleyip, çekilen fotoğraflarda en son hangi tuşlara basıldığı rahatlıkla görülebilmektedir[46]. Hatta termal izin boyutuna bağlı olarak tuşların basılma sırası dahi anlaşılır. Kısacası siz ATM'den ayrıldıktan sonra plastik tuş takımları üzerine bıraktığınız izle şifreniz öğrenilebilinir. Bu bilgiyle yukarıda

bahsedilen kart kopyalama teknikleri kart basıp elde ettikleri şifre ile kazanç elde etmektedirler.



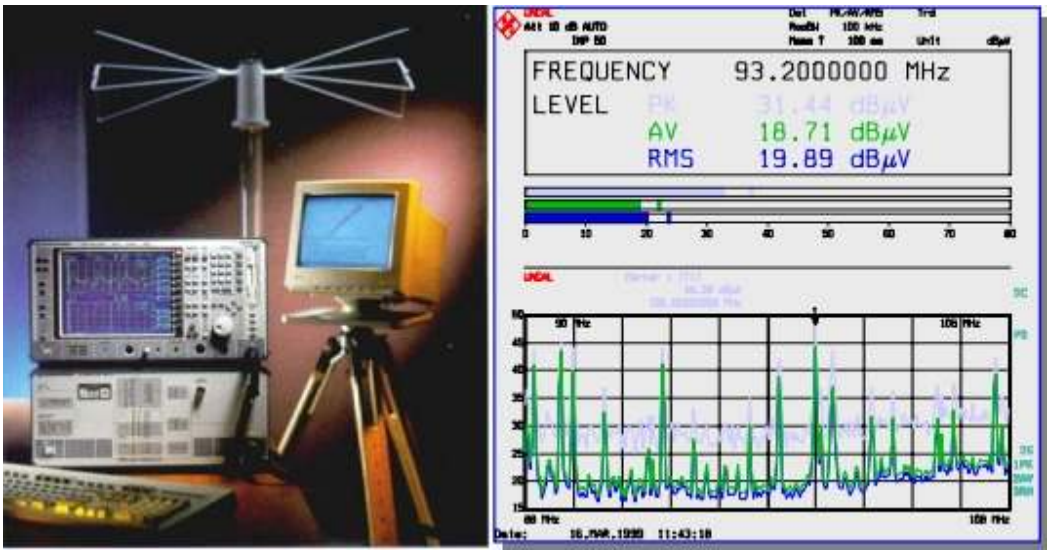

Resim 2.10.a. Kart kopyalama düzeneği

Resim 2.10.b. Kart kopyalama düzeneği giriş yuvası


Resim 2.11. ATM şifre görüntüleme düzeneği

### 2.6.16. TEMPEST (Transient electro magnetic pulse emanation standard)

İstem dışı yayılımın kaydedilerek veri analizi yapılmasına imkân veren istihbarat şeklidir. TEMPEST standartlarının tümü gizlidir. TEMPEST bilgi/veri istihbaratına en yaygın örnek bir bilgisayar ekranından yayılan istem dışı elektromanyetik dalgaların yüzlerce metre öteden kaydedilerek analizidir. Örneğin, bir çalışma odasındaki bilgisayar kullanıcısının bastığı her tuş bina dışında, karşı apartmanda bulunan bir TEMPEST alıcısının ekranında görüntülenebilir. Elektromanyetik sızıntıdan bilgi üretileceği için, geniş bantlı, hassas ve dinamik sınırı yüksek alıcı bir anten ile buna bağlı bir EMI (elektromanyetik girişim) cihazı ve TEMPEST amaçlarına uygun ilave devre ve cihazlarla elektromanyetik dinleme gerçekleşebilmektedir[47].




Resim 2.12.a. TEMPEST alıcısı ve kaydedilen işaret örneği[47].

TUBİTAK, NATO AMSG 720B standardına göre gizli bilgilerin işlenebileceği bilgisayarlar geliştirmektedir. Gizlilik dereceli bilgi işlerken doğru cihaz kullanılması büyük önem taşımaktadır. Cihazlar çalışırken, gizlilik dereceli bilgiler kullanıcı farkında olmadan elektromanyetik yollarla istenmeyen kişiler tarafından uzaktan ele geçirilebilir. TEMPEST standartları bu tehdidin ortadan kaldırılmasına yönelik olarak, doğru cihazın doğru bölgede kullanılmasını gerektirir.

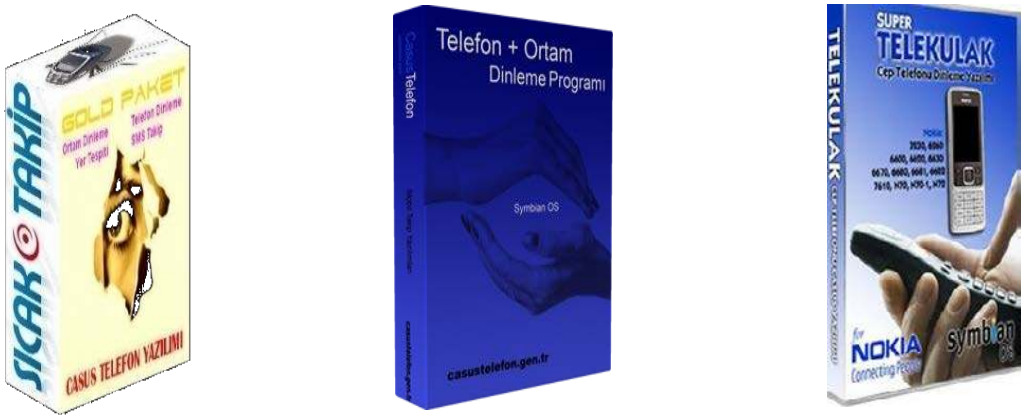
Resim 2.12.b. TUBİTAK TEMPEST PC

### 2.6.17. Cep telefonu casus yazılımları

Cep telefonları günümüzde minik bir bilgisayara dönüşmesi ve artık pek çok fonksiyonu üzerinde barındıran işletim sistemi ve uygulamalardan oluşması nedeniyle, kötü amaçla kullanılan bazı yazılımlar ile iletişimin gizliliğinin ihlal edilmesi mümkün olmuştur. Cep telefonlarında Internet üzerinden satın alınacak veya indirilecek bazı kötü amaçlı yazılımlar ile aşağıdaki işlemleri yapmak mümkün olmaktadır:

**Ortam Dinleme:** Hedef telefonun numarasını çevirerek, bulunduğu ortam istendiği zaman dinlenebilir. Akıllı yazılım sayesinde, hedef telefon sadece belirtilen numaranızdan arandığında zil sesi, titreşim ve benzeri herhangi bir uyarı olmadan açılır ve böylece hedef kişi fark etmeden istendiği kadar dinlenebilir.

**Telefon Dinleme:** Hedef telefonda bir görüşme başladığı zaman, anında tanımlanan cep telefonuna bu görüşmeyi bildiren bir SMS gelir. Gelen SMS de hedef kişinin görüştüğü numara belirtilir. Ayrıca aranan mı yoksa arayan mı olduğu da bildirilir. Bu SMS alındıktan sonra, görüşmeyi dinlemek için hedef telefonun numarasını aramak yeterlidir. Anında araya girerek görüşmeyi dinlemek mümkündür.




Resim 2.13. Casus yazılımlar

**Mesaj Bildirimi:** Hedef telefona bir mesaj geldiğinde veya hedef telefondan bir mesaj gönderildiğinde, bu mesajın aynısı gerçek zamanlı olarak tanımlı telefon numarasına da gelir.

**Arama Bildirim:** Hedef telefona bir arama geldiğinde veya hedef telefon arama yaptığında, hangi numara ile görüşüldüğünü bildiren bir mesaj gelir.

**SIM Bilgisi:** Hedef telefona başka bir SIM kart takıldığında, bu değişiklik anında bir SMS ile bildirilir.

**Yer Bilgisi:** Hedef telefona, tanımlı telefondan bir komut göndererek, nerede olduğunu bildirmesini isteyebilirsiniz.

Normal bir telefona kötü amaçlı yazılım kurarak iletişim bilgilerini almak mümkün olduğu gibi, bu amaca uygun hale getirilmiş telefonları alarak da bu işlem yapılabilir. Yine telefonun üzerine kurulan casus yazılımlar ile sadece bu işlemler için özel olarak satılan cep telefonları mevcuttur. Bu telefonlar genellikle resmi satış noktaları dışında 'Merdiven Altı' şeklinde tabir edilen bölgelerde veya Internet kanalı ile satılmaktadır.

Bu telefonların çalışma şekli mevcutta var olan telefon komutlarının yüklenen yazılım ile değiştirilmesi sonucu oluşmaktadır. Telefona gönderilen komutlar veya tanımlanan özel numaradan gelen aramalarda casus işlevi görmesi sağlanmaktadır. Örneğin casus telefon onu kumanda eden telefon tarafından aradığında pasif dinleme özelliği hemen aktif olup ortamdaki tüm sesler dinlenebilmektedir. Benzer şekilde arama yapıp (#*) tuşlarına basıldığında ise mevcutta yapılan konuşmaya paralel olarak girilebilmektedir.

### 2.6.18. Gizlice dinleme

Kablosuz dinleme cihazları bulundukları ortamdaki sesleri toplayarak sinyaller üzerinden sınırlı bir mesafedeki tanımlı alıcısına ulaştırmaktadır. Alıcı üzerinden de konuşmalar dinlenebilmektedir. Bu tür tehditler ile karşı karşıya olan firmalar düzenli olarak dinleme cihazı araması yaparak böyle bir durum ile karşı karşıya kalmayı önlemeye çalışmaktadırlar.

Özellikle sık ziyaretçi alan ve dinlenmesi durumunda rakiplerin veya ilgili başka kurumların eline önemli bilgiler verebilecek olan kişi veya grupların bu konuda

dikkatli olması gerekmektedir. Bu cihazlar oldukça küçük olduğundan gözle fark edilmesi çok zordur. Bazen tek başına cihaz olarak değil, bir süs eşyası veya bir hediyenin parçası olarak da konumlandırılabilir.

Dinleme cihazlarının en büyük dezavantajı yakın bir mesafe (sinyal görüş açısına ve gücüne bağlı olarak 0-100 m.) üzerinden dinleme faaliyetinin gerçekleştirilebilmesidir. Parabolik antenli uzaktan ses alma cihazları ile yaklaşık 100 metre uzaklıktaki insan sesi ve bu aralıktaki frekansları duymanızı sağlar. Ortamın ve konuşan kişinin yüzünü döndüğü yöne bağlı olarak konuşma net veya gürültülü olarak dinlenebilir. Daha uzak mesafelerde dinleme ise amplifikatör aynı kalmak kaydıyla sadece parabolik anten değiştirilerek sağlanabilir.300 metreye kadar 60 cm parabolik antenle bu dinleme sağlanır. Stereo kulaklıklar vasıtasıyla ortam gürültülerinden etkilenmeden istemiş oluğunuz bir ses şiddetinde dinleme yapılabilir. Dinleme esnasında, standart herhangi bir kaydediciye kayıt da yapılabilir. Fakat mesafe arttıkça dinleme imkânsız hale gelir. Bu nedenle mesafe sorunu cep telefonları ile çözülmüştür. Bugün casus cep telefonları olarak bilinen cihazlar aslında birer dinleme cihazıdır. En önemli avantajları ise mesafe sınırı olmaksızın dinleme yapılabilmesini sağlamalarıdır. Fakat cihazın normal bir dinleme cihazı gibi bir alana bırakılması durumunda pili biteceğinden dinleyeceğiniz kişiye bu cihazı vermeniz durumunda düzenli olarak şarj edileceğinden ve sürekli yanında olacağından bu kişiyi dinlemek mümkün olacaktır.

Resim 2.14. Parabolik antenli dinleme aleti

Bir diğer yaratıcı dinleme cihazı ise hem enerji problemini hem de mesafe problemini çözen casus GSM uzatmalı prizdir. Oldukça zekice hazırlanmış, şüphe uyandırmadan, evinize veya ofisinize yerleştirebilecek olan bir dinleme cihazıdır. GSM vericisi sayesinde kesinlikle mesafe sınırı yoktur. Dünyanın neresinde olursanız olun, sadece uzatmalı prize yerleştirilmiş cihazın içindeki numarayı cep telefonunuzdan arayarak, Türkiye′deki evinizi veya işyerinizi dinleyebilirsiniz. Bu cihazı etkin kılan diğer bir özelliği ise vericiyi çalıştırmak için gereken enerjiyi prizin takılı olduğu elektrik hattından almasıdır. Aynı şekilde bilgisayardan enerjisini alan içine SIM kart yerleştirilen fare ile de ortam dinlemesi yapılabilir.

Resim 2.15. Ortam dinleme aletleri

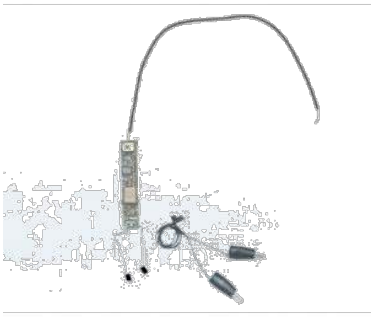
GSM Intercept A5.41 ChatterGuard adlı cihaz ile belli bir zaman içinde sadece numarası verilen tek bir cep telefonunu dinlenebilir. En büyük özelliği ise bazı anahtar sözcükleri tanıyabilmesidir. Zanlı bir telefon konuşmasında ne zaman anahtar sözcükleri kullansa, cihaz devreye girer ve konuşma aynen hafızaya kaydedilir. GSM Intercept cihazı GSM A5.1 kriptolama algoritmasını kırarak gerçek zamanlı dinleme imkânı verir.


Resim 2.16. GSM Intercept A5.41 Chatter Guard

Kızılötesi Uzaktan Dinleme sistemi ise Lazer ışınını dinlenmek istenen binanın penceresine doğrultur. Işın, içerideki konuşmanın yaydığı ses dalgalarının camda yaptığı titreşimleri algılayarak ikinci bir ışınla geriye gönderir. Cihaz, lazerle geri gelen ses dalgalarını deşifre ederek ses sinyallerine çevirir ve konuşmaları kaydeder.

Resim 2.17. Kızılötesi uzaktan dinleme sistemi

Paralel Telefon Vericisi adı verilen cihaz, sabit telefonların ahizelerine veya telefon kablolarına takılır. Sabit hatlardaki konuşmaları radyo dalgaları ile dinleme yapan kişinin yanındaki alıcıya iletir. Pilsiz çalışan cihaz, enerjisini telefon kablolarındaki elektrik akımından elde eder.



Resim 2.18. Paralel telefon vericisi

Ayrıca küçük bir radyo vericisinden oluşan ve algıladığı sesleri anında radyo alıcısına gönderen böcek diye tabir edilen cihazlar da mevcuttur. Böcekler ortamda insanların dikkatlerini çekmeyecek objeler üzerine monte edilirler. Böcekler saat, tablo, masa lambası, koltuk gibi eşyalara monte edilebilirler. Verici tespit cihazları ile istenilen mekânda böcek araması yapma mümkündür.

Resim 2.19. Verici tespit cihazı

## 2.7. Bilişim Suçları Konusunda Yapılan Çalışmalar ve Kaynak Araştırması

Bilişim suçları ile ilgili olarak özellikle hukukçular tarafından suçun unsurlarını ve çeşitleri ile bilişim suçlarının ceza hukukundaki yerini inceleyen tez çalışmaları yapılmıştır. Türk Ceza Hukuku`nda bilişim suçları konulu doktora teziyle Muammer KETİZMEN[48] bilgi toplumunun ortaya çıkardığı sosyoekonomik değişimin bilişim alanında yaptığı etkilerini ceza hukuku bakımından incelemiştir. Ayrıca ceza kanununda belirtilen suçların mevcut hukuki ihlal şekillerinin bilişim sistemleri

aracılığıyla işlenmesi durumunda ortaya çıkabilecek yeni ihlal şekillerini açıklamıştır. Mevcut suçlar ile yeni suçlar arasındaki kapsam sorununa değinmiştir.

Türk Ceza Hukuku`nda Bilişim Suçları yüksek lisans tezinde Murat Volkan DÜLGER[14], Yeni Türk Ceza Kanunu'nda yer alan bilişim suçları ile ilgili düzenlemeleri ve ilgili kanun maddelerini açıklamıştır. DÜLGER'e göre banka veya kredi kartlarının kötüye kullanılması suçu, koruduğu hukuksal değere göre malvarlığına karşı suçlar bölümünde yer alması gerekirken bu yapılmayarak bilişim sistemlerine karşı suçlar bölümünde düzenlenmektir. Bu durumun düzeltilmesi ve suç tipine ilgili olduğu bölümde yer verilmesi gerekmektedir.

"Bilişim Suçları ve Türk Hukuk Sistemindeki Yeri" konulu yüksek lisans teziyle Halil İbrahim DİLEK[49], bilişim suçlarının sadece ceza hukuku yönünü ele almış ve suçları teknik açıdan incelemiştir. Teknik açıdan bu suçların delillendirilmesinin ayrıntılı olması sebebiyle bu konuda yetişmiş personel ihtiyacına dikkat çekmiştir.

"Yeni Türk Ceza Kanunu Kapsamında Bilişim Suçları ve Emniyet Genel Müdürlüğü Uygulamaları" konulu yüksek lisans teziyle Necmi Murat GÜNGÖR, bilgisayar suçları ve bu suçlar ile mücadele için görevli bulunan Emniyet Teşkilatının durumu irdelemiştir. Bunun yanında Emniyet Genel Müdürlüğü için bilişim suçları ile mücadeleye yönelik olarak öneriler getirilmiş ve idari yapılanmanın nasıl olması gerektiği konusunda personel, eğitim ve benzeri çeşitli unsurlarda göz önünde bulundurularak bu öneriler içerisinde incelenmiştir. Güngör'e göre Emniyet Genel Müdürlüğü altında Bilişim Suçları ile Mücadele Daire Başkanlığı kurulmalıdır. Bu sayede taşra teşkilatlarında yani illerimizde bu dairenin karşılığı olarak Bilişim Suçları Şube Müdürlükleri oluşturulmalıdır[50].

"Türk Bankacılık Sisteminde İnternet Bankacılığı İle Yapılan Dolandırıcılıklar ve Bilişim Suçları Hukuku" konulu yüksek lisans teziyle Seher ERGÜÇ, Elektronik bankacılık işlemlerini gerçekleştiren kimselerin maruz kalabilecekleri riskten kaynaklanan yükümlülük ve sorumlulukların, tarafların (banka ve müşteri) menfaatlerine aykırı düşmeden belirlenmesi ve paylaştırılması konusuna değinmiştir. ERGÜÇ'e göre sistemden kaynaklanan eksiklik ve aksaklık sebebiyle oluşan

zararlara banka katlanmalıdır. Kullanıcının hatasından kaynaklanan zararlara ise sistemi kullanan banka müşterisi katlanmalıdır[51].

“5237 Sayılı Türk Ceza Kanununda Bilişim Sistemine Girme, Sistemi Engelleme ve Bozma Suçları” konulu yüksek lisans teziyle Mehmet Burak KIZILTAN[52],konuyla ilgili teknik kavramlar, tarihi gelişim ve Yargıtay kararlarına yer vermiş ve diğer ülkelerin hukuk sistemlerindeki düzenlemelere değinmiştir.

“Ülkemizde Bilişim Suçları ve İnternetin Suça Etkisi” konulu teziyle Bahaddin ALACA konuyu antropolojik ve hukuki boyutlarıyla incelemiştir. ALACA’ya göre bilişim sektörünün gelişmesiyle aile yapısı bozulmuş ve yüksek gelir grubuna sahip olan bireylerin teknolojik yararlardan daha fazla oranda pay alması sebebiyle toplumda eşitlik ilkesine aykırı bir durumun oluşmuştur. İnternet üzerinden birçok bilimsel eser, makale ve konferans notlarına ulaşabilme imkânının sunulması ile kişilerin küresel düzeyde mukayeseli bilgi edinerek kendilerini geliştirmelerinin yolu açılmıştır[53].

“Bilişim Suçları İle Mücadele” konulu teziyle İsmail TULUM bilişim suçlarının uluslararası platformda ele alınması gerekliliğine değinmiş; işlenen suçun, suçun işlendiği mahal ve uygulanacak hukuk sorunu gündeme getirmiştir.

İsmail TULUM (2006) şöyle demektedir[54].

“Örneğin on ayrı ülkede işlenmiş bir internet suçu hangi ülke hukukuna göre yargılanacaktır. Ya da işlenen fiil bazı ülke kanunlarına göre suç olurken kimilerinde de suç kabul edilmeyebilir. Dolayısıyla siber suçlarla mücadelede, uluslararası iş birliği son derece önemlidir.”

“Bilişim Suçlarının Sosyo-Kültürel Seviyelere Göre Algı Analizi” konulu teziyle Çığır İLBAŞ[55] Türkiye ve 17 farklı ülkenin bilişim suçları mevzuatlarını incelemiş. Teknoloji, bilgisayar ve İnternet konularına yönelik ilginin ölçülmesi ve beraberinde katılımcının İnternet kullanım profilinin belirlenmesi hakkında üniversite öğrencilerine yönelik olarak algı analizi çalışması yapmıştır.

“Türkiye’de Eğitimli İnsanların Bilişim Suçlarına Yaklaşımı” konulu teziyle Hikmet DiJLE[56] yaptığı anket ile eğitimli insanların bilişim suçlarına bakışını incelemiş lisanssız yazılım kullanma ve internetten illegal film, müzik ve oyun indirmenin katılımcılar tarafından bilişim suçu oluşturduğunu bilmediklerini ortaya koymuştur.

Bilişim Suçları ve Adana İlinde 2006-2009 Yılları Arasında Meydana Gelen Bilişim Suçlarının Değerlendirilmesi konulu yüksek lisans teziyle Kezban ATALIÇ TAŞ[57] Adana ilinde Adana Emniyet Müdürlüğü arşiv kayıtlarındaki toplam 648 olay ve 1872 kişi üzerinde inceleme yapmıştır. Bilişim suçlarındaki olay ve şüpheli sayılarındaki artış yönünden Adana’nın Türkiye geneli ile benzerlik gösterdiğini ortaya koymuş. Adana’nın bilişim suçu işlenen ilk on il sıralamasında dördüncü sırada yer aldığı ortaya çıkmıştır.

“Bilişim Alanında Suçlar” konulu yüksek lisans teziyle Tunç DEMİRCAN’a[58] göre 5237 sayılı kanunla getirilen yeni düzenleme, 765 sayılı TCK’ndaki Bilişim Suçları’nda düzenlenen 525. maddede yer alan eksiklikleri gidermek bakımından oldukça yerinde olmuştur. Yeni kanunla sadece teorik alanda düzenlemeler yapmakla böylesine önemli bir alan geçiştirilmemiş aynı zamanda da 1991 yılından 2004 yılına kadar geçen süre zarfı içinde uygulamada yaşanan sıkıntılardan ders alınmıştır. Sadece bununla kalınmayıp, 21. yüzyılda bilişim sektöründe yaşanan büyük ilerlemelere güncellik sağlanmıştır.

“Bilişim Suçlarıyla Mücadelede Polisin Eğitimi” konulu doktora teziyle Çetin GÜMÜŞ[59] Türk polisinin bilişim suçları alanında genel bir profilinin çıkarılması amacıyla 81 İl Emniyet Müdürlüğü Kaçakçılık ve Organize Suçlarla Mücadele Şube Müdürlüğü ve Bilgi İşlem Şube Müdürlükleri’nde bilişim suçları konusunda görev yapan 379 personele yönelik anket uygulanarak bilişim suçlarına ilişkin yeterlilikleri hakkında araştırma yapmıştır. GÜMÜŞ’e göre “Emniyet Genel Müdürlüğü bünyesinde “Bilişim Suçları” konusunda görev yapan birimlerden olan 81 İl Emniyet Müdürlüğü Kaçakçılık Organize Suçlarla Mücadele ve Bilgi İşlem Şube Müdürlüğü personeli toplam 379 personelin; en çok üniversite veya yüksek okul düzeyinde bulunduğu (% 53,0), bunu lise ve dengi okul düzeyinde bulunanların (% 25,3) takip ettiği görülmektedir. Meslek Yüksek Okulu mezunlarının oranı, % 18,8 olup, bunu %

2,9 ile yüksek lisans ve doktora düzeyinde bulunan personel takip etmektedir. Personelin; büyük çoğunluğunun polis memuru rütbesindeki personelden (% 86,5) oluştuğu görülmektedir. Amir seviyesindeki personelin oranı ise %13,5'tir. Genel olarak bakıldığında, "Bilişim Suçları" konusunda görev yapan personelin eğitim düzeyinin yüksek eğitim düzeyinde olduğu görülmektedir. Bu tür suçlarla ilgili görevli personelin eğitim düzeyinin, lise seviyesinin altında bulunmaması bilişim suçlarıyla mücadelede önemli bir unsur olarak ortaya çıkmaktadır."

"Siber Terörizm Bağlamında Türkiye'ye Yönelik Faaliyet Yürüten Terör Örgütlerinin İnternet Sitelerine Yönelik Bir İçerik Analizi" konulu yüksek lisans teziyle Tezcan ÖZKAN[60] interneti diğer iletişim araçlarından ayıran ve onu diğerlerinden görece üstün kılan özelliklerin, terör örgütleri ve sempatizanları için basit ama etkili bir propaganda aracı olarak kullanıldığını ve internetin kötü niyetli kişiler ve yasadışı gruplar tarafından denetimsiz bir şekilde kullanımının yaratabileceği sorunları ortaya koymaktadır

"Bilişim Suçlarının Sosyolojik Analizi" Konulu yüksek lisans teziyle Şükrü DURMAZ[61] bilişim suçlarının çeşitleri, işleniş şekilleri, işlenme nedenleri ve alınması gereken tedbirler, bilişim suçlarını işleyen şahıslar ile bu konunun uzmanları ile yapılan görüşmeleri sosyolojik bir bakış açısıyla incelenmiştir. DURMAZ'a göre "Emniyet güçlerinin bilişim suçlarını önlemede yetersiz kalması ya da suçun faillerini yakalamaya yönelik yeterince güven telkin etmemesi nedeniyle, suça maruz kalan bankacılık ve finans sektörleri, suçu emniyet güçlerine bildirmemekte ve oluşan zararı kendi ödenekleri ile kapatmaktadırlar. Bu durum suçun boyutunun tespit edilmesini engellediği gibi, faillerin bulunamaması ve dolayısı ile toplumdaki huzur ve güvenin sağlanamaması gibi çeşitli aksaklıklara neden olmaktadır."

"Ülkemizde Bilişim Suçları ve Mücadele Yöntemleri" konulu makalesiyle Semih DOKURER[62] 1998-2001 yılları arasındaki bilişim suçu verilerini değerlendirmiştir. 1999-2001 yılları arasındaki istatistiklerde %100 oranında artış olduğunu göstermiş. Bu artışı da teknolojinin hızlı ilerlemesiyle birlikte ceza kanunlarının yetersiz kalmasına bağlamıştır.

“Phishing: İnternet Denizinin Popüler Avlanma Yöntemi” adlı makalesiyle Şükrü ALATAŞ ve Murat ATAN[63] Anti-Phishing Working Group (APWG)’un yayınlamış olduğu 2004-2006 yılları arasındaki firmaların maruz kaldıkları phishing saldırılarına ait verileri incelemiştir. Sosyal mühendislik yöntemlerinin phising saldırılarındaki rolünü açıklamıştır.

“İnternet Yayıncılığında Etik ve Hukuki İhlaller” adlı makalesiyle Feridun NİZAM ve Serkan BİÇER kişilik haklarının ihlalinde en çok rastlanan yöntem olan internet yoluyla yapılan kişilik haklarına saldırı konusunda etik ve hukuki düzenlemelerin eksikliğine dikkat çekmiştir. NİZAM ve BİÇER (2005) söyle demektedir[64]:

“Geleneksel kitle iletişim araçlarında ihlaller karşısında önleme, yayın durdurma, toplatma ile maddi ve manevi tazminat davaları gibi korunma araçları bulunurken, internet medyasında mağdur durumdaki kişi haklarını aramak için fiziksel olarak muhatap bile bulamamaktadır.

İnternet yayıncılığının bir diğer kanayan yarası, özel hayatın gizliliğine ilişkin yapılan ihlallerdir. Geleneksel kitle iletişim araçlarında daha fazla özen gösterilen özel hayatın gizliliği prensibi, internet medyasında hiçe sayılarak kişinin özel hayatı tam anlamıyla deşifre edilmektedir.”

“Bilişim Suçları Bağlamında Yeni Medya Olarak İnternet ve Kişisel Güvenlik” adlı makalesiyle Serhat KOÇ ve Selva KAYNAK ülkemizde her gün çok sayıda masum vatandaşımızın e-posta hesapları çeşitli şifre kırma yöntemleriyle ele geçirilmekte ve suçun oluşmasından sonra bahsedilen tahkikat aşamalarına dahi hiç geçilemediğini belirtmiştir. Bunun sebebinin genel olarak bu konuların hukuk sistemi tarafından düzenlendiğinin geniş kitlelerce bilinmiyor olması olduğudur. Failler tarafından bu cezalar bilinmediği gibi mağdurlar da bunu yapanların üzerine gitmemekte ve haklarını savunmamaktadırlar[29].

“Sanal Ortamda Gerçek Tehditler Siber Terör” konulu makalesiyle Bünyamin ATICI ve Çetin GÜMÜŞ 11 Eylül 2001’den sonraki dünyadaki terör saldırılarındaki yöntem değişikliklerine değinmiştir. ATICI ve GÜMÜŞ (2003) söyle demektedir[65]:

“Ülkemiz, tarih boyunca özellikle jeopolitik konumu gereği, her zaman için, çeşitli devletlerin ve terör örgütlerinin hedefi haline gelmiştir. Günümüzde, terör örgütlerinin kendilerine destek veren dış merkezli bilgisayar sistemleri aracılığıyla, ülkemize yönelik siber saldırı hareketlerinde bulunabilecekleri göz ardı edilmemeli ve olası siber saldırılara karşı bu durum kurumlar koordinasyonunda her zaman yakından gözlemlenmeli ve siber saldırı acil eylem planları ile hazırlıklı bulunmalıdır. Unutulmamalıdır ki, siber terörizme karşı hazırlıksız bir şekilde bulunmak günlük hayatın akışını da derinden felce uğratabileceği gibi, ülke güvenliğini ciddi bir şekilde tehdit edebilecektir.

Ülkemiz aleyhinde faaliyet gösteren zararlı internet sitesi sayısı yaklaşık 8000 civarındadır. Bu sitelerden 150 tanesini aktif olarak faaliyette olup, her gün ortalama 500-1000 bin kişi ziyaret etmektedir. Genelde com, org, net uzantılı olan bu siteler Amerika, Almanya, Hollanda ve diğer Batı Avrupa ülkeleri üzerinden yayın yapmaktadırlar”.

Bilgisayar Suçları adlı makalesiyle Hatcher: “Başlangıçta bilişim suçları geleneksel suçların bilgisayar yoluyla işlenmesi olarak kabul edilirken, zamanla teknolojinin getirmiş olduğu önceki suç tanımlarına benzemeyen yeni suç tipleri ortaya çıkmaktadır. Bilişim suç tiplerindeki çeşitlilik ve sürekli artış, bu suçlarda tek bir tanımın yeterli olmamasına neden olmaktadır. Diğer yandan bilgisayar teknolojisinin ve internetin hızlı gelişimi, yeni suç tiplerini ortaya çıkarmakta ve suçla mücadelede yeni yasaları gerekli kılmaktadır[66].”

Campbell faillerin ortak özelliklerini şöyle açıklamaktadır: Bilişim suçu faillerinin bazıları, belirli bir yerde çalışmakla birlikte, isimsiz olarak interneti kullanarak, çalıştıkları iş dışında bilgi elde eden ve bunları kişisel kazanç için kullanan kimselerdir. Bu kimseler, çalıştıkları işten kovulma aşamasındadırlar ve işlerinde mutsuzdurlar. Bu failler, çalıştıkları işyerlerinin bilgisayarlarıyla suç işlemektedirler

ve işverenleriyle de ilişkileri bozuk durumdadır. Anılan failler, bilişim sistemindeki hassas bilgileri çalmak ve bunları satmak suretiyle kazanç elde etmeyi isterler[67].”

Carter’ın faillerin hareket tarzlarını açıklayan makalesinde şöyle demektedir: “Bilişim suçu faillerinin teknolojideki en son yenilikleri suç işlerken kullanmaları ise suçla mücadele eden görevlileri bilişim suçlarıyla mücadelede yeterli olmaktan uzak tutmaktadır. Bu bakımdan bu suçlarla mücadele eden birimlerin, faillerin suç işleme tekniklerini, kullandıkları teknolojiyi ve faillerin niteliklerini bilmeleri ve buna göre stratejiler üretmeleri zorunludur[68].”

# 3. MATERYAL VE METOT

## 3.1. Materyal

Bu çalışmada iki farklı kategoride veri toplanmıştır. Birinci kategori literatür taramasına dayanır. Araştırmada her türlü yazılı kaynağa özellikle bu konu ile ilgili yapılmış olan tez, yayınlanmış makale, dergi ve kitaplara ulaşılmaya çalışılmıştır. Ayrıca araştırma raporları, kuruluşların raporları ve bültenleri incelenmiştir.

İkinci kategori ise alan çalışmasıdır. Alan araştırması iki boyutlu bir çalışma olup ilk kısmını bilişim suçundan cezaevinde bulunan hükümlüler oluşturmaktadır. Belirlenen cezaevinde toplam 30 hükümlü ile görüşülmüştür.

Cezaevinde uygulanan anket çalışması Ceza ve Tevkifevleri Genel Müdürlüğü Yetişkin Eğitim Bürosunun görüşleri dikkate alınarak hazırlanmıştır. Ayrıca İstatistik Şubeden alınan cezaevlerine göre hükümlü dağılımları anketin yapılacağı cezaevlerinin belirlenmesine yardımcı olmuştur.

Nicel çalışma kısmın ise bilişim suçları ile ilgili üniversitelerde bilgisayar ve öğretim teknolojileri bölümünde okuyan öğrenciler araştırmanın evren kısmını oluşturmaktadır. Bu bölümde BÖTE bölümü öğrencilerinin bilişim teknolojilerini kullanma durumları ve bilişim suçları konusunda bilgi düzeyleri ile tutumları ölçülmüştür.

Çalışmada kullanılan istatistikler Türkiye İstatistik Kurumundan Gazi Üniversitesi Bilişim Enstitüsü aracılığıyla, İçişleri Bakanlığı Kaçakçılık İstihbarat Harekât ve Bilgi Toplama Daire Başkanlığına ve Bankalararası Kart Merkezine şahsen başvuru yapılarak elde edilmiştir. Adalet Bakanlığından alınan verileri ise Adalet Bakanlığı Adli Sicil ve İstatistik Genel Müdürlüğü'nün internet sitesinden alınmıştır.

## 3.2. Metot

Çalışmasının nitel araştırma boyutunda tarama modeli kullanılmıştır. Tarama modeli geçmişte ve hala var olan bir durumu var olduğu şekliyle tanımlamayı amaçlayan bir yaklaşımdır. Bu model verinin, bütünlük, derinlik ve zenginliği içerisinde betimlenmesine ve aktörlerin perspektiflerini anlatmaya yardımcı olmaktadır.

Nitel araştırma, gözlem, görüşme ve doküman analizi gibi nitel veri toplama yöntemlerinin kullanıldığı, algıların ve olayların doğal ortamda gerçekçi ve bütüncül bir biçimde ortaya konmasına yönelik bir sürecin izlendiği araştırma türüdür. Bu maksatla 19 soruluk anket formu kullanılarak hükümlülerin işledikleri suçları kendi açılarından aktarmaları sağlanmış, arkadaş çevresinin ve suça iten sebeplerin hükümlüler açısından değerlendirilmesi yapılmıştır. Anket bilgilerinin hükümlülerin aleyhinde kullanılmayacağı özellikle belirtilmiş ve hükümlülerin anketi cevaplarken rahat olmaları için kimliklerini tespitine yönelik soru sorulmamıştır.

Anketi uygulamak için Ceza İnfaz Kurumları Genel Müdürlüğünden izin alınmıştır. Ceza İnfaz kurumunu belirlemek amacıyla Ceza İnfaz Kurumları İstatistik şubesinden bilişim suçundan hükümlü bulunanların ceza infaz kurumlarına göre sayısal dağılımı incelenmiş ve Ankara Ceza İnfaz Kurumları Kampusunda yer alan 1 ve 2 Numaralı L tipi Ceza İnfaz Kurumları uygun bulunmuştur. Anket, Adalet Bakanlığı Ceza ve Tevkifevleri Genel Müdürlüğünden 20.08.2010 tarihinde alınan izinle Ankara 1 ve 2 Numaralı L Tipi Kapalı Ceza İnfaz Kurumunda ses kaydı ve görüntü alınmadan hükümlülere kapalı ceza infaz kurumunun kütüphanesinde, ceza infaz memurları ve ceza infaz kurumu sosyal çalışmacısı eşliğinde yapılmıştır. Hükümlülerin sosyal çalışmacı eşliğinde daha rahat davrandıkları gözlenmiştir, ayrıca anket uygulayan araştırmacıya yönelik samimi ortamın sağlanmasına olumlu katkıları olmuştur.

TUİK ve Adalet Bakanlığı verileri incelendiğinde (bknz. Şekil 2.2) hükümlülerin çoğunun 5237 sayılı Türk Ceza Kanununu 245'inci maddesinden dolayı cezaevinde bulunduğu görülmüştür. Bu sebepten nitel anket formu TCK 245'inci maddesinde belirtilen suçtan hüküm giyenlere göre oluşturulmuştur. Anket soruları açık uçlu olup

hükümlülerin demografik özelliklerini ortaya koymak için kapalı uçlu sorular da hazırlanmıştır. Anket formu EK-2'dedir.

Türk Ceza kanununda 26.09.2004 tarihinde değişiklik yapılmış ve Yeni TCK 1 Haziran 2005 tarihinde yürürlüğe girmiştir[7]. Bu değişiklikten önceki bilişim suçları Adalet Bakanlığı verileri Ulusal Yargı Ağı Projesi (UYAP) üzerinde ve İçişleri Bakanlığı Kaçakçılık İstihbarat Harekât ve Bilgi Toplama Daire Başkanlığı (KİHBİ) verilerinde yer almamaktadır. Bu sebeple 1 Haziran 2005 tarihinden önceki bilişim suçları kapsamında olmayan veriler dikkate alınmamıştır.

Nicel çalışma kısmında ise bilişim suçları ile ilgili üniversitelerde bilgisayar ve öğretim teknolojileri bölümünde okuyan öğrencilerin bilişim teknolojilerini kullanma durumları ve bilişim suçları konusunda bilgi düzeyleri ve tutumları ölçülmüştür. Nicel araştırma olgu ve olayları nesnelleştirerek gözlemlenebilir, ölçülebilir ve sayısal olarak ifade edilebilir bir şekilde ortaya koyan bir araştırma türüdür. Nicel araştırma yöntemleri herhangi bir etkeni inceleyerek değişkenler arasındaki neden-sonuç ilişkilerini tespit etmek ve sonuçları karşılaştırmak amacıyla kullanılır.

BÖTE bölümü öğrencilerine anket çalışması uygulanmadan önce internet üzerinden 100 kişiyle 51 soruluk ön uygulama yapılmıştır. İstatistik açıdan anlamlı olmayan 2 soru anketten çıkarılmıştır. 49 soruluk yeni anket formu oluşturulduktan sonra bünyesinde BÖTE bölümü bulunan üniversitelerin öğretim üyeleriyle ve sosyal platformlar vasıtasıyla öğrenci gruplarıyla irtibata geçilmiştir. Bu sayede anketin farklı sınıflarda ve farklı üniversitelerdeki öğrencilere ulaşması sağlanmaya çalışılmıştır.

Anket formunda sorulacak sorular öğrencilerin tutum ve bilgi seviyeleri tespit edildikten sonra oluşturulmuştur. Ön uygulama safhasında anketin geçerliliği ve güvenirliği ölçülmüştür. Bu maksatla ön uygulamada sorulan 51 soruluk anket formuna verilen cevaplara göre faktör analizi yapılmış ve istatistik açıdan önemsiz olan sorular çıkarılmış ve bazı sorularda düzeltme yapılarak yeni form oluşturulmuştur. Anketin güvenilirliği hakkında bilgi elde etmek amacıyla yapılan iç tutarlılık güvenilirliği analizlerinde Crombach Alpha ( $\alpha$ ) katsayısı 0.94 olarak

bulunmuştur. Alfa katsayısı $0.80 \leq \alpha \geq 1.00$ olduğundan ölçeğin yüksek derecede güvenilir olduğunu söylenebilir.

Katılımcılara en son oluşturulan 49 soruluk Ek-1'deki sorular yöneltilmiştir. Sorular www.online-anket.gen.tr web sitesi üzerinden yöneltilmiş olup basit tesadüfi örnekleme yöntemi ile 312 Bilgisayar ve Öğretim Teknolojileri Eğitimi Bölümü öğrencisine ulaşılmıştır. Bu kişiler farklı illerden ve okullardan olduğu için Türkiye'yi temsil etmektedirler. Anket doldurulurken sorular eksiksiz yanıtlanmak zorunda olduğundan ankette değerlendirilmeyen soru olmayıp değerlendirme 312 kişi üzerinden yapılmıştır. Anketler 24 günlük süre içerisinde tamamlanmıştır.

# 4. UYGULAMA

## 4.1. Üniversite Öğrencilerinin Bilişim Suçlarına Yönelik Tutum ve Bilgi Düzeyleri Üzerine Araştırma

### 4.1.1. Araştırmanın çözümü

Katılımcılara Ek-1'deki sorular yöneltilmiştir. Sorular www.online-anket.gen.tr web sitesi üzerinden yöneltilmiş olup 312 Bilgisayar ve Öğretim Teknolojileri Eğitimi Bölümü öğrencisi ankete katılmıştır.

Ankete katılanların demografik özellikleri

Çizelge 4.1. Cinsiyet dağılımı

| Cinsiyet | f | % |
|---|---|---|
| ERKEK | 187 | %59.94 |
| KADIN | 125 | %40.06 |

Katılımcıların 187'si (%59,94) erkek, 125'i (%40,06) kadındır.

Çizelge 4.2. Sınıflara göre dağılım.

| Sınıflar | f | % |
|---|---|---|
| I.SINIF | 36 | %11.03 |
| II. SINIF | 37 | %11.86 |
| III. SINIF | 73 | %23.40 |
| IV. SINIF | 166 | %53.21 |

Ankete katılanların 36'sı(%11.03) 1.sınıf öğrencisi, 37'si (%11.86) 2.sınıf öğrencisi, 73'ü (%23.40) 3.sınıf öğrencisi ve 166'sı (%53.21) 4.sınıf öğrencisidir.

Çizelge 4.3. Ankete katılan üniversiteler

| **Üniversiteler** | **f** | **%** |
|---|---|---|
| Afyon Kocatepe Üniversitesi | 10 | %3,21 |
| Anadolu Üniversitesi | 12 | %3,85 |
| Ankara Üniversitesi | 11 | %3,53 |
| Atatürk Üniversitesi | 8 | %2,56 |
| Bahçeşehir Üniversitesi | 9 | %2,88 |
| Başkent Üniversitesi | 16 | %5,13 |
| Boğaziçi Üniversitesi | 10 | %3,21 |
| Çanakkale Onsekiz mart Üniversitesi | 12 | %3,85 |
| Çukurova Üniversitesi | 11 | %3,53 |
| Ege Üniversitesi | 35 | %11,22 |
| Fırat Üniversitesi | 21 | %6,73 |
| Gazi Üniversitesi | 36 | %11,54 |
| Karadeniz Teknik Üniversitesi | 7 | %2,24 |
| Marmara Üniversitesi | 12 | %3,85 |
| Ondokuz Mayıs Üniversitesi | 8 | %2,56 |
| Orta Doğu Teknik Üniversitesi | 13 | %4,17 |
| Sakarya Üniversitesi | 8 | %2,56 |

| | | |
|---|---|---|
| Selçuk Üniversitesi | 23 | %7,37 |
| Uludağ Üniversitesi | 10 | %3,21 |
| Yıldız Teknik Üniversitesi | 10 | %3,21 |
| Yüzüncü Yıl Üniversitesi | 19 | %6,09 |
| Eskişehir Osmangazi Üniversitesi | 11 | %3,53 |

Katılımcıların okudukları üniversiteler Tablo 4.3'te gösterildiği gibidir. 23 farklı üniversiteden BÖTE bölümlerinden katılım olmuştur.

Çizelge 4.4. Bilgisayara sahip olma durumu

| **KENDİNE AİT BİLGİSAYARI** | **f** | **%** |
|---|---|---|
| VAR | 289 | %92.63 |
| YOK | 23 | %7.37 |

Ankete katılanların 289'unun kendine ait bir bilgisayarı vardır. 23'ünün ise kendine ait bilgisayarı yoktur.

Ankete katılanların vermiş olduğu cevaplara göre hazırlanmış olan frekans tabloları ve % değerleri aşağıdadır.

Çizelge 4.5. İnternette geçirilen zaman

| **İnternette geçirilen zaman** | **Sayı** | **Yüzde** |
|---|---|---|
| 0-1 SAAT | 54 | %17.31 |
| 1-3 SAAT | 118 | %37.82 |
| 3-5 SAAT | 74 | %23.72 |
| 5 SAAT VE ÜZERİ | 66 | %21.15 |

Katılımcılardan "**Bir Gün İçerisinde İnternete Bağlı Olarak Geçirdiğiniz Süre Ne Kadar?**" sorusuna 118 kişi (%37.82) 1-3 saat aralığında bir gün içerisinde internete bağlı olduğu cevabını vermiştir.

Çizelge 4.6. İnternete bağlanırken kullanılan cihaz

| **Seçenekler** | **f** | **%** |
|---|---|---|
| BİLGİSAYAR | 306 | %98.08 |
| CEP TELEFONU | 6 | %1.92 |
| PDA -Tablet PC | 0 | %0.00 |

Katılımcılardan "**İnternet genellikle nereden bağlanırsınız?**" sorusuna 306 kişi (%98.08) bilgisayar cevabını vermiştir.

Çizelge 4.7. İnternete bağlanılan yer

| **Seçenekler** | **f** | **%** |
|---|---|---|
| EV | 233 | %74.68 |
| OKUL | 21 | %6.73 |
| YURT | 32 | %10.26 |
| İŞ YERİ | 10 | %3.21 |
| İNTERNET KAFE | 16 | %5.13 |

Katılımcılardan "**İnternet genellikle nereden bağlanırsınız?**" sorusuna 233 kişi (%74.68) evden bağlandığı yanıtını vermiştir.

Çizelge 4.8. Şifre ve parolaları değiştirme durumu

| **Seçenekler** | **f** | **%** |
|---|---|---|
| EVET DEĞİŞTİRİRİM | 72 | %23.08 |
| HAYIR DEĞİŞTİRMEM | 240 | %76.92 |

Katılımcılardan "**İnternet üzerinde kullandığınız şifre ve parolaları sıklıkla değiştirir misiniz?**" sorusuna 240 kişi (%76.92) sıklıkla değiştirmediği yanıtını vermiştir.

Çizelge 4.9. İnternet bankacılığı veya cep bankacılık kullanma durumu

| Seçenekler | f | % |
|---|---|---|
| EVET KULLANIYORUM | 87 | **%27.88** |
| HAYIR KULLANMIYORUM | 225 | **%72.12** |

Katılımcılardan "**İnternet bankacığı ve cep bankacılığı uygulamalarını kullanıyor musunuz?**" sorusuna 225 kişi (%72.12) internet ve cep bankacılığını kullanmadığını söylemiştir.

Çizelge 4.10. İnternet üzerinden alışveriş durumu

| Seçenekler | f | % |
|---|---|---|
| EVET | 125 | **%40.06** |
| HAYIR | 187 | **%59.94** |

Katılımcılardan "**İnternet üzerinden alışveriş yapıyor musunuz?**" sorusuna 187 kişi (%59.94) internet üzerinden alışveriş yapmadığını söylemiştir.

Çizelge 4.11. İşletim sistemi lisans durumu

| Seçenekler | f | % |
|---|---|---|
| EVET | 183 | **%58.65** |
| HAYIR | 106 | **%33.97** |
| DENEME SÜRÜMÜ KULLANIYORUM | 23 | **%7.37** |

Katılımcıların "**Kullandığınız işletim sistemi lisanslı mıdır?**" sorusuna 183 kişi (%58.65) lisanslı işletim sistemi kullandığı yanıtını vermiştir.

Çizelge 4.12 Anti virüs veya firewall yazılımı kullanma durumu

| **Seçenekler** | **f** | **%** |
|---|---|---|
| EVET KULLANIYORUM | 279 | **%89.42** |
| HAYIR KULLANMIYORUM | 33 | **%10.58** |

Katılımcılardan "**Kişisel bilgisayarınızda anti virüs veya firewall yazılımı kullanıyor musunuz?** " sorusuna 279 kişi (%89.42) anti virüs veya firewall yazılımı kullanıyorum yanıtını vermiştir.

Çizelge 4.13. Bilişim suçlarına yönelik tutum

| **Sorular** | Katılıyorum | | Fikrim yok | | Katılmıyorum | |
|---|---|---|---|---|---|---|
| | **f** | **%** | **f** | **%** | **f** | **%** |
| İnternet bankacılığını güvenli buluyorum. | 107 | 34.29 | 106 | 33.97 | 99 | 31.73 |
| İnternet üzerinden alışverişi güvenli buluyorum. | 117 | 37.5 | 70 | 22.44 | 125 | 40.06 |
| Bilişim suçları ile ilgili yasal düzenlemeleri yeterli buluyorum. | 28 | 8,97 | 109 | 34,94 | 175 | 56,09 |
| Bilişim suçlarının tespiti zor olduğu için gerekli bilgiye sahip olsam bende hacker'lik yapardım. | 77 | 24,68 | 70 | 22,44 | 165 | 52,88 |

| | | | | | | |
|---|---|---|---|---|---|---|
| Gizli kamera görüntülerinin ve kişisel bilgilerin internet aracılığıyla ifşa edilmesini doğru bulmuyorum | 222 | 71,15 | 22 | 7,05 | 68 | 21,79 |
| İnternette hackerlık yöntemlerini anlatan ve gerekli casusluk yazılımlarını temin etmemizi sağlayan siteler yasaklanmalı. | 199 | 63,78 | 47 | 15,06 | 66 | 21,15 |
| İnternetten film, oyun, müzik ve oyun dosyaları indirmenin ve lisanssız yazılım kullanmanın suç olduğunu biliyorum | 262 | 83,97 | 29 | 9,29 | 21 | 6,73 |
| Bilgisayarımı ve cep telefonumu tamire verirken önemli bilgilerimi silerim veya şifrelerim / gizlerim | 255 | 81,73 | 37 | 11,86 | 20 | 6,41 |
| Kolluk kuvvetlerinin (polis, jandarma) bilişim suçlarını önlemede ve tespitinde yapmış olduğu çalışmaları yeterli buluyorum | 53 | 16,99 | 113 | 36,22 | 146 | 46,79 |
| Kredi kartı ile yapılan alışverişlerde şifre uygulaması (chip&pin) ile kredi kartı kullanımının daha güvenli hale geldiğini düşünüyorum. | 206 | 66,03 | 65 | 20,83 | 41 | 13,14 |
| Cep telefonu görüşmelerinin ve e-posta yazışmalarının adli makamlar tarafından dinlenip takip edilmesini kamu güvenliği açısından yararlı buluyorum. | 125 | 40,06 | 53 | 16,99 | 134 | 42,95 |
| Sosyal paylaşım sitelerinin ( FACEBOOK, TWITTER vb.) kişisel bilgilerimi ve fotoğraflarımı başka kişi ve şirketlerle/kurumlarla paylaştığı yönünde endişelerim var.” | 190 | 60,90 | 68 | 21,79 | 54 | 17,31 |

| | | | | | | |
|---|---|---|---|---|---|---|
| Mahkeme kararıyla içinde suç unsuru olduğu tespit edilen ve kapatılmasına karar verilen web sitelerine yapılan hukuki engellemelerin düşünce özgürlüğüne aykırı olduğunu düşünüyorum. | 125 | 40,06 | 68 | 21,79 | 119 | 38,14 |

Katılımcılara "**İnternet bankacılığını güvenli buluyorum.**" konusundaki fikirleri sorulduğunda 107 kişi (%34.29) güvenli bulduğu yanıtını vermiştir.

Katılımcılara "**İnternet üzerinden alışverişi güvenli buluyorum.**" konusundaki fikirleri sorulduğunda 125 kişi (%40.06) güvenli bulmadığı yanıtını vermiştir.

Katılımcılara "**Bilişim suçları ile ilgili yasal düzenlemeleri yeterli buluyorum.**" konusundaki fikirleri sorulduğunda 175 kişi (%56.09) yeterli bulmadığı yanıtını vermiştir.

Katılımcılara "**Bilişim suçlarının tespiti zor olduğu için gerekli bilgiye sahip olsam bende hacker'lik yapardım.**" konusundaki fikirleri sorulduğunda 165 kişi (%52.88) katılmadığı yanıtını vermiştir.

Katılımcılara "**Gizli kamera görüntülerinin ve kişisel bilgilerin internet aracılığıyla ifşa edilmesini doğru bulmuyorum.**" konusundaki fikirleri sorulduğunda 222 kişi (%71.15) bu hususu doğru bulmadığı yanıtını vermiştir.

Katılımcılara "**İnternette hackerlık yöntemlerini anlatan ve gerekli casusluk yazılımlarını temin etmemizi sağlayan siteler yasaklanmalı**." konusundaki fikirleri sorulduğunda 199 kişi (%63.78) bu tür sitelerin yasaklanması yanıtını vermiştir.

Katılımcılara "**İnternetten film, oyun, müzik ve oyun dosyaları indirmenin ve lisanssız yazılım kullanmanın suç olduğunu biliyorum.**" konusundaki fikirleri

sorulduğunda 262 kişi (%83.97) lisanssız yazılım kullanmanın ve film, oyun indirmenin yasal olmadığını bildiği yanıtını vermiştir.

Katılımcılara "Bilgisayarımı ve cep telefonumu tamire verirken önemli bilgilerimi silerim veya şifrelerim / gizlerim." konusundaki fikirleri sorulduğunda 255 kişi (%81.73) önemli bilgilerini gizlediği veya sakladığı yanıtını vermiştir.

Katılımcılara "**Kolluk kuvvetlerinin (polis, jandarma) bilişim suçlarını önlemede ve tespitinde yapmış olduğu çalışmaları yeterli buluyorum.**" konusundaki fikirleri sorulduğunda 146 kişi (%46.79) kolluk kuvvetlerinin yürütmüş olduğu çalışmaların yeterli olmadığı yanıtını vermiştir.

Katılımcılara "**Kredi kartı ile yapılan alışverişlerde şifre uygulaması (chip&pin) ile kredi kartı kullanımının daha güvenli hale geldiğini düşünüyorum.**" konusundaki fikirleri sorulduğunda 206 kişi (%66.03) alışverişlerde şifre uygulamasını güvenli bulduğu yanıtını vermiştir.

Katılımcılara "**Cep telefonu görüşmelerinin ve e-posta yazışmalarının adli makamlar tarafından dinlenip takip edilmesini kamu güvenliği açısından yararlı buluyorum.**" konusundaki fikirleri sorulduğunda 134 kişi (%42.95) adli makamların yürüttüğü dinleme ve takip faaliyetlerinin kamu güvenliği açısından yararlı bulmadığı yanıtını vermiştir.

Katılımcılara "**Sosyal paylaşım sitelerinin ( FACEBOOK, TWITTER vb.) kişisel bilgilerimi ve fotoğraflarımı başka kişi ve şirketlerle/kurumlarla paylaştığı yönünde endişelerim var.**" konusundaki fikirleri sorulduğunda 190 kişi (%60.90) bu konuda endişelerinin olduğu yanıtını vermiştir.

Katılımcılara "**Mahkeme kararıyla içinde suç unsuru olduğu tespit edilen ve kapatılmasına karar verilen web sitelerine yapılan hukuki engellemelerin düşünce özgürlüğüne aykırı olduğunu düşünüyorum**." konusundaki fikirleri sorulduğunda 125 kişi (%40.06) web sitelerine yönelik hukuki engellemeleri doğru bulduğu yanıtını vermiştir.

Çizelge 4.14. Bilişim suçlarına yönelik bilgi düzeyi

| **Sorular** | Bilgi Sahibiyim | | Sadece Duydum | | Bilgim Yok | |
|---|---|---|---|---|---|---|
| | **f** | **%** | **f** | **%** | **f** | **%** |
| 01.03.2006 tarihinde yürürlüğe giren 5464 no'lu Banka Kartları ve Kredi Kartları Kanunu gereği, kart hamilleri, yapacakları kayıp ya da çalıntı bildiriminden önceki yirmi dört saat içinde kartları ile gerçekleştirilen hukuka aykırı kullanımdan doğan zararlardan 150 TL. ile sınırlı olmak üzere sorumludurlar. Bunun üzerindeki zararların bankanızın güvencesi altında olduğunu biliyor musunuz? | 54 | 17,31 | 73 | 23,40 | 185 | 59,29 |
| Bankamatiklerden (ATM) banka veya kredi kartınızla işlem yaparken sahte klavye, kartın manyetik şerit bilgisinin kopyalanması (skimmer cihazı) gibi yöntemlerle hesabınızdan para çekilebileceğini biliyor musunuz? | 149 | 47,76 | 100 | 32,05 | 63 | 20,19 |
| Sosyal mühendislik yöntemleri ile suçluların bilgisayarınıza erişim sağlayarak bilgisayarınıza gizlice casus yazılımlar ya da diğer istenmeyen yazılımlar yüklemek veya parolalarınızı ya da önemli mali ve kişisel bilgilerinizi vermeniz için sizi ikna etmeye çalışabileceğini biliyor musunuz? | 170 | 54,49 | 85 | 27,24 | 57 | 18,27 |

| | | | | | | |
|---|---|---|---|---|---|---|
| Kendilerini kamu görevlisi olarak tanıtan veya ödül kazandığınızı belirterek para/kontör transferi talep ederek dolandırılabileceğinizi biliyor musunuz? | 227 | 72,76 | 57 | 18,27 | 28 | 8,97 |
| Java Script' içeren sahte bir program aracılığı ile hedef bilgisayara hacker tarafından gönderilen sahte program açıldığında, bilgisayar ekranına ŞİFRENİZİ YENİDEN GİRİN yazısı çıkartılıp kullanıcının şifresini öğrenerek saldırgana ulaştırılabileceğini biliyor musunuz? | 123 | 39,42 | 84 | 26,92 | 105 | 33,65 |
| Müşterek kullanıma açık olan yerlerdeki bilgisayarlara loadpowerprof.exe, keylogger.exe vb. programlar yüklenerek internet bankacılığı ile işlem yapan mevduat sahiplerinin hesabına erişim sağlanabileceğini biliyor musunuz? | 122 | 39,10 | 78 | 25,00 | 112 | 35,90 |

Katılımcılara " **01.03.2006 tarihinde yürürlüğe giren 5464 no'lu Banka Kartları ve Kredi Kartları Kanunu gereği, kart hamilleri, yapacakları kayıp ya da çalıntı bildiriminden önceki yirmi dört saat içinde kartları ile gerçekleştirilen hukuka aykırı kullanımdan doğan zararlardan 150 TL. ile sınırlı olmak üzere sorumludurlar. Bunun üzerindeki zararların bankanızın güvencesi altında olduğunu biliyor musunuz?**" konusunda bilgi sahibi olup olmadıkları sorulduğunda 185 kişi (%59.29) bu konu hakkında bilgi sahibi olmadığı yanıtını vermiştir.

Katılımcılara " **Bankamatiklerden (ATM) banka veya kredi kartınızla işlem yaparken sahte klavye, kartın manyetik şerit bilgisinin kopyalanması (skimmer cihazı) gibi yöntemlerle hesabınızdan para çekilebileceğini biliyor musunuz?**" konusunda bilgi sahibi olup olmadıkları sorulduğunda 149 kişi (%47.76) bu konu hakkında bilgi sahibi olduğu yanıtını vermiştir.

Katılımcılara "**Sosyal mühendislik yöntemleri ile suçluların bilgisayarınıza erişim sağlayarak bilgisayarınıza gizlice casus yazılımlar ya da diğer istenmeyen yazılımlar yüklemek veya parolalarınızı ya da önemli mali ve kişisel bilgilerinizi vermeniz için sizi ikna etmeye çalışabileceğini biliyor musunuz?**" konusunda bilgi sahibi olup olmadıkları sorulduğunda 170 kişi (%54.49) bu konu hakkında bilgi sahibi olduğu yanıtını vermiştir.

Katılımcılara "**Kendilerini kamu görevlisi olarak tanıtan veya ödül kazandığınızı belirterek para/kontör transferi talep ederek dolandırılabileceğinizi biliyor musunuz?**" konusunda bilgi sahibi olup olmadıkları sorulduğunda 227 kişi (%72.76) bu konu hakkında bilgi sahibi olduğu yanıtını vermiştir.

Katılımcılara "**Java Script' içeren sahte bir program aracılığı ile hedef bilgisayara hacker tarafından gönderilen sahte program açıldığında, bilgisayar ekranına ŞİFRENİZİ YENİDEN GİRİN yazısı çıkartılıp kullanıcının şifresini öğrenerek saldırgana ulaştırılabileceğini biliyor musunuz?** " konusunda bilgi sahibi olup olmadıkları sorulduğunda 123 kişi (%39.42) bu konu hakkında bilgi sahibi olduğu yanıtını vermiştir.

Katılımcılara "**Müşterek kullanıma açık olan yerlerdeki bilgisayarlara loadpowerprof.exe, keylogger.exe vb. programlar yüklenerek internet bankacılığı ile işlem yapan mevduat sahiplerinin hesabına erişim sağlanabileceğini biliyor musunuz?**" konusunda bilgi sahibi olup olmadıkları sorulduğunda 122 kişi (%39.10) bu konu hakkında bilgi sahibi olduğu yanıtını vermiştir.

Çizelge 4.15. Suç teknikleri

| **Bilişim Suçları Teknikleri** | Bilgi Sahibiyim | | Sadece Duydum | | Bilgim Yok | |
|---|---|---|---|---|---|---|
| | **f** | **%** | **f** | **%** | **f** | **%** |
| Bilgisayar Korsanlığı | 231 | %74.04 | 57 | %18.27 | 24 | %7.69 |
| Ağ Solucanları | 157 | %50.32 | 89 | %28.53 | 66 | %21.15 |
| Web Sayfası Hırsızlığı | 156 | %50.00 | 111 | %35.58 | 45 | %14.42 |
| Bilgisayar Virüsleri | 260 | %83.33 | 42 | %13.46 | 10 | %3.21 |
| Kredi / Banka Kartları Sahteciliği ve Dolandırıcılığı | 171 | %54.81 | 114 | %36.54 | 27 | %8.65 |
| Elektronik İmza | 132 | %42.31 | 139 | %44.55 | 41 | %13.14 |
| Mantık Bombaları | 45 | %14.42 | 96 | %30.77 | 171 | %54.81 |
| İstem Dışı Alınan E-Posta | 210 | %67.31 | 67 | %21.47 | 35 | %11.22 |
| Truva Atı | 213 | %68.27 | 56 | %17.95 | 43 | %13.78 |
| Oltalama (phising) | 60 | %19.23 | 99 | %31.73 | 153 | %49.04 |
| Siber Şantaj ve Tehdit | 112 | %35.90 | 112 | %35.90 | 88 | %28.21 |
| Siber Kumar ve Bahis | 115 | %36.86 | 115 | %36.86 | 82 | %26.28 |
| Siber Dolandırıcılık | 122 | %39.10 | 112 | %35.90 | 78 | %25.00 |

| | | | | | | |
|---|---|---|---|---|---|---|
| Çocuk Pornografisi | 153 | %49.04 | 130 | %41.67 | 129 | %9.29 |

Katılımcılara tablo 3.27'deki suç teknikleri hakkında bilgi sahibi olup olmadıkları sorulduğunda sırasıyla bilgisayar virüsleri hakkında 260 kişinin, bilgisayar korsanlığı (hacking) hakkında 231 kişinin, Truva atı hakkında 213 kişinin ve istem dışı alınan e-postalar hakkında 210 kişinin bilgi sahibi olduğu yanıtı alınmıştır.

Çizelge 4.16. Ders ve seminer ihtiyacı

| **Seçenekler** | **f** | **%** |
|---|---|---|
| evet | 299 | **%95.83** |
| hayır | 7 | **%2.24** |
| fikrim yok | 6 | **%1.92** |

Katılımcılara "Üniversitelerde teknolojik gelişmeler ve siber suçlarla ilgili konuların derslerde anlatılmasını ayrıca bu konularla ilgili seminer düzenlenmesini istiyor musunuz?" sorusu sorulduğunda katılımcılardan 299 kişi (%95.83) bu konu hakkında ders ve seminer verilmesinin uygun olacağını belirtmiştir.

### 4.1.2. Araştırmanın bulguları

Anket sonuçları incelenirken öncelikle dikkat edilmelidir ki, katılımcılar bilgisayar ve öğretim teknolojileri eğitimi bölümü öğrencileridir. Bu öğrenciler birinci sınıftan itibaren bilgisayar eğitimi almaya başlamışlardır. Bilişim dünyası ile iç içe olan bu öğrenciler eğitim ve bilişim sektöründe istihdam olacaklardır. Dolayısıyla hem bilişim güvenliği konularının öğreticisi hem bilişim sektöründe bu konularının yöneticisi hem de herkes gibi doğal olarak bu sistemlerin kullanıcıları olacaklardır.

Öğrencilerin kendine ait bilgisayar sahip olma oranı %93.63'tür. TUİK'in 2011 yılı 2011 yılı Hane Halkı Bilişim Teknolojileri Kullanım Araştırmasına göre ise Türkiye de 16–74 yaş arası bilgisayar sahip olma oranı %46,4, internet kullanım oranı ise

%45'tir[42]. Bu oranlar 2010 yılında sırasıyla %43,2 ve %41,6 idi[69]. Bu oranların Türkiye ortalamasından yüksek olmasının sebebi yaş grubu itibariyle genç olmaları ve öğrencilerin okudukları bölümün bilgisayar teknolojilerini yakından takip etmelerinden kaynaklanmaktadır.

Katılımcıların %98.08'i internete bilgisayar üzerinden bağlandığını söylemiştir. Teknolojinin birbirine yakınsaması ve teknolojideki gelişmeler internete bağlanan platformların da özelliklerini değiştirmiştir. Örneğin cep telefonlarımızdan internete girebiliyoruz aynı zamanda navigasyon aleti olarak kullanıp fotoğraf da çekebiliyoruz. Kablosuz erişim noktalarından sokakta dahi internete ulaşabiliyoruz. Bu yüzden gelecekte bağlantı şeklimizde de büyük ölçüde değişikler olacağı açıktır.

Katılımcıların internete bağlandıkları yer olarak %74,68 ile ev cevabı verilmiştir. Katılımcılar öğrenci olduklarından ve bir kısmının öğrenci yurtlarında kaldığı düşünüldüğünde bağlantı yerine yurt cevabını veren %10,26'lık oranın ev kullanıcılarla beraber düşünülmesi gerekmektedir. TUİK 2011 verilerine göre internete evden bağlanma oranı %67,62dır. Anketi cevaplayan örneklem ortalamanın üzerindendir.

Ankete katılanların %76,92'si internette kullandığı parolaları sıklıkla değiştirmezken, %72,12 internet bankacılığı ve cep bankacılık uygulamalarını kullanmıyor ve %59,94'ü internetten alış veriş yapmamaktadır. Bankacılık uygulamalarını kullanmamaların sebebi katılımcıların öğrenci olması sebebiyle düzenli bir geliri olmadığından bankacılık işlemleri yapmadığı şeklinde değerlendirilmektedir. İnternet bankacılığını kullanmayanların %36,3'ü internet bankacılığını güvenli bulmadıklarından, internet üzerinden alış veriş yapmayanların ise %22,4'ü internet üzerinden alışverişi güvenli bulmadıklarından alışveriş ve bankacılık işlemleri yapmamaktadır.

TÜİK'e göre internet kullanan bireylerin internet üzerinden kişisel kullanım amacıyla mal veya hizmet siparişi verme ya da satın alma oranı %18,6'dır. Ankette oranın %40,06 olması örneklemin çevrimiçi alış veriş sitelerini daha çok kullandığı sonucunu göstermektedir.

Katılımcıların % 58,65'i lisanslı işletim sistemi kullanmaktadır. Lisanslı işletim sistemi kullananların %60,93'ü bilgisayarında anti virüs veya firewall yazılımı bulundurmaktadır. Lisanslı işletim sistemi kullanmak güncellemeler vasıtasıyla güvenlik yamalarını kullanıcının bilgisayarına yüklemesi imkânını sağlayacak ve antivirüs programı kullanmak ise sistemimizin virüs tanımlamalarını güncel tutup sistemin daha iyi çalışmasına imkân verecektir. Sonuç olarak katılımcıların %60,93'ü internete güvenli olarak bağlanmaktadır.

Business Software Alliance(BSA)'nın kişisel bilgisayar kullanıcılarının yazılım korsanlığı ve fikri mülkiyet hakları konularındaki davranış ve tutumları konusunda yapılan araştırmasının sonuçlarına göre, PC kullanıcılarının yaklaşık yarısı % 47'si yazılımlarını çoğu zaman, hatta her zaman yasa dışı yollardan elde ederken gelişmekte olan ekonomilerde bu rakamlar çok daha yüksek seviyelere ulaşabilmektedir[70].

BSA'nın araştırmasının sonuçlarına göre, Türkiye'de halen %63 olan lisanssız yazılım kullanım oranının 2 yılda %53'e indirilmesi bilişim teknolojileri sektöründe mühendis seviyesinde 2180 kişilik ek istihdam yaratılması anlamına gelirken, ekonominin söz konusu 2 yıllık süre zarfında 1 milyar dolar düzeyinde büyümesini ve 205 milyon dolar ek vergi kazancının elde edilmesini sağlayacak[30]. Ankete katılanlardan lisanlı işletim sistemi kullanmıyorum cevabını veren %33,87'lik rakam azımsanmayacak kadar fazladır. 2011 rakamlarıyla Windows 7 Professional işletim sisteminin fiyatı yaklaşık 450 TL ve MsOffice 2010 Home&Student yazılımı da 200 TL'dir. Öğrencilerin çoğunun sabit kazancı olmadığı ve asgari ücretin 2012 yılı birinci yarısı itibariyle 701,44 TL (net ücret) olduğundan lisanssız yazılımın tercih sebebi olmasının nedenlerinden en önemlisinin ekonomik sebepler olduğu değerlendirilmelidir.

Katılımcıların % 56,9'u bilişim suçları ile yasal düzenlemeleri yetersiz bulmaktadır. Savcılıklar bilişim suçları alanında işlenen suçlar bürosu kurmuşlardır. Bu kadrolara bilişim suçlarında uzmanlaşan kadrolar atanmaya başlamıştır. Üniversitelerde bilişim suçları konusunda yüksek lisans programları açılmıştır. Fakat bilgisayar uzmanları ile hukukçuları aynı platformda birleştirmek zordur.

Ankete katılanların %24.68'si gerekli bilgiye sahip olsam hackerlık yapabileceğini söylemiştir. İlginç bir sonuç olarak hacker olabilirim diyenlerin %11,68'si yasal düzenlemeleri yetersiz bulmaktadır ve %17'si gizli kamera görüntülerinin ve kişisel bilgilerin internet aracılığıyla ifşa edilmesini doğru bulmaktadır.

Bilişim suçlarının tespitinin zor ve bu konuda yeterli teknik bilgiye sahip kişilerin az olması sadece ülkemizde değil tüm dünyada hükümetleri savunmasız bırakmıştır. Suçları cezasız bırakmış suçlular serbestçe suç işlemeye devam ederken mağdur sayıları artmıştır.

Katılımcıların %63,78'i internette hackerlık yöntemlerini anlatan ve gerekli casusluk yazılımlarını temin edilmesini sağlayan siteler yasaklanmalı cevabını vermiştir. Bu sitelerde hackerlık yöntemlerini öğrenen ve çoğunlukla network ve yazılım bilgisine sahip olmayan LAMER diye tabir edilen saldırganlar özellikle kablosuz ağ bağlantılarını kırmak gibi saldırı tekniklerini öğrenmektedirler.

Katılımcıların %83,7'si internetten film, oyun, müzik ve oyun dosyaları indirmenin ve lisanssız yazılım kullanmanın suç olduğunu bildiği cevabını vermiştir. TUİK 2011 verilerine göre hanelerin %39,3'ü geniş bant bağlantı ile internet erişim imkânına sahiptir. ADSL bağlantı ile sınırsız kota kullanımına sahip kullanıcılar internet üzerinden film ve müzik indirmektedir. Dünyada korsan yazılım kullanım oranı %39 olarak tahmin edilmektedir. Türkiye ortalaması dünya ortalamasının yaklaşık 15 puan üzerindedir. Farklı değerlendirmeler mevcut olmakla beraber; müzik eserlerinde (Kaset ve CD) korsan kullanım oranının ortalama olarak %70'ler seviyesinde olduğu tahmin edilmektedir[71].

Katılımcıların %81,73'ü bilgisayarını ve cep telefonunu tamire verirken önemli bilgilerini sildiği veya şifrelediği cevabını vermiştir. Özellikle çöpe dalma tekniği denilen ve bozuk, hurda veya tamir edilmek üzere servise bırakılan bilgisayar ve cep telefonları kurcalanarak kullanıcının özel bilgilerine erişilebilmektedir. Şirketler ve kurumlar bilgisayarlarını tamire vermeden önce önemli bilgileri veya ticari sırları çalınmasın diye harddiskleri sökmeli veya içeriği güvenli olarak silmelidir.

Unutulmamalıdır ki harddisk üzerinden veri silerken sadece veriye erişim yolu silinmekte veri istenirse tekrar kurtarılabilmektedir.

Katılımcıların %40,06'sı cep telefonu görüşmelerinin ve e-posta yazışmalarının adli makamlar tarafından dinlenip takip edilmesini kamu güvenliği açısından yararlı bulduğu cevabını vermiştir. Bu görüşmelerin takip edilmesi özel hayatın gizliliğini ihlal edebileceği gibi takip edilen şüphelinin konusu suç teşkil etmeyen yazışma ve görüşmelerinde takip edilip iddianame safhasında teşhir edilmesi oldukça düşündürücüdür. Suçlular yakalanmamak için telefonlar üzerinden şifreli konuşurken e-posta yazışmalarında şifreli metni farklı yollarla karşı tarafa iletmektedirler. Örneğin dijital watermark tekniği ile şifreli metin resim içerisine gizlenebilmektedir. Ayrıca küresel dinleme ve istihbarat ağları da mevcuttur. Bunların en ünlüsü ECHELON'dur.

ECHELON, UKUSA anlaşmasına dayalı bir istihbarat sinyalleri toplama ve analiz ağı işletimini açıklarken kullanılan isimdir.

Katılımcıların %60,9'u sosyal paylaşım sitelerinin ( FACEBOOK, TWITTER vb.) kişisel bilgileri ve fotoğrafları başka kişi ve şirketlerle/kurumlarla paylaştığı yönünde endişeleri olduğunu söylemiştir. Bilgi çağının yaşandığı günümüzde gerek istihbarat kuruluşları ve gerekse kötü amaçlı kişiler sosyal ağlar aracılığıyla kişilerin kendi kendilerini fişlemelerinden faydalanmaktadır. Özellikle Facebook gibi sosyal ağlarda kişilerin şahsi bilgilerine ve görüntülerine fazlasıyla yer vermeleri dolayısıyla birçok kullanılabilir veri ortaya çıkmaktadır. Bu veriler açık kaynak istihbaratı olarak kullanılmaktadır. Cep telefonlarımız rehberimizdeki kişi listesi ile sosyal paylaşım sitelerindeki arkadaş listesini senkronize edip eşleştirmektedir. Bu eşleşmenin sonucunda ve Facebook profil bilgileri ile birlikte bir kişinin telefon numarası, telefonu aracılığıyla bulunduğu konum, arkadaşları, mesleği ve ilgi alanları gibi bir çok bilgi elde edilebilir hale gelmiştir. Bu kadar güvenlik açıklarına rağmen Facebook sosyal ağının Eylül 2011 itibariyle 30,5 milyon Türk kullanıcı vardır. Bu rakam ile Türkiye Facebook'ta 4. sıradadır. İnsanların bu kadar endişeye rağmen özel hayatlarını tanımadığı kişilere ifşa etmesi toplum bilimciler açısından değerlendirilmesi gerek bir konudur.

Katılımcıların %40,06'sı mahkeme kararıyla içinde suç unsuru olduğu tespit edilen ve kapatılmasına karar verilen web sitelerine yapılan hukuki engellemelerin düşünce özgürlüğüne aykırı olduğunu düşünmektedir. İnternet üzerinden engelleme çözüm değildir. Çünkü birçok yolla yasaklanan sitelere erişilebilir. Örneğin DNS sunucusu adresi değiştirilerek Türkiye'de yasaklanan sitelere girilebilir. BTK'in "Güvenli İnternet Hizmeti" adını verdiği filtreleme uygulaması hizmete girmiş olmakla birlikte filtrelemenin hangi kriterlere göre olacağı tartışma konusu olmuştur. Çünkü uygulamanın kullanıcıları zararlı içeriklerden uzak tutarken belli bir ideolojiye aykırı olan siteleri yasaklaması söz konusu olabilir. Bu konunun internet özgürlüğü açısından tartışılması gerekir. Çünkü filtreleme devlet tarafından değil kullanıcıların kendileri tarafından belirlenmelidir. Örneğin çocuğunun porno içerikli sitelere girmesini engellemek isteyen ebeveynler basit filtreleme yazılımları ile bunu yapabilirler.

Katılımcıların %59,29'u 5464 numaralı Banka Kartları ve Kredi Kartları Kanunu gereği, yapacakları kayıp ya da çalıntı bildiriminden önceki yirmi dört saat içinde kartları ile gerçekleştirilen hukuka aykırı kullanımdan doğan zararlardan 150 TL ile sınırlı olmak üzere sorumlu olduklarını bilmemektedir. Kart başvurusu yapılırken imzalanan başvuru belgeleri içerisinde bu hususa yer verilmektedir.

Katılımcıların %47,76'sı kredi ve banka kartı kopyalama teknikleri hakkında bilgi sahibidir. Eğer ATM'den şüphelenildiyse süratle kolluk kuvvetlerine bildirilmelidir. Ayrıca kart işlemlerde POS makinesi iyice kontrol edilmeli eğer kontrol edilme mümkün olmuyorsa mobil POS terminaller aracılığıyla işlemin yakınızda yapılması sağlanmalıdır.

Katılımcıların %39'u internet üzerinde bankacılık ve alışveriş işlemlerinde kullanılan loadpowerprof.exe, keylogger.exe gibi programlarla yapılan işlemlerin takip edilebildiği ve JavaScript kodlarıyla yazılan sahte programlarla hedef bilgisayar kullanıcısın kişisel bilgilerine ulaşılabildiği hakkında bilgi sahibidir.

Katılımcıların %72,76'sı kendilerini kamu görevlisi olarak tanıtan veya ödül kazandığınızı belirterek para transferi talep ederek dolandırılabileceği konusunda

bilgi sahibidir. Bu konunun bu kadar bilinmesinin sebebi cep telefonlarına bu hususa dikkat edilmesi gerektiğini anlatan SMS gönderilmesidir. Ayrıca bu yöntemle ilgili televizyon kanallarında da birçok haber yapılmıştır.

Katılımcılara bilişim suçları tekniklerini biliyor musunuz sorusu sorulduğunda sırasıyla bilgisayar virüsleri (%83.33), hacking (%74.04) ve spam (%67.31) tekniklerini diğer tekniklere nazaran daha çok bilindiği sonucu çıkmıştır. Ayrıca mantık bombası (%54,81) ve oltalama (%49,04) en bilinmeyen teknikleridir. Bu tekniklerin bilinmemesinin sebebi mantık bombasının bir tür virüs olması ve aslında mantık bombası gibi çalışan zararlı yazılımlara genel olarak virüs denmesinden, oltalama yani phishing tekniğinin de sosyal mühendislik saldırıları içerisinde değerlendirilmesinden kaynaklanmaktadır.

Anketten çıkan en önemli sonuç bilişim suçları hakkında üniversitelerde ders ve seminer isteyen katılımcıların oranının %95,83 olmasıdır. Bilişim suçları konusunda bilinç kazandırma okullarda öncelikle üzerine düşülmesi gereken konulardan biridir. İlköğretimden itibaren öğrencilere bilgisayar eğitimi verilmeye başlandığına göre bu konular basitten zora doğru milli eğitim sistemi içerisinde öğrencilere aktarılmalıdır. Bilişim teknolojileri ile ilgili bölümlerde okumayan öğrencilerin bu konuda daha fazla bilgiye ihtiyacı olduğu unutulmamalıdır.

Güvenlik zincirindeki en zayıf halka insandır[27]. Dünya üzerindeki hiç bir kurum veya firma tamamen güvende değildir. Sistemlerini ne kadar güvenlik altına da alsalar, ne kadar gelişmiş yazılımlar ve eğitimli insanlar da kullansalar yine de savunmasız durumdadırlar. Çünkü bireyler tamamen savunmasızdır ve hata yapmaya açıktırlar. Ünlü bilim adamlarından Albert EİNSTEİN; “Yalnızca iki şey sonsuzdur, evren ve insanoğlunun aptallığı; aslında evrenin sonsuzluğundan o kadar da emin değilim.” sözüyle hata yapmaya ne kadar açık olduğumuz söylemiştir.

## 4.2. Kredi Kartı ve Banka Kartlarının Kötüye Kullanılması Suçunun Analizine İlişkin Ceza infaz kurumlarında Nitel Anket Çalışması

### 4.2.1. Araştırmanın çözümü

Anket yapılan her kişiye 1'den 27'ye kadar numaralar verilmiştir(R1,R2 vb.). Her kişinin her soruya verdiği cevap, gruplandırılmıştır. Örneğin; 27 kişinin 1. soruya verdiği cevap, 27 kişinin 2. soruya verdiği cevap v.b. Yapılan bu gruplamalardan sonra ankete verdikleri cevaplar soru başlıkları altında incelenmiştir. Yapılan incelemeden sonra tümevarım yöntemiyle 24 kişi için genellemeye gidilmiştir.

Hükümlülere kendi rızalarıyla ankete katılıp katılmadıkları sorulmuştur. Ankete 3 hükümlü katılmak istememiştir. 3 hükümlü ise soruları boş bıraktığından anket formları değerlendirmeye alınmamıştır. Ankete katılanlardan 3'ü kendilerine isnat edilen suçu kabul etmediklerinden ankete suçsuz olduğu yönünden cevaplar vermiş dolayısıyla kendilerinden suç işleme teknikleri ve suça iten sebepler konusunda istenilen cevaplar alınamamıştır. Ses kayıt cihazı kullanılamadığından anket dışında hükümlülerin belirttiği görüşler ayrıca belirtilecektir.

Çizelge 4.17.a. Katılımcıların demografik özellikleri

| Rumuz | Cinsiyet | Yaş | Eğitim Seviyesi | Meslek |
|---|---|---|---|---|
| R1 | Erkek | 18-30 | Lise | Yaya kurye |
| R2 | Erkek | 31-45 | İlköğretim | Çiçekçi |
| R3 | Erkek | 31-45 | Lise terk | Serbest meslek |
| R4 | Erkek | 46 üstü | Lise | Serbest meslek |
| R5 | Erkek | 18-30 | Lisans | Turizm işletmecisi |
| R6 | Erkek | 31-45 | İlköğretim | ***yanıt vermedi*** |
| R7 | Erkek | 18-30 | İlköğretim | Çiftçi |
| R8 | Erkek | 31-45 | Lise terk | Çay ocağı işletmecisi |
| R9 | Erkek | 31-45 | İlköğretim | Market sahibi |
| R10 | Erkek | 31-45 | Lisans | Biyolog |
| R11 | Erkek | 31-45 | İlköğretim | Esnaf( inşaat malzemeleri) |
| R12 | Erkek | 18-30 | Lise | Serbest meslek |
| R13 | Erkek | 18-30 | İlköğretim | İnşaat işçisi |
| R14 | Erkek | 31-45 | İlköğretim | Şoför |
| R15 | Erkek | 31-45 | Lise terk | Kafe işletmecisi |

| | | | | |
|---|---|---|---|---|
| R16 | Erkek | 31-45 | Lise | Sağlıkçı |
| R17 | Erkek | 46 üstü | Lise | Kunduracı |
| R18 | Erkek | 31-45 | Önlisans | Emlakçı |
| R19 | Erkek | 31-45 | İlköğretim | Marangoz |
| R20 | Erkek | 46 üstü | Lise | Sabun imalatçısı |
| R21 | Erkek | 18-30 | Lisans terk | ***yanıt vermedi*** |
| R22 | Erkek | 31-45 | Lise | İşmakinesioperatörü |
| R23 | Erkek | 31-45 | İlköğretim | Mermer ustası |
| R24 | Erkek | 31-45 | İlköğretim | Mobilya döşemecisi |
| R25 | Erkek | 31-45 | Lise | Elektronik teknisyeni |
| R26 | Erkek | 18-30 | İlköğretim | Sabun imalatçısı |
| R27 | Erkek | 31-45 | İlköğretim | İşsiz |

Çizelge 4.17.b. Katılımcıların demografik özellikleri

| Rumuz | Medeni Hali | Gelir (TL) | İkamet Yeri | Şehir |
|---|---|---|---|---|
| R1 | Evli(1 çocuk) | 0-1000 | Büyükşehir | Ankara |
| R2 | Evli | 2001-3000 | İlçe | Antalya |
| R3 | Evli(2 çocuklu) | 0-1000 | Büyükşehir | Ankara |
| R4 | Boşanmış(2 çocuklu) | 0-1000 | Büyükşehir | Ankara |
| R5 | Bekâr | 2001-3000 | Büyükşehir | Ankara |
| R6 | Bekâr | 750 | Büyükşehir | Ankara |
| R7 | Evli(2 çocuklu) | 800 | İlçe | Gaziantep |
| R8 | Boşanmış | 0-1000 | Büyükşehir | Ankara |
| R9 | Evli(4 çocuklu) | 3000+ | İlçe | Şanlıurfa |
| R10 | Boşanmış(1 çocuk) | 1001-2000 | Büyükşehir | Ankara |
| R11 | Evli | 3000+ | Büyükşehir | İstanbul |
| R12 | Bekâr | 0-1000 | Şehir | Van |
| R13 | Bekâr | 0-1000 | İlçe | Diyarbakır |
| R14 | Evli | 0-1000 | Köy | Ankara/ Hasanoğlan |
| R15 | Bekâr | 2001-3000 | Büyükşehir | Ankara |
| R16 | Evli | 0-1000 | Büyükşehir | Ankara |

| | | | | |
|---|---|---|---|---|
| R17 | Evli | 0-1000 | Büyükşehir | İstanbul |
| R18 | Bekâr | 2001-3000 | Büyükşehir | Almanya / Hamburg |
| R19 | Evli(3 çocuklu) | 0-1000 | İlçe | Gaziantep/Nizip |
| R20 | Evli(3 çocuklu) | 3000+ | İlçe | Gaziantep/Nizip |
| R21 | Bekâr | 1001-2000 | Büyükşehir | Ankara |
| R22 | Evli(2 çocuklu) | 3000+ | Büyükşehir | Ankara |
| R23 | Evli | 3000+ | Büyükşehir | Ankara |
| R24 | Evli | 0-1000 | Büyükşehir | Ankara |
| R25 | Bekâr | 1001-2000 | Büyükşehir | Ankara |
| R26 | Evli | 2001-3000 | İlçe | Gaziantep/Nizip |
| R27 | Bekâr | ***yanıt vermedi*** | Büyükşehir | Ankara |

Ankete katılan hükümlülerin hepsi erkektir. Katılımcıların 7'si (%25.92) 18-30 yaş aralığında, 17'si (%62.96) 31-45 yaş aralığında ve 3'ü (%11.1) 46 yaş üzerindedir. Katılımcıların 12'si (%44.4) ilköğretim mezunudur, 11'i (%40.74) lise mezunu ve lise öğrenimini yarıda bırakmıştır, 1'i (%3,7) önlisans mezunu, 3'ü (%11,1) lisans mezunu ve lisans eğitimini yarıda bırakmıştır.

Ankete katılan hükümlülerin 9'u (%33.3) bekar, 15'i (%55.5) evli ve 3'ü (%11.1) boşanmıştır. Evlilerden 7'sinin çocuğu ve boşananlardan 2'sinin çocuğu vardır.

Katılımcıların 13'ünün (%48.14) cezaevine girmeden önce aylık geliri 0–1000 TL. arasında, 3'ünün (%11.1) 1001–2000 TL. arasında, 5'inin (%18.51) 2001–3000 TL arasında ve 5'inin 3000 TL üzerindedir. Katılımcılardan 1'i cevap vermemiştir. Katılımcıların meslekleri Tablo 4.17'de gösterilmiştir. Katılımcılardan 2'si mesleğine cevap vermemiştir.

Katılımcılardan cezaevine girmeden önce 18'i (%66.6) büyükşehirde, 1'i (%3.7) şehirde, 7'si (%25.92) ilçede ve 1'i (%3.7) köyde ikamet etmektedir.

Katılımcıların bilgisayar kullanma seviyelerini öğrenmek ve suç işlerken bilgisayar kullanıp kullanmadıklarını tespit etmek maksadıyla katılımcılara **"Bilgisayar**

**kullanmayı biliyor musunuz? Kendinizi nasıl bir bilgisayar kullanıcısı olarak görürsünüz? Kaç yıldır bilgisayar kullanıyorsunuz?"** soruları yöneltilmiştir katılımcıların verdikleri cevaplar Tablo 4.19'da gösterilmiştir.

Çizelge 4.18. Bilgisayar kullanma seviyeleri

| Rumuz | Bilgisayar kullanımı | Bilgisayar Kullanma Düzeyi | Kaç Yıldır Bilgisayar Kullanıyor |
|---|---|---|---|
| R1 | Evet | alt düzeyde | 1-2 yıl |
| R2 | Hayır | ***yanıt vermedi*** | ***yanıt vermedi*** |
| R3 | Hayır | ***yanıt vermedi*** | ***yanıt vermedi*** |
| R4 | Hayır | ***yanıt vermedi*** | ***yanıt vermedi*** |
| R5 | Evet | orta düzey | 5 yıl + |
| R6 | Hayır | ***yanıt vermedi*** | kullanmıyorum |
| R7 | Hayır | ***yanıt vermedi*** | kullanmıyorum |
| R8 | Kısmen | alt düzeyde | 1-2 yıl |
| R9 | Hayır | alt düzeyde | 1-2 yıl |
| R10 | Evet | orta düzey | 5 yıl + |
| R11 | Kısmen | alt düzeyde | 1-2 yıl |
| R12 | Evet | orta düzey | 3-4 yıl |
| R13 | Hayır | alt düzeyde | kullanmıyorum |
| R14 | Hayır | ***yanıt vermedi*** | kullanmıyorum |
| R15 | Hayır | ***yanıt vermedi*** | kullanmıyorum |
| R16 | Evet | orta düzey | 3-4 yıl |
| R17 | Hayır | ***yanıt vermedi*** | kullanmıyorum |
| R18 | Evet | orta düzey | 5 yıl + |
| R19 | Hayır | alt düzeyde | kullanmıyorum |
| R20 | Hayır | ***yanıt vermedi*** | kullanmıyorum |
| R21 | Evet | profesyonel düzeyde | 5 yıl + |
| R22 | Evet | orta düzey | 5 yıl + |
| R23 | Hayır | ***yanıt vermedi*** | kullanmıyorum |

| | | | |
|---|---|---|---|
| R24 | Kısmen | orta düzey | 1-2 yıl |
| R25 | Evet | alt düzeyde | 1-2 yıl |
| R26 | Evet | orta düzey | 1-2 yıl |
| R27 | Evet | alt düzeyde | 1-2 yıl |

Katılımcıların 11'i (%40.74) bilgisayar kullandığını, 13'ü (%48.14) bilgisayar kullanmadığını, 3'ü (%11.1) kısmen kullandığı cevabını vermiştir.

Katılımcılardan 1'i (%3.07) profesyonel düzeyde, 8'i (%29.62) orta düzeyde, 8'i (%29.62) alt düzeyde, 10'u (%37.03) ise yanıt vermemiştir. Yanıt vermeyenlerin tamamının bilgisayar kullanmadığı görülmüştür.

Katılımcıların 5'i (%18.51) 5 yıl ve daha fazla süre bilgisayar kullandığını, 2'si (%7.4) 3-4 yıl süre ile kullandığını, 8'i (%29.62) 1-2 yıl süre ile bilgisayar kullandığını ve 12'si (%44.4) yanıt vermemiştir veya kullanmadığını söylemiştir.

Katılımcılara **"Suç işlerken bilgisayar, bilgisayar teknolojileri veya herhangi bir teknolojik araçtan faydalandınız mı?"** sorusu sorulduğunda R5 suçu internet üzerinden işlediğini söylemiştir. R9 pos cihazı kullandığını fakat yaptığını suç olduğunu bilmediğini söylemiştir. R21 ise işlediği suçun altyapısının bilgisayar programlarına dayandığını belirtmiştir. R27 ise bankamatik üzerine düzenek takarak suçu işlediğini söylemiştir. Diğer katılımcılar bilgisayar teknolojilerinden faydalanmadığını belirtmişlerdir.

Katılımcılara yöneltilen **"Suç işlerken, bilişim suçlarının tespitinin zor olacağını düşünüp rahat davranır mısınız?"** sorusunaR27 "Tespiti zor yakalanmam diye düşündüm." yanıtını vermiştir. R23 ise "Yakalanma kesinlikle söz konusuydu bilerek bu işe girdim." cevabını vermiştir. R6 ve R16 suçu işlediklerinden pişman olduklarını söylemiştir. Katılımcıların 17'si hayır rahat davranmadım yanıtını vermiştir. Anketin uygulanması esnasında hükümlülerin kendi aralarında "Biz ayak takımıyız asıl bu işi ustaca yapanlar dışarıda." ve "Zaten bu konuda iyi olsaydım yakalanmazdım, arkadaşlarımdan daha yakalanmayanlar var." dedikleri tespit edilmiştir.

Katılımcılara **“Suçu işleme sürecini nasıl planlıyorsunuz?”** sorusu sorulduğunda

R5 ise “kara düzen, plan yok iyi işlemiş olsak buraya düşmezdik.” ,

R8 “çok kısa süre işlediğim suça iştirak ettim planlama sürecini merak etmedim.”

R15 ise “ilk suçum ve teşebbüs olduğundan plansızdır.”

R23 “ TC kimlik numarasını öğrendikten sonra nasıl nüfus cüzdanı çıkartılır ve bankaya gittiğimde kredi başvurusu esnasında hangi sorular sorulacak konusunda araştırma yaptım.”

R24 “Suç işlerken plan yapmadım yaptığımın bu kadar ağır bir bedelinin olduğunu da bilmiyordum.”.

R25 “Paraya ne zaman ihtiyacım olsa rahatlıkla yapıyorum.”

R26 “Suç işlemedim esnafın yapması gereken her şeyi yaptım.” cevabını vermişledir.5 kişi bu soruya cevap vermemiştir.15 kişi ise herhangi bir planlarının olmadığını söylemiştir.

Katılımcılara **“Bugüne kadar bilişim suçu işleyen arkadaş ve aile çevrenizden herhangi birisi var mıdır? Yakalandı mı?”** sorusuna 8 kişi bu suçu işleyen arkadaşlarının olduğu; R6, R8, R15, R22 ve R27 arkadaşlarının yakalandığını R15 ise yakalan arkadaşının şuan cezaevinde olduğunu söylemiştir. 13 hükümlü ise bu suçu işleyen arkadaşının olmadığını söylemiştir.

Katılımcılara **“Başkasına ait kredi kartını nasıl ele geçirirsiniz veya kopyalarsınız? Suçu hangi şekilde işlediniz?”** sorusuna

R1 “Kartı başkasından aldım, çalınmış karttı. Çalınan kartla alışveriş yaparken yakalandım. Kopyala yapmadım. Bilmiyorum.”

R3 “Şahsen yapmasını bilmiyorum. Bilen biriyle yaptım. Arkadaşımla birlikte yakalandım”

R8 “ATM’ye düzenek kurarak şifresini öğrendim. Karı sıkıştırıp para çektim. Kopyalama yapmadım.”

R10 “Birlikte yaşadığım bayan arkadaşımın kredi kartlarını kendisinden habersiz kullandım.”

R12 “Kuryeden kartı ele geçirdim.”

R14 “Arkadaşım tanıdığı birinin dükkânına giderek onun başka bir odaya geçmesinden faydalanarak ceketinin cebinden cüzdanını alıp bana bulduğunu söyledi beraber parayı ATM’den çektik.”

R15 “ATM yolu ile işlemeye çalışsam da vicdanım el vermedi yapamadım suç işleyenlerle aynı ortamda bulunmak zorunda kaldım. Suça ortak olmuş oldum.”

R16 “Maktulun cüzdanından aldım ve sıkıntıda olduğum için ATM’den çektim.”

R17 “Bilmeyerek müşteri şeklinde gelen kişiler tarafından dolandırıldım.”, R18 “Kopyalanmış kartları başka bir şahıstan aldım kartlar üzerimde yakalandı.”

R19 “Dükkânımdaki pos makinesinden çekilmiş.”

R21 “Kredi kartı bilgisi tutan sistemleri hackleyerek bu sistemlerden alınan bilgileri mail order kullanarak para çekiyordum.”

R22 “ATM'de kart sıkıştırma yöntemiyle başkasına ait kredi ve banka kartlarını alıyoruz.”

R23 “Bankalar rahatlıkla kredi kartı veriyor. Herhangi bir bankamatikten işini halledebilirisin.”

R24 “Ben sadece kullandım nasıl kopyalanır hiç bilmem.”

R26 “İşyerime geldiler alış veriş yapıp beni dolandırdılar.”

R27 “bankamatiklerde düzenek kurarak kartın makinede sıkışmasını sağlayıp şifreyi öğrenerek ele geçirdim.” demiştir. R2, R4, R6, R7, R8, R20 ve R24 bu konuda yeteri kadar bilgi sahibi olmadıklarını belirtmişlerdir. 4 kişi suçu nasıl işlediğine dair herhangi bir açıklamada bulunmamıştır.

Katılımcılara yöneltilen **“Sizi suç işlemeye iten sebepler nedir? Niçin bu yolu-suçu tercih ettiniz?”** sorusuna

R1, R3, R5 maddi sıkıntılar yüzünden bu suça bulaştığını söylemiştir.

R4: “ Esnafım, battım. Zor durumdaydım bu yüzden suç işledim.”

R7: “ Suça iten bir sebep yok.”

R8: “Ekonomik kriz yüzünden oldu. Resmi devlet dairesinde çay ocağı işletirdim. Çayı çok ucuza satardık iflas ettim. Bu işlerle uğraşan arkadaşım vardı onunla irtibata geçtim.”

R9: "Bana suç atıldı. Suça itilmiş değilim”

R10: “Elbette ekonomik sıkıntı yüzünden ama birlikte yaşadığım insanın kartını kullanmanın suç olduğunu düşünmüyorum. Benden şikayetçi oldu.”

R11: “Dükkânımdan sahte kartla alışveriş yapılmış. Benim maddi durumum iyi böyle işlerle alakam yok.”

R12: “Bir yıldır işsizim. Profesyonel değilimdir bu konulara da. Rahatça yapılabildiği için bu yola düştüm.”

R13: “Yanlış arkadaş seçimi. Beni bu suçun içine attılar.

R14: “İşsizim, ev kirasını ödemek için yaptım.”

R15: “Aslında suçu işlememi gerektiren bir durum olmadığı gibi maddi olarak da bir sıkıntım yok. Bu işi yapan insanların yanında bulundum.”

R16: “Maddi yönden sıkıntıdaydım kiramı ödeyemiyordum.”

R17: “Esnaf olarak bu konu hakkında yeteri kadar bilgim yok Dükkânımdan sahte kart kullanılmış.”

R18: “Türkiye’de mahsur kaldım uçak bileti için yaptım.”

R19: “Suç olduğunu bilmiyordum arkadaş çevrem ve maddi imkânsızlılar yüzünden oldu.”

R21: “Merak yüzünden.”

R22: “Ailemi geçindirmek için yaptım. Eski bir sabıkalı olduğumdan iş bulamadım. İki kızımı okutmak için yaptım.”

R23: “20 yıllık evliydim daha sonra ayrıldım. Ayrıldıktan sonra bu işe düştüm. İşsizlik ve ailevi, sorunlar yüzünden bu işe bulaştım.”

R24: “Önceden esnaftım çok borcum vardı. Biri ile tanıştım bana nasıl yapacağımı anlattı. Çok sıkıştığım için kabul ettim.”

R25: “Kumar ve uyuşturucu yüzünden.”

R26: “Benim bu tür işlere ihtiyacım yok maddi durumum çok iyi. Ailem maddi olarak çok iyi.”

R27: “İşsizlik ve bu suçu kolay öğrendiğimden.”diyerek cevaplamıştır. R2 suç işlemediğini belirtmiştir. R20 bu soruyu cevaplamamıştır.

Katılımcılara yöneltilen **“Kredi kartlarına getirilen şifre uygulaması, son dönemlerde artan dolandırıcılık vakalarına çözüm sağladı. Şifreli çipli kart (CHİP&PİN) sistemi suç işlemenizi zorlaştırdı mı?”** sorusuna

R1: “Kredi kartı kullanmadığı için bilgim yok.”

R2, R3, R4, R5, R11, R13 ve R26 bu soruya cevap vermemişlerdir.

R6: “ Bilgisayar ve çipli kart kullanmadığımdan sıkıntım yok.”

R7: “ Kullanmadığım için bilgim yok.”

R8: “Kimsenin kartıyla şifresiyle işim olmaz ben dersimi aldım.”

R9: “ Bilgim yok anlamam.”

R10: “Sevgilimin kartı olduğu için şifresini rahatlıkla öğrendim.”

R12: “Kartlar şifresiz olduğu için sorun olmadı.”

R14: “Bana kartları getiren şifresini de öğrenmişti.”

R15: “Pek bilgim yok.”

R16: “Cüzdanından kartını aldığım kişinin ehliyetinden doğum tarihini öğrendim ATM’den denedim doğrulayınca 1000 TL çektim.”

R17: “Önce esnaf bilgilendirilmeli eğitimsiz toplum bitmiş toplumdur.”

R18: “ Bilgim yok.”

R19: “Hiçbir bankanın kredi kartını kullanmadım. Dükkânımdan sahte kart kullananlar şifresini de biliyorlardı.”

R20: “Ben kart kopyalamadan anlamam. Tutuklandıktan sonra böyle bir konuyu öğrendim.”

R21: “Mail order yöntemini kullandığımdan PİN sorgusu gerekmez.”

R22: “PİN sorgusu hiç de zor olmuyor. Şifreyi ATM'ye kurduğum telefon düzeneği ile alıyoruz..”

R23: “Şifre işi hiç zorlaştırmadı aksine daha kolay oldu.”

R24 ve R27 bu soruya “Bilmiyorum.” yanıtını vermiştir.

R25: “Buraya İstanbul metris cezaevinden geldim. Bulgarların çipli kart sistemini çözdüğü söyleniyordu.” cevabını vermişlerdir.

Katılımcılara yöneltilen **“Kredi kartı sahteciliği teknik olarak zordur. Manyetik bilgilerin kopyalanması bir takım aletleri gerektirir. Bu bilginizi nasıl elde ettiniz?”** Bilgilerinizi başkalarıyla paylaştınız mı?” sorusuna

R14: “ Ben bilmiyordum. Suçu beraber işlediğim arkadaşım biliyordu.”

R17: “İnsanlar kendilerini bu konuda eğitiyor ve bunu uyguluyor gerçek suçlular etrafta ellerini kollarını sallayarak geziyor.”

R21: “Kopyalama hakkında bilgim var fakat hiç denemedim.”

R23: “Manyetik bilgileri bilmem. TC kimlik numarası yeterli.”

R25: “Bulgarlar ile bilgi alış verişi yapıyordum.” cevabını vermişlerdir. 9 hükümlü soruyu cevaplamazken diğer hükümlüler ise bilgi sahibi olmadıklarını söylemiştir.

### 4.2.2. Araştırmanın bulguları

Anketin sonuçlarına bakıldığında hükümlülerin bir kısmının detaylı cevap vermekten kaçındığı görülmüştür. 3 kişi bu suçu işlediğini kabul etmediğinden verdikleri yanıtlar ile herhangi bir değerlendirme yapılamamıştır. Hükümlülerin ayrıntılı cevap vermek istemeyişlerin bir sebebi de verdikleri bilgilerin aleyhlerinde kullanılmayacağından emin olamamalarıdır. Hükümlülere özellikle kimliklerini doğrudan tespite yönelik demografik özelliklerini belirleyici soru sorulmaktan uzak durulmuş böylelikle rahat bir şekilde anketi çözmeleri hedeflenmiştir.

Katılımcıların %62.96’sinin 31–45 yaş aralığında olduğunu ve bunların %48.14’ünün cezaevine girmeden önce aylık geliri 1000 TL’nin altında olduğu görülmüştür.

Kredi kartı sahteciliği ve dolandırıcılığı üst düzey bilgisayar kullanımını gerektirmez. İkinci bölümde bu suç tekniğinin nasıl olduğu açıklanmıştır. Anket formundaki teknik sorular hükümlüler içerisinde teknik bilgi sahibi olanların tespitine yöneliktir.

Anketi cevaplayan hükümlüleri üç grupta incelemek gerekir. Bunlar suçu profesyonel bir şekilde işleyenler, arkadaşlarının yardımı veya basit dolandırıcılık yöntemlerini kullananlar ve işyerindeki POS terminalini kullandırmak suretiyle suçun işlenmesine yardımcı olanlardır.

Bilişim suçlarının tespiti zor olduğundan katılımcılara suç işlerken rahat davranışlarda bulup bulunmadıkları ve yakalanma ihtimaline yönelik önlemleri sorulduğunda yalnızca bir hükümlü (R27) rahat davrandığını söylemiştir. Görülüyor ki hükümlülerin bu suça yönelmeden önce yakalanma endişesi içinde oldukları sonucuna varılmıştır. Bu sonuç kolluk kuvvetlerinin suçun tespitine yönelik tecrübesinin artmasına ve uzman kadroların yetişmesine bağlanabilir. Son zamanlarda polis ve jandarmanın uluslararası işbirliği içinde yürütmüş olduğu başarılı operasyonların da etkisi vardır.

Hükümlülere suçu planlama süreci sorulduğunda ayrıntılı planlama yapmalarına gerek olmadığı görülmüştür. Hatta hükümlülerden biri (R25) ihtiyacı olduğu her zaman yapabildiğini söylemiştir. Sonuçlardan da anlaşıldığı üzere ayrıntılı planlama ve hesaplamaya gerek yoktur görüşü ağırlık kazanmıştır. Kredi kartı dolandırıcılığı nitelikli dolandırıcılık suçuna benzerlik gösterdiği için diğer bilişim suçlarına göre farklılık gösterir. Aslında planlama olmadan bu suçu işlemek zordur. ATM'de düzenek kurarken yakalanma ihtimaline karşın alternatif planlar yapmayı gerektirir. Bir bilgisayar korsanı hedef bilgisayara saldırırken yakalanmamak için kendini gizleyici önlemler alır. Örneğin görev çubuğunda gözükmemek, sistem kayıtlarını temizlemek vb.

Hükümlülerin bu suçu nasıl işlediklerine bakıldığında klasik hırsızlık yöntemiyle ele geçirip şifresini denemekten, internet ortamında mail order sistemini kullanmaya kadar çeşitli yöntemler kullanılmıştır. 3 kişinin kart sıkıştırma yöntemini kullandığı görülmüştür. Kart sıkıştırma yöntemini kullananlardan birinin ATM'ye sahte müşteri

hizmetleri telefon hattı da kurduğu anket sonrası yapılan görüşmede tespit edilmiştir. Dükkânında sahte olarak hazırlanmış kartları kullandıran hükümlüler suçsuz olduklarını anket formunun sonuna yazarak ayrıca belirtmişlerdir. İşyerinde POS terminalini, kart sahibinin rızası olmaksızın kullandırtanlar da TCK'nın 245.maddesine göre suçlu durumuna düşmektedirler. R10 rumuzlu hükümlü bayan arkadaşının kartının şifresini bildiğini ve bu kartla alışveriş yaptığını daha sonra arkadaşından ayrılınca şikâyet üzerine tutuklandığını söylemiştir. TCK'nın 245.maddesine göre "Suçun haklarında ayrılık kararı verilmemiş eşlerden birinin, üstsoy veya altsoyunun veya bu derecede kayın hısımlarından birinin veya evlat edinen veya evlâtlığın, aynı konutta yaşayan kardeşlerden birinin zararına ait olarak işlenmesi hâlinde, ilgili akraba hakkında cezaya hükmolunmaz."

R23 bankaların rahatlıkla kart verdiğini söylemiştir. Bankaların müşterilerini kredi kartı sahibi yapmak için düşük gelir grubunda olan insanlara yüksek limitli kartlar verdiği bilinmektedir. Hatta kişilerin çalıştığı kurumlardan alabilecekleri maaş bordrolarında maaşlarını yüksek gösterebilmeleri halinde yüksek limitli kredi kartı verebilecekleri yönünde müşteri temsilcilerinin sahteciliğe teşvik oldukları bilinmektedir.

Hükümlülerin kendi aralarında bir hükümlüye "hocam" diye hitap ettiği tespit edilmiştir. "Hocam" diye hitap edilen hükümlüyle yapılan sohbetle ATM'ye kurulan düzenekler hakkında Emniyet Müdürlüğüne meslek içi eğitim kapsamında eğitim verdiği için hoca denildiği anlaşılmıştır. Suçun önlenmesi ve tespiti için bu konudaki profesyonel bilgi sahibi suçluları kullanmak istihbarat ve emniyet birimlerinin başvurduğu yöntemlerden biridir. Hatta şirketler ve bankalar kendi sistemlerinin açıklarını tespit etme için hackerlara saldırılar düzenlettiği bilinmektedir.

Sahte nüfus cüzdanı ile banka hesabı açarak haksız kazanç sağlayan hükümlünün bu suçu çok rahatlıkla işleyebilmesi sitemde çok büyük bir açıklık olduğunu göstermektedir. Ayrıca sahte kimlikle cep telefonu hattının iptal edilip kart sahibinin hesap hareketlerinden haberdar olmasının önlenmesi de bu suçla birlikte işlenebilecek bir suç tekniğidir. Hem nüfus müdürlükleri hem bankalar hem de GSM operatörleri bu konuda ciddi önlemler almalıdırlar.

Katılımcıların 14'ünün bu suçu işleyen arkadaşlarının olduğu ve 5'inin arkadaşların yakalandığı cevabı vermesi bu suçun organize hareket ve bilgi paylaşımı gerektirdiğini ortaya koymuştur.

Suçu hangi sebeplerden ötürü işledikleri sorulduğunda çoğunlukla maddi sıkıntılar yüzünden işlediklerini söylemiştir. Sadece R21 rumuzlu hükümlü merak yüzünden işlediğini söylemiştir. R27 ise bu suçu kolay öğrendiğinden dolayı işlediğini söylemiştir. Yüksek kazancın kolay ve risksiz bir şekilde elde edilmesi işsiz olan ve geçim sıkıntısı çeken insanları bu yöntemlere itmiştir. Bu soruya hükümlülerden pişman olduklarını belirtenler de bulunmaktadır.

Şifreli kart uygulamasıyla birlikte dolandırıcılar yeni teknikler uygulama yoluna gitmiştir. Kart kopyalandıktan sonra şifrenin tespiti gerekmektedir. Örneğin R22 şifreyi ATM'ye kurduğu telefon düzeneği ile öğrenmektedir. R23 ise şifre uygulamasın dolandırmayı daha da kolaylaştırdığını söylemiştir. R16 ise çaldığı kartın şifresini çaldığı kişinin doğum tarihi olarak denemiş ve başarılı olunca hesaptan para çekmiştir. Kartlarda şifre uygulaması kartları tamamen güvenli hale sokmaz. Tahmin edilmesi güç şifreler belirlenmelidir. Şifre, TC kimlik numarası, anne kızlık soyadı gibi özel bilgiler kesinlikle paylaşılmamalıdır. Hiçbir müşteri hizmetleri çalışanı bu bilgilerin hepsini sizden istemez. Örneğin, annenizin kızlık soyadının birkaç hanesini isterler. Şifrenizi de asla istemezler.

Manyetik kart kopyalama hakkında hükümlülerin bilgi sahibi olmadıkları, bir kişinin bildiği, bir kişinin de Bulgar dolandırıcıların bu tekniği kullandığını ve bilgileri paylaştığını söylemişleridir. Saldırganlar kartları kopyalayıp ekonomik sıkıntı çeken insanlara bu kartları satmadıktadırlar. Kendiler bu sahte kartları kullanmadıklarından yakalanmazken bu kartları kullanan ve üzerinde bulunduranlar rahatlıkla yakalanmaktadır. Asıl suçlulara yakalanan basit dolandırıcılar aracılığıyla ulaşılmaya çalışılsa da asıl suçlular yakalanmadan suç işlemeye devam etmektedir. Hatta hükümlülerden biri "Biz ayak takımıyız asıl suçlular dışarıda." diyerek bu konuyu en güzel şekilde özetlemiştir.

# 5. SONUÇ VE ÖNERİLER

Bilgi çağı olan günümüzde etkili ve yaygın kullanım alanıyla İnternet dünya üzerinde milyarlarca insana hizmet vermekte, İnternet ve teknolojinin sunduğu diğer haberleşme alt yapılarını kullanan cihazlar vasıtasıyla, sağlık hizmetlerinden bankacılık ve sigorta işlemlerine, alışverişten vergi ödemeye kadar birçok alanda insanlar bu platformlardan faydalanmaktadırlar. Dünyayı bir örümcek ağı gibi saran bu devasa haberleşme ağı, ulusal ve uluslararası ticari ya da resmi kurum ve kuruluşları birbirine bağlamakta, ticari ve sosyal bağlar bu sistemler üzerinde kurulup işletilmektedir.

Siber orduların kurulduğu, iletişim alt yapılarının çok uluslu güçler tarafından yönetildiği, uydu ağlarının dünyayı kuşattığı günümüzde, ihtiyaç olarak ortaya çıkan bu sistemler aynı zamanda sahip olan devletlere stratejik güç kazandırmıştır. Türkiye coğrafi konumu itibariyle Asya ile Avrupa arasında klasik anlamda ticaret yolu olmasının yanı sıra aynı zamanda internet omurgasının üzerinden geçtiği bir veri köprüsü durumundadır. Bu veri köprüsünün güvenliği devletin sağladığı koruma tedbirlerine ilave olarak yaygın sorumluluk anlayışı içerisinde gerek vatandaşlar tarafından bilinçlenmek suretiyle gerekse bilişim şirketleri tarafından kullanıcıları bilgilendirmek ve imkânları ölçüsünde güvenlik tedbirlerini almak suretiyle sahip çıkılıp korunmak zorundadır. Sağladığı kolaylık ve iletişim imkânları sayesinde ulaştığımız refah seviyesini sürdürebilmek adına, içinde bulunduğumuz teknoloji çağında yaşantımızın vazgeçilmezleri arasında yerini almış olan bilişim sistemlerine sahip çıkmak ve korumak için her türlü tedbiri almak durumundayız.

Bilişim suçları ve alınabilecek tedbirler hususunda toplumumuzdaki farkındalık düzeyini araştırarak sonuçlarını ortaya koyan çalışmamda farklı kesimlerinden insanlara anketler uygulanmıştır. Bu kapsamda, Türkiye'de bilişim suçlarına yönelik üniversite lisans öğrencilerinin görüşlerine baktığımızda üniversite öğrencilerinin bilişim suçlarına yönelik farkındalıklarının yüksek olduğu görülmüştür. Bunun en büyük sebebi anket uygulanan öğrencilerin BÖTE bölümü öğrencileri olmasıdır. BÖTE bölümü öğrencilerinin mezun oldukları bölümün temel amacı, bilgisayar öğretmeni ve bilgisayar destekli öğretim uzmanları yetiştirmektir. Öğrenciler mezun

olduklarında görev yapacakları özel veya kamu öğretim kurumlarında bilgisayar okuryazarlığı derslerini gerekli materyalleriyle birlikte planlayıp verebilme imkânına sahip olacaklardır. Görev alacakları her tür kurumda bilgisayar destekli öğretim çalışmalarını başlatıp yürütebilme, eğitim yazılımı geliştirebilme ve bu süreçte hem öğretim tasarımı yapabilme hem de gerekli programları yazma ve programlama dillerini kullanabilme niteliklerine sahip olarak mezun olmayı amaçlamaktadır. Bu açıdan bakıldığında sonuçların istenilen şekilde olması eğitim sistemimiz açısından mutluluk vericidir. Öğrencilerin bilişim suçları konusunda bilgi düzeylerinin yüksek olduğu gözlemlenmesine rağmen birtakım teknik konularda eksik oldukları da ortaya çıkmıştır.

Öğrencilerin %74,68'i evlerinden internete bağlanmaktadırlar. Ülkemizde hanelerin %39,3'ünün geniş bant internet bağlantısına sahip olduğu günümüzde; ev kullanıcılarının güvenli bağlantıya sahip olmaları ile bilgisayarlarında lisanslı ve güncel yazılım bulundurmaları hususları gibi güvenliğe yönelik konular en az ticari amaçlara hizmet eden kurum ve kuruluşların bilgisayar sistemlerindeki kadar önemlidir. Çünkü insanlar artık evlerini "ev-işyeri" (homeoffice) olarak kullanmaktadırlar.

Ankete katılanların %76,92'si şifre ve parolalarını sıklıkla değiştirmemektedir. Parolamız başkaları tarafından öğrenildiğinde ister ticari ister sosyal amaçlı olsun hangi sistemi kullanırsak kullanalım maddi ve manevi zararlara uğrayacağımız açıktır. Bu hususta, özellikle sistem yöneticilerinin, parola güvenliği ile kullanıcıları parola değiştirmeye zorlama konularında yöntemler geliştirmeleri önem arz etmektedir.

Ankete katılanların %40,06'sı internet üzerinden alışveriş yapmaktadır. İnternet üzerinden yapılan alışveriş her ne kadar internet site yöneticilerinin geliştirmiş olduğu politikalarla güvence altına alınmış gibi gözükse de, bu alışveriş sisteminde hem karşılıklı güven hem de alışveriş yapılan sistemin güvenliği önem kazanmaktadır. Çünkü kimlik ve banka bilgileri sistem üzerinden işlem görmekte; ortada olmayan ürün henüz kullanıcıya ulaşmadan paralar transfer edilmektedir.

Öğrencilerin % 58,65'i lisanslı işletim sistemi kullanmaktadır. Bu rakamın oldukça düşük olması vahim bir tablo oluşturmaktadır. Güncel güvenlik yamaları yapılamadığından, lisanslı olmayan işletim sistemleri saldırıların hedefi haline gelmektedir. Ancak, güncelleme zorunluluğu işletim sistemi üreten firmayı tekel haline getirmiştir. Lisanlı yazılım kullanma zorunluluğu söz konusu işletim sistemlerine kullanıcı alışkanlığı sağlamasına rağmen, işletim sistemi üreten firmalara maddi bağımlılığa da sebep olmaktadır. Ücretsiz ve kullanım kolaylığı olan işletim sistemleri yaygınlaştırılmalı ve kullanımı küçük yaştan itibaren eğitim müfredatları içine dâhil edilmelidir.

Öğrencilerin %24.68'si gerekli bilgiye sahip olsa hackerlık yapabileceğini söylemiştir. TUİK'in verilerine göre bilişim suçları daha çok erkekler tarafından işlemektedirler. (Bknz. Çizelge 2.1) Ayrıca, bu suçu en fazla ilkokul mezunlarının işlediği görülmüştür. (Bknz. Çizelge 2.2.) Verilerin bu şekilde olması öğrencilerin merak duyguları ve kendini ispatlama dürtüsüyle hareket ettiklerini göstermektedir. Aslında veriler başka bir duruma işaret etmektedir. Suçlular genellikle 25–34 yaş arası, ilkokul mezunu ve işsiz kimselerdir. Hükümlülere uygulanan ankette görüldüğü üzere (Bknz. Tablo 4.17.a) iyi eğitim almış gençler bilişim suçluları profilinde yer almamaktadır. Yalnız gözden kaçırılmaması gerek en önemli husus TCK m.245 kredi ve banka kartlarının kötüye kullanılması suçu bilişim suçları kapsamında değerlendirildiğinden ve bilişim suçundan en fazla işlenen suçun bu maddenden olması suçlu profilinde değişikliklere sebep olmuştur. Ceza mahkemelerinde bilişim suçları ile ilgili en çok dosya banka ve kredi kartı sahteciliği ve dolandırıcılığı suçundandır[72]. Adalet Bakanlığı'ndan alınan veriler bize geçmişte başlayıp da karara bağlanabilmiş davaların sonuçlarını göstermektedir. Fakat hala karara bağlanamayan ve davanın hem davacı hem de davalılarını mağdur durumuna sokan yüzlerce dosya hala aydınlatılmayı beklemektedir.

İnternet vasıtasıyla genel ahlak kurallarına ters düşen yayınlar çocukların ve gençlerin fiziksel, zihinsel, ruhsal ve ahlaki gelişimini olumsuz yönde etkilemektedir. Buna rağmen, öğrencilerin %40,06'sı mahkeme kararıyla içinde suç unsuru olduğu tespit edilen ve kapatılmasına karar verilen web sitelerine yapılan hukuki

engellemelerin düşünce özgürlüğüne aykırı olduğu görüşündedir. Özgürlükler alanı olan İnternet ortamında fikir, sanat ve düşünceler engellenmemelidir. Devlet aleyhine yayın yapan siteler ve çocukların ruh ve zihin gelişimine karşı zararlı olan siteler elbette yasaklanmalıdır, ancak bu işlem devlet eliyle değil bilinçli bireylerin uyguladıkları filtreleme seçenekleri veya servis sağlayıcıların sunduğu güvenlik paketleriyle sağlanmalıdır. Toplumu ayakta tutan geleneksel değerlere, ahlak ve adalet anlayışına ve ülke güvenliğine aykırı yayınların düşünce özgürlüğü kapsamında değerlendirilip değerlendirilmemesi kamu vicdanınca sorgulanmalıdır.

Öğrencilerin %47,76'sı bankamatiklerden (ATM) banka veya kredi kartınızla işlem yaparken sahte klavye, kartın manyetik şerit bilgisinin kopyalanması gibi yöntemlerle banka hesaplarından para çekilebileceği konusunda bilgi sahibidir. Bu oranın yüksek olmasına karşın ülkemizde en çok işlenen bilişim suçu kredi ve banka kartları sahteciliği ile dolandırıcılığı olmuştur. Cezaevinde hükümlülere uygulanan ankette de görüldüğü gibi, suçlular kopyalama tekniklerini bilmeseler dahi çalıntı ve kopya kartları rahatlıkla elde etmişlerdir. PIN kullanımı başlamadan önce, kredi kartları ödeme işlemleri kartın arkasında bulunan manyetik şerit üzerinden yapılmaktaydı. Manyetik şerit kullanımında kredi kartı ile ilgili tüm işlem sorumluluğu, satışı gerçekleştiren kişi/firmaya aittir. Satıcının kredi kartı ile işlem yapmadan önce kredi kartı sahibinin doğruluğunu kontrol etme mecburiyeti vardır. Bu doğrulamada satış yapan firma yetkilisinin, kredi kartı üzerinde yazan isim ile kişinin nüfus cüzdanındaki bilgileri kontrol ettikten sonra, POS cihazından çıkan fişe atılan imza ile kredi kartı arkasında bulunan imzayı karşılaştırması gerekmektedir. Ülkemizde genel olarak işyerlerinde yapılan hata, kredi kartı işlemi yapıldıktan sonra hiçbir bilgi kontrolü yapılmadan işlemin tamamlanmasıdır. Manyetik şerit, çok eski bir teknoloji olduğundan geliştirilememekte ve kopyalanabilmektedir. Bu durumu engellemek için BKM Chip&Pin denen teknolojinin kullanımına geçmiştir. Chip&Pin kullanımına geçiş yapıldıktan sonra kredi kartından yapılan işlemlerin sorumluluğu, işyerlerinden kart kullanıcılarına geçmiştir. Kartınızın şifresinin(PIN), başka birine söylemeyeceğiniz şahsınıza ait bir bilgi olduğu düşünüldüğünden, o işlemi %100 kredi kartı sahibinin yaptığı varsayılarak sorumluluk tamamen kart sahibine bırakılmıştır. Bu durum, sahibine ait olan kredi kartı ile yapılan tüm işlemler

doğrudur, işleme değil sadece işlem tutarına itiraz edebilirsiniz anlamına gelmektedir. PIN uygulaması her ne kadar güvenli gözükse de hükümlülere uygulanan ankette anlaşıldığı üzere artık suçlular şifreyi öğrenmeye yönelik taktikler geliştirmektedirler. Hatta R23 rumuzlu hükümlünün "Şifre, işi hiç zorlaştırmadı aksine daha kolay oldu." cevabı oldukça ürkütücüdür. ATM kopyalama düzenekleri, sahte müşteri hatları ve sahte POS makinelerinin kullanım amacı kartı kopyalama ve PIN bilgisini öğrenmeye yöneliktir. Bankaların biometrik güvenlik sistemlerinin uygulanmasına yönelik yatırım yapmaları gerekmektedir. Retina tarayıcılar, parmak izi okuyucuları, ses algılayıcıları, imza tanıyıcılar, el geometrisi ve yüz tanıyıcılar gibi kişiye özgü ve taklit edilemez fiziki özelliklerin banka işlemleri ve e-devlet projelerinin vazgeçilmez güvenlik koşulu olarak değerlendirilmesi gerekmektedir.

Bilişim suçları ile ilgili başka bir konuda bu suçların tespitinde kullanılan adli bilişim yöntemleridir. Adli bilişim uzmanları bilişim sistemi içerisinde işlenen suçlarla ilgili elektronik delil araştırırken, delilin elde etmeleri ve buna bağlı olarak dava açabilmeleri zorluklar taşımaktadır[73]. Delillerin adli bilişim kurallarına uygun olarak toplanması gerekmektedir. Delillerde sehven yapılabilecek değişiklikler ve analiz esnasında yapılabilecek hatalar ciddi sonuçlara yol açabilmektedir. Örneğin iyi niyetli, deneyimsiz, yeterli eğitimi olmayan, teknolojiden uzak, tembel veya dikkatsiz kişiler, kötü niyetli bir tanık gibi veya mağdur veya araştırmacı gibi, elektronik delili değiştirebilir veya yanlış anlatabilir ve mahkemede yanlış bir mahkûmiyete sebep olabilirler. Üstelik bu tür kişilerin elektronik delil sunumlarının standartlarına uygun ve güvenilir olduğuna da inanılmış olabilir. Fakat mahkemeye sunulan elektronik delillerin, bağımsız uzmanlarca kontrolü ve duruşmada tartışılması ise bu ihtimali azaltmaktadır[74]. Bilişim suçları diğer suçlara göre farklılık göstermektedir. Bu suçlarla başa çıkabilmek için Bilişim Suçlarıyla Mücadele Kanunu çıkarılmalıdır. Bilişim suçları konusunda uzman personelin yetiştirilmesi için tüm kolluk kuvvetlerinin kullanabileceği bilişim suçlarıyla mücadele bilgi veri tabanı oluşturulmalı; yeni suç tipleri ve anlık olarak işlenen veya ihbar edilen suçlar bu veri tabanına eklenerek durumsal farkındalık sağlanmalıdır.

Sonuç olarak, bilgi ve teknoloji çağının vazgeçilmezi bu devasa haberleşme ağı ve sistemlerinin güvenli olması, bireylerin sahip olduğu kazanımlardan etkili ve güvenli bir şekilde faydalanarak huzur ve refah içinde hayatlarını idame ettirmelerini sağlayacaktır. Teknolojinin sunduğu bu imkânlardan güvenli olarak en üst düzeyde faydalanmaya devam edebilmek adına, bilinçli vatandaşlar olarak hepimizin kanunlarla belirlenmiş kural ve kaidelerle bilişim uzmanlarının tavsiyelerine harfiyen uyması önem arz etmektedir. Bilgi güçtür felsefesinden hareketle, hayatımızın her alanında kullandığımız teknoloji ürünlerine karşı bilgi düzeyimizi her fırsatta artırmalı, öğrenmek için çaba sarf ederek farkındalık düzeyimizi her zaman yüksek tutmalıyız.

## KAYNAKLAR

1. Aydın, E., "Bilişim Suçları ve Hukukuna Giriş", ***Doruk Yayınları*** , Ankara, 24 (1992).

2. Schjolberg, S., "The Legal Framework – Unauthorized Access to Computer Systems, Penal Legislation in 44 Countries"***, Moss Bölge Mahkemesi Yayını***, Norveç,(2003).

3. Bozkurt, V., "Elektronik Ticaret Hukuk Çalışma Grubu Raporu, Elektronik Ticaret", ***Alfa Yayınları***, İstanbul, 266 (2000).

4. Değirmenci, O., "Bilişim Suçları", ***Marmara Üniversitesi Sosyal Bilimler Enstitüsü***, Yayımlanmamış Yüksek Lisans Tezi, İstanbul, 9-27 (2002).

5. İnternet: OECD input to te UN workinggroup on internet govarnence, www.oecd.org/document/40/0,3343,en_21571361_34590630_34888424_1_1_1_1,00.html (2011).

6. Yazıcıoğlu R. Y., "Bilgisayar Suçları, Sosyolojik, Kriminolojik ve Hukukî Boyutları İle", ***Alfa Yayınları***, İstanbul, 29-155 (1997).

7. İnternet: Türk Dil Kurumu, www.tdk.gov.tr/TR/Genel/SozBul.aspx?F6E10F8892433CFFAAF6AA849816B2EF4376734BED947CDE&Kelime=bilgisayar (2012).

8. Akbulut, B., "Bilişim Suçları", ***Selçuk Üniversitesi Hukuk Fakültesi Dergisi Milenyum Armağanı***, S. 1-2, C.8, Konya, 545-546 (2000).

9. Ceyhun Y.,Ç., "Bilgi Teknolojileri Türkiye için Nasıl Bir Gelecek Hazırlamakta", ***Türkiye İş Bankası Kültür Yayınları***, Ankara, 1-2 (1997).

10. Hennessy J. L., PATTERSON David A., ARPACİ-DUSSEAU Andrea, "Computer Architecture", ***Morgan Kaufmann***, 1 (2007).

11. Türkiye İstatistik Kurumu,***2010 Yılı Hane Halkı Bilişim Teknolojileri Kullanım Araştırması Sonuçları***, Sayı: 148, Ankara (2010).

12. Güngör, Nemci Murat, "Yeni Türk Ceza Kanunu Kapsamında Bilişim Suçları Ve Emniyet Genel Müdürlüğü Uygulamaları", ***İstanbul Üniversitesi Sosyal Bilimler Enstitüsü Kamu Yönetimi Anabilim Dalı***, Yüksek Lisans Tezi, İstanbul, 20-22, (2007).

13. Yazıcıoğlu Y., "Yeni Türk Ceza Kanunundaki Bilişim Suçlarının Genel Değerlendirmesi", ***Yeditepe Üniversitesi Hukuk Fakültesi Dergisi (YÜHFD),*** C:II, S: 2, İstanbul, 403 (2005).

14. Dülger M. V., "Bilişim Suçları", ***Seçkin Yayınları***, İstanbul, 45 (2004).

15. İnternet: TBMM, kanunlar, www.tbmm.gov.tr/kanunlar/k5237.html, (2012).

16. Bensghir T. K., "Bilgi Teknolojileri ve Örgütsel Değişim", ***TODAİE***, Ankara, 14 (1996).

17. Merriam Webster's Dictionary & Thesaurus, ***Merriam-WebsterInc,*** London (2008).

18. İnternet: Boğaziçi Üniversitesi Bilgi İşlem Merkezi, http://www.cc.boun.edu.tr/training/internet_tur.pdf (2012).

19. İnternet: Ankara Üniversitesi Bilgi İşlem Daire Başkanlığı, http://bid.ankara.edu.tr/yardim/hii/bolum1.html (2012).

20. Ferrara G. R. ve arkadaşları, "Cyber Law Text and Cases", ***South-Western Colege Publishing***, ABD, 3 (2001).

21. İnternet: Milli Eğitim Bakanlığı, Türkiye'de İnternet http://www.meb.gov.tr/belirligunler/internet_haftasi_2005/turkiyede_internet.htm (2010).

22. Dönmezer S., "Kriminoloji", ***İstanbul Üniversitesi Yayını***, İstanbul, 62 (1981).

23. Gözübüyük A. P., "Türk Ceza Kanunu Şerhi", ***Kazancı Yayınları***, c:1, İstanbul, 4 (1988).

24. Dönmezer Sulhi, ERMAN Sahir, "Nazari ve Tatbiki Ceza Hukuku Genel Kısım", ***Beta***, c.1, İstanbul, 5-354 (1987).

25. İnternet: Yeni TCK'nun Hazırlanmasında Esas Alınan Suç Teorisi İzzet ÖZGENÇ, www.ceza-bb.adalet.gov.tr/makale/pp2.ppt (2011).

26. Önemli Murat, "İnternet Suçlarıyla Mücadele Yöntemleri", TODAİE yüksek lisanas tezi, Ankara, 29 (2004).

27. Mitnick K., D., SIMON W. L., "Aldatma Sanatı", ***ODTÜ Geliştirme Vakfı Yayıncılık***, Ankara, 4 (2005).

28. Akıncı H., ALIÇ A.E, ER C., "Türk Ceza Kanunu ve Bilişim Suçları", İnternet ve Hukuk, ***İstanbul Bilgi Üniversitesi Yayınları***, İstanbul, 158 (2004).

29. Koç S., KAYNAK S., "Bilişim Suçları Bağlamında Yeni Medya Olarak İnternet ve Kişisel Güvenlik", ***XIV. Türkiye'de İnternet Konferansı,*** İstanbul (2009).

30. The 2010 BSA Global Software Piracy Study***, Eighth Annual BSA and IDC Global Software PiracyStudy***, NewYork (2011).

31. Demir Ö, İnternet Servis Sağlayıcısın Hukuki Sorumluluğu, ***Uluslar arası internet Hukuku Sempozyumu***, İzmir, 481-484 (2002).

32. Atıcı, B., GÜMÜŞ Ç., Sanal Ortamda Gerçek Tehditler: Siber Terör. ***Polis Dergisi***, Yıl: 9, Sayı: 37, Ankara, 57–66 (2003).

33. İnternet: Google arama istatistikleri, http://www.google.com/trends?q=child+porn&ctab=0&geo=all&date=all&sort=0 (Kasım 2011).

34. Bayraktark l, "Banka Kredi Kartları ile Ortaya Çıkan Ceza Hukuku Sorunları", ***Beta Yayınevi***,s.72-73, İstanbul, 2000.

35. Bankalar arası Kart Merkezi 2010 Faaliyet Raporu, İstanbul, 18, (2011).

36. İnternet: Telekomünikasyon İletişim Başkanlığı http://www.tib.gov.tr/kat/baskanlik.html (2012).

37. Sağıroğlu Ş., BULUT H., "Mobil Ortamlarda Bilgi ve Haberleşme Güvenliği Üzerine Bir İnceleme", ***Gazi Üniv. Müh. Mim. Fak. Der***. Cilt 24, No 3, 499-507 (2009).

38. O'loughlin, J., Witmer Frank D. W., Andrew LİNKE M., Thorwardson N., "Peeringin to the Fog of War: The Geography of the WikiLeaks Afghanistan War Logs", 2004–2009,***Eurasian Geography and Economics***, ,ABD,472–495 (2010).

39. Yılmaz D., "Hacking Bilişim Korsanlığı ve Korunma Yöntemleri", ***Hayat Yayınları***, İstanbul, 381,277 (2004).

40. Akbulut, B., "Türk Ceza Hukukunda Bilişim Suçları", ***Selçuk Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı Ceza ve Ceza Usul Hukuku Bilim Dalı,*** doktora tezi, Konya, 60 (1999).

41. Önemli M.," İnternet Suçlarıyla Mücadele Yöntemleri", ***TODAİE*** yüksek lisanas tezi, Ankara, 29 (2004).

42. TUİK Hane halkı Bilişim Teknolojileri Kullanım Araştırması, sayı:170, Ankara (2011).

43. Symantec Internet Security Threat Report Volume 16, ABD (2011).

44. Özen Ü., SARI A., ***Gazi Üniversitesi Bilişim Teknolojileri Dergisi***, Cilt: 1, Sayı: 3, Ankara (2008).

45. Berry A., "Sonsuzluğun Kıyıları", ***TÜBİTAK Popüler Bilim Kitapları***, Ankara, 226-227, (2003).

46. Mowery K., MEIKLEJOHN S. S., "Heat of the Moment: Characterizing the Efficacy of Thermal Camera-Based Attacks", ***USENIX Security Symposium University of California***, ABD (2011).

47. Sevgi L., Elektronik Savaşlar, "Bilgi Casusluğu ve TEMPEST", ***Endüstriyel &Otomasyon***, Ocak sayısı, İstanbul (2005).

48. Ketizmen M., "Türk Ceza Hukukunda Bilişim Suçları", ***Ankara Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı***, doktora tezi,s.1-2,45 Ankara (2006).

49. Dilek H. İ., "Bilişim Suçları ve Türk Hukuk Sistemindeki Yeri", ***Dicle Üniversitesi Sosyal Bilimler Enstitüsü***, yüksek lisans tezi, Diyarbakır, 3-4 (2007).

50. Güngör N. M., "Yeni Türk Ceza Kanunu Kapsamında Bilişim Suçları ve Emniyet Genel Müdürlüğü Uygulamaları", ***İstanbul Üniversitesi Sosyal Bilimler Enstitüsü Kamu Yönetimi Anabilim Dalı***, yüksek lisans tezi, İstanbul, 164-166 (2007).

51. Ergüç S., "Türk Bankacılık Sisteminde İnternet Bankacılığı İle Yapılan Dolandırıcılıklar ve Bilişim Suçları Hukuku", ***Kadir Has Üniversitesi Sosyal Bilimler Enstitüsü İşletme Bölümü***, yüksek lisans tezi, İstanbul, 107 (2008).

52. Kızıltan M. B.,, "5237 Sayılı Türk Ceza Kanununda Bilişim Sistemine Girme, Sistemi Engelleme ve Bozma Suçları", ***İstanbul Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı***, yüksek lisans tezi, İstanbul, 1-2 (2007).

53. Alaca B., "Ülkemizde Bilişim Suçları ve İnternetin Suça Etkisi", ***Ankara Üniversitesi Sosyal Bilimler Enstitüsü Antropoloji Anabilim Dalı,*** yüksek lisans tezi, Ankara, 118-120 (2008).

54. Tulum İ., "Bilişim Suçları İle Mücadele", ***Süleyman Demirel Üniversitesi Sosyal Bilimler Enstitüsü Kamu Yönetimi Anabilim Dalı,*** yüksek lisans tezi, Isparta,101 (2006).

55. İlbaş, Ç., "Bilişim Suçlarının Sosyo-Kültürel Seviyelere Göre Algı Analizi", ***Başkent Üniversitesi Fen Bilimleri Enstitüsü***, yüksek lisans tezi, Ankara (2009).

56. Dijle H., "Türkiye'de Eğitimli İnsanların Bilişim Suçlarına Yaklaşımı", ***Gazi Üniversitesi Fen Bilimleri Enstitüsü Elektronik Bilgisayar Eğitimi Anabilim dalı,*** yüksek lisans tezi, Ankara (2006).

57. Taş K. A., "Bilişim Suçları ve Adana İlinde 2006-2009 Yılları Arasında Meydana Gelen Bilişim Suçlarının Değerlendirilmesi", ***Çukurova Üniversitesi Sağlık Bilimleri Enstitüsü Adli Tıp Ana Bilim Dalı,*** yüksek lisans tezi, Adana (2010).

58. Demircan T., "Bilişim Alanında Suçlar", ***Selçuk Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı,*** yüksek lisans tezi, Konya, 126 (2007).

59. Gümüş Ç., "Bilişim Suçlarıyla Mücadelede Polisin Eğitimi", ***Fırat Üniversitesi Sosyal Bilimler Enstitüsü Eğitim Bilimleri Anabilim Dalı,*** doktora tezi, Elazığ, 253 (2008).

60. Özkan T., "Siber Terörizm Bağlamında Türkiye'ye Yönelik Faaliyet Yürüten Terör Örgütlerinin İnternet Sitelerine Yönelik Bir İçerik Analizi", ***Anadolu Üniversitesi Sosyal Bilimler Enstitüsü Basın ve Yayın Anabilim Dalı,*** yüksek lisans tezi, Eskişehir (2006).

61. Durmaz Ş.,"Bilişim suçlarının sosyolojik analizi", ***Gazi Üniversitesi Sosyal Bilimler Enstitüsü Kamu Yönetimi Anabilim Dalı***, Ankara, 191 (2005).

62. İnternet: Türkiye'de bilişim suçları ve Mücadele Yöntemleri, http://www.bayar.edu.tr/bid/dokumanlar/bilisim-suclari.pdf (2012).

63. Alataş Ş., ATAN M., "Phishing: İnternet Denizinin Popüler Avlanma Yöntemi", ***XII. Türkiye'de İnternet Konferansı*** "İnternet ve Toplum; Bilgi Toplumuna Doğru" Bilkent Üniversitesi, Ankara (2007).

64. Nizam F., BİÇER S., "İnternet Yayıncılığında Etik ve Hukuki İhlaller", **V. *Türkiye'de İnternet Konferansı,*** İstanbul (2005).

65. Alataş Ş., ATAN M., "Phishing: İnternet Denizinin Popüler Avlanma Yöntemi", ***XII. Türkiye'de İnternet Konferansı*** "İnternet ve Toplum; Bilgi Toplumuna Doğru" Bilkent Üniversitesi, Ankara (2007).

66. Hatcher, M. McDannel, OSTFELD Stacy, "Computer Crimes", ***American Criminal aw Review***, vo.36, no.397, USA, 398-399 (2001).

67. Campbell, D. S., "Focus on Cyber-Fraud", ***The Internel Auditor***, 59, No 1, 30 (2002).

68. Carter D. L., "Computer Crime Categories How Techno-criminals Operate", ***FBI Law Enforcement Bulletin***, v.64, 26 (1995).

69. TUİK Hane halkı Bilişim Teknolojileri Kullanım Araştırması, sayı:148, Ankara (2010).

70. The 2010 BSA Global Software Piracy Study, BSA Global Survey of PC User Attitudes, NewYork (2011).

71. İnternet: Telif Hakları Genel Müdürlüğü, http://www.telifhaklari.gov.tr/belge/1-26483/korsanlikla-ilgili-istatistikler.html (2012).

72. İlbaş, Ç., KÖKSAL M.A., "Türkiye Bilişim Suçları Raporu 1990-2011 Temmuz", ***2.Uluslararası Bilişim Hukuku Kurultayı***, İzmir (2011).

73. Stephon, P. R., " Intrusion Management: A Top Level Model For Securing Information Assets in Enterprise Enviroment" In E.U. Gattiker, ***EICAR*** (2000).

74. Talleur T., "Digital Evidence: The Moral Challange***", International Journal of Digital Evidence***, v.1 (2002).

# EKLER

EK-1. Cezaevi görüşme formu

## BİLİŞİM SUÇLARININ ANALİZİNE İLİŞKİN GÖRÜŞME FORMU

***NOT:*** ***CEVAPLARINIZ TEZ ÇALIŞMASINDA KULLANILACAK OLUP VERDİĞİNİZ CEVAPLAR BAŞKA KURUM VE KİŞİLERCE PAYLAŞILMAYACAKTIR. ALEYHİNİZDE KULLANILMAYACAKTIR.***

**Görüşmenin yapıldığı yer:**
**Görüşmenin yapıldığı tarih-saat:**

1. Cinsiyet
( ) Erkek ( ) Kadın

2. Yaş
( )18-30 ( )31-45 ( )46 ve üstü

3. Eğitim durumu ( terk durumunda ilgili hanenin yanına yazınız.)

( ) okur- yazar ( ) ilköğretim ( ) lise

( ) önlisans ( ) lisans ( ) lisansüstü

4. Medeni hali

( ) bekar ( ) evli ( ) boşanmış varsa çocuk sayısını yazınız……

5. Meslek
……

6. Gelir durumu ( cezaevine girmeden önce)

( ) 0-1000 TL

( )1001-2000 TL

( ) 2001-3000 TL

( )3001 TL ve üstü

**7.** İkamet ettiği yer (cezaevine girmeden önce)

( ) büyükşehir ( ) şehir ( ) ilçe ( ) köy

**8.** ikamet ettiğiniz şehri yazınız ( cezaevine girmeden önce)

……

EK-1(Devam). Cezaevi görüşme formu

**9.**Bilgisayar kullanmayı biliyor musunuz?

( ) evet ( ) kısmen ( ) hayır

**10.** Kendinizi nasıl bir bilgisayar kullanıcısı olarak görürsünüz?

( ) Usta-Profesyonel ( ) orta düzeyde ( ) alt düzeyde ( ) cevap yok

**11**. Kaç yıldır bilgisayar kullanıyorsunuz.

( ) 1-2 yıl ( ) 3-4 yıl ( ) 5 yıl ve daha fazla

**12.**Suç işlerken bilgisayar veya herhangi bir teknolojik bir araçtan faydalandınız mı? Lütfen kısaca belirtiniz.

……
……
……
……
……

**13.** Suç işlerken bilişim suçlarının tespitinin zor olacağını düşünüp rahat davranır mısınız?

……
……
……

**14.** Suçu işleme sürecini nasıl planlıyorsunuz? (Planlamadan Uygulamaya-eylem sonuna kadar)

……
……
……
……
……

EK-1(Devam). Cezaevi görüşme formu

**15.** Bugüne kadar bilişim suçu işleyen arkadaş ve aile çevrenizden herhangi birisi var mıdır? Yakalandı mı?

……
……
……

**16.** Başkasına ait kredi kartını nasıl ele geçirirsiniz veya kopyalarsınız? Suçu hangi şekilde işlediniz? (İnternet, ATM, Ticari İşletmelerde Alışveriş Yaparak) Kısaca anlatınız.

……
……
……

**17.** Sizi suç işlemeye iten sebepler nedir? Niçin bu yolu-suçu tercih ettiniz. Lütfen içtenlikle cevaplayınız.

……
……
……
……

**18.** Kredi kartlarına getirilen şifre uygulaması, son dönemlerde artan dolandırıcılık vakalarına çözüm sağladı. Şifreli çipli kart (chip&pin) sistemi suç işlemenizi zorlaştırdı mı? Sizler ne gibi tedbir aldınız.

……
……
……
……
……
……
……

**19.** Kredi kartı sahteciliği teknik olarak zordur. Manyetik bilgilerin kopyalanması bir takım aletleri gerektirir. Bu bilginizi nasıl elde ettiniz? Bilgilerinizi başkalarıyla paylaştınız mı?

……
……
……

EK-2. Online anket formu

## ÜNİVERSİTE ÖĞRENCİLERİNİN BİLİŞİM SUÇLARINA YÖNELİK TUTUM VE BİLGİ DÜZEYLERİ ÜZERİNE ARAŞTIRMA

Bu anketin amacı bilişim suçlarına yönelik üniversite öğrencilerinin tutumunu ve bilgi düzeylerini ölçmektir.

LÜTFEN AŞAĞIDAKİ SORULARI CEVAPLAYINIZ. TEŞEKKÜR EDERİM.

**SORU1:**Cinsiyet

□Erkek

□Kadın

**SORU2:**Kaçıncı Sınıftasınız?

□Hazırlık

□1

□2

□3

□4

**SORU3:**Bölümünüz

□Bilgisayar ve Öğretim Teknolojileri Eğitimi Bölümü

□Diğer

Ek-2(Devam). Online anket formu

**SORU4:**Üniversitenizi işaretleyiniz (Alfabetik Sıraya Göre Değildir!)

□Afyon Kocatepe Üniversitesi

□Anadolu Üniversitesi

□Ankara Üniversitesi

□Atatürk Üniversitesi

□Bahçeşehir Üniversitesi

□Başkent Üniversitesi

□Boğaziçi Üniversitesi

□Çanakkale Onsekizmart Üniversitesi

□Çukurova Üniversitesi

□Ege Üniversitesi

□Fırat Üniversitesi

□Gazi Üniversitesi

□Karadeniz Teknik Üniversitesi

□Marmara Üniversitesi

□Ondokuz Mayıs Üniversitesi

□Orta Doğu Teknik Üniversitesi

□Sakarya Üniversitesi

□Selçuk Üniversitesi

□Uludağ Üniversitesi

□Yıldız Teknik Üniversitesi

□Yüzüncü Yıl Üniversitesi

□Eskişehir Osmangazi Üniversitesi

□Diğer

**SORU5:**Kendinize ait bilgisayarınız var mı?

□var

□yok

Ek-2(Devam). Online anket formu

**SORU6:**Bir gün içerisinde internete bağlı olarak geçirdiğiniz süre ne kadar?

□0-1 saat

□1-3 saat

□3-5 saat

□5 saat ve üzeri

**SORU7:**İnternete genellikle aşağıdakilerden hangisi üzerinden bağlanırsınız?

□bilgisayar

□cep telefonu

□pda- tablet pc

**SORU8:**İnternet genellikle nereden bağlanırsınız?

□ev

□okul

□yurt

□iş yeri

□internet kafe

**SORU9:** İnternet üzerinde kullandığınız şifre ve parolaları sıklıkla değiştirir misiniz?

□evet değiştiririm

□hayır değiştirmem

Ek-2(Devam). Online anket formu

**SORU10:**İnternet bankacılığı veya cep bankacılık uygulamalarını kullanıyor musunuz?

□evet kullanıyorum

□hayır kullanmıyorum

**SORU11:** İnternet üzerinden alışveriş yapıyor musunuz?

□evet

□hayır

**SORU12:** Kullandığınız işletim sistemi lisanslı mıdır?

□evet

□hayır

□deneme sürümü kullanıyorum

**SORU13:** Kişisel bilgisayarınızda antıvırus veya fırewall yazılımı kullanıyor musunuz?

□evet kullanıyorum

□hayır kullanmıyorum

**SORU14:**Teknoloji, bilgisayar ve internet konularıyla yakından ilgiliyimdir.

lütfen aşağıdaki sorulardan size uygun olan seçeneği işaretleyiniz.

□Katılıyorum □Fikrimyok □Katılmıyorum

Ek-2(Devam). Online anket formu

**SORU15**: İnternet bankacılığını güvenli buluyorum.

□Katılıyorum □Fikrim yok □Katılmıyorum

**SORU16:** İnternet üzerinden alışverişi güvenli buluyorum.

□Katılıyorum □Fikrim yok □Katılmıyorum

**SORU17:** Bilişim suçları ile ilgili yasal düzenlemeleri yeterli buluyorum.

□Katılıyorum □Fikrim yok □Katılmıyorum

**SORU18:** Bilişim suçlarının tespiti zor olduğu için gerekli bilgiye sahip olsam bende hacker'lık yapardım.

□Katılıyorum □Fikrim yok □Katılmıyorum

**SORU19:** Gizli kamera görüntülerinin ve kişisel bilgilerin internet aracılığıyla ifşa edilmesini doğru bulmuyorum.

□Katılıyorum □Fikrim yok □Katılmıyorum

**SORU20**: İnternette hackerlık yöntemlerini anlatan ve gerekli casusluk yazılımlarını temin etmemizi sağlayan siteler yasaklanmalı.

□Katılıyorum □Fikrim yok □Katılmıyorum

**SORU21**: İnternetten film, oyun, müzik ve oyun dosyaları indirmenin ve lisanssız yazılım kullanmanın suç olduğunu biliyorum.

□Katılıyorum □Fikrim yok □Katılmıyorum

Ek-2(Devam). Online anket formu

**SORU22:** Bilgisayarımı ve cep telefonumu tamire verirken önemli bilgilerimi silerim veya şifrelerim / gizlerim.

□Katılıyorum □Fikrim yok □Katılmıyorum

**SORU23:** Kolluk kuvvetlerinin (polis, jandarma) bilişim suçlarını önlemede ve tespitinde yapmış olduğu çalışmaları yeterli buluyorum.

□Katılıyorum □Fikrim yok □Katılmıyorum

**SORU24:** Kredi kartı ile yapılan alışverişlerde şifre uygulaması (chip&pin) ile kredi kartı kullanımının daha güvenli hale geldiğini düşünüyorum.

□Katılıyorum □Fikrim yok □Katılmıyorum

**SORU25:** Cep telefonu görüşmelerinin ve e-posta yazışmalarının adli makamlartarafından dinlenip takip edilmesini kamu güvenliği açısından yararlı buluyorum.

□Katılıyorum □Fikrim yok □Katılmıyorum

**SORU26:** Sosyal paylaşım sitelerinin ( FACEBOOK, TWITTER vb.) kişisel bilgilerimi ve fotoğraflarımı başka kişi ve şirketlerle/kurumlarla paylaştığı yönünde endişelerim var.

□Katılıyorum □Fikrim yok □Katılmıyorum

**SORU27:** Mahkeme kararıyla içinde suç unsuru olduğu tespit edilen vekapatılmasına karar verilen web sitelerine yapılan hukuki engellemelerin düşünce özgürlüğüne aykırı olduğunu düşünüyorum.

□Katılıyorum □Fikrim yok □Katılmıyorum

Ek-2(Devam). Online anket formu

AŞAĞIDAKİ SUÇ İŞLEME YÖNTEMLERİ HAKKINDA BİLGİNİZ VAR MI? LÜTFEN SİZE UYGUN OLAN SEÇENEĞİ İŞARETLEYİNİZ.

**SORU28**: 01.03.2006 tarihinde yürürlüğe giren 5464 no'lu Banka Kartları ve Kredi Kartları Kanunu gereği, kart hamilleri, yapacakları kayıp ya da çalıntı bildiriminden önceki yirmi dört saat içinde kartları ile gerçekleştirilen hukuka aykırı kullanımdan doğan zararlardan 150 TL. ile sınırlı olmak üzere sorumludurlar. Bunun üzerindeki zararların bankanızın güvencesi altında olduğunu biliyor musunuz?

□Bilgi sahibiyim □Sadece duydum □ Bilgim yok

**SORU29:** Bankamatiklerden (ATM) banka veya kredi kartınızla işlem yaparken sahte klavye, kartın manyetik şerit bilgisinin kopyalanması(skimmer cihazı) gibi yöntemlerle hesabınızdan para çekilebileceğini biliyor musunuz?

□Bilgi sahibiyim □Sadece duydum □ Bilgim yok

**SORU30:** Sosyal mühendislik yöntemleri ile suçluların bilgisayarınıza erişim

sağlayarak bilgisayarınıza gizlice casus yazılımlar ya da diğer istenmeyen yazılımlar yüklemek veya parolalarınızı ya da önemli mali ve kişisel bilgilerinizi vermeniz için sizi ikna etmeye çalışabileceğini biliyor musunuz?

□Bilgi sahibiyim □Sadece duydum □ Bilgim yok

**SORU31:** Kişisel bilgisayarın ya da DNS server'ın korsanlar tarafından ele geçirilip, bilgisayar içerisinde bulunan "hosts" isimli dosyanın içeriğinin değiştirilmesi ve müşterinin orjinal internet sayfasına girdiği zannettirilerek sahte sitelere yönlendirildiğini biliyor musunuz?

□Bilgi sahibiyim □Sadece duydum □ Bilgim yok

Ek-2(Devam). Online anket formu

**SORU32:** 'Java Script' içeren sahte bir program aracılığı ile hedef bilgisayara hackertarafından gönderilen sahte program açıldığında, bilgisayar ekranına ŞİFRENİZİYENİDEN GİRİN yazısı çıkartılıp kullanıcının şifresini öğrenerek hacker'aulaştırılabileceğini biliyor musunuz?

□Bilgi sahibiyim □Sadece duydum □ Bilgim yok

**SORU33:** Müşterek kullanıma açık olan yerlerdeki bilgisayarlara loadpowerprof.exe, keylogger.exe vb. programlar yüklenerek internet bankacılığı ile işlem yapan mevduat sahiplerinin hesabına erişim sağlanabileceğini biliyor musunuz?

□Bilgi sahibiyim □Sadece duydum □ Bilgim yok

**SORU34:** Kendilerini kamu görevlisi olarak tanıtan veya ödül kazandığınızı belirterek para/kontör transferi talep ederek dolandırılabileceğinizi biliyor musunuz?

□Bilgi sahibiyim □Sadece duydum □ Bilgim yok

LÜTFEN AŞAĞIDAKİ KAVRAM, TEKNİK VE SİBER SUÇ ÇEŞİTLERİNİN KARŞISINA SİZE GÖRE UYGUN OLAN CEVABI

İŞARETLEYİNİZ.

**SORU35**: BİLGİSAYAR KORSANLIĞI

□Bilgi sahibiyim □Sadece duydum □ Bilgim yok

**SORU36**: AĞ SOLUCANLARI (WORMS)

□Bilgi sahibiyim □Sadece duydum □ Bilgim yok

Ek-2(Devam). Online anket formu

**SORU37**: WEB SAYFASI HIRSIZLIĞI

□Bilgi sahibiyim □Sadece duydum □ Bilgim yok

**SORU38**: BİLGİSAYAR VİRÜSLERİ

□Bilgi sahibiyim □Sadece duydum □ Bilgim yok

**SORU39**: KREDİ / BANKA KARTLARI SAHTECİLİĞİ VE DOLANDIRICILIĞI

□Bilgi sahibiyim □Sadece duydum □ Bilgim yok

**SORU40**: ELEKTRONİK İMZA

□Bilgi sahibiyim □Sadece duydum □ Bilgim yok

**SORU41**: MANTIK BOMBALARI (LOGİC BOMBS)

□Bilgi sahibiyim □Sadece duydum □ Bilgim yok

**SORU42:** SPAM (İSTEM DIŞI ALINAN E-POSTA)

□Bilgi sahibiyim □Sadece duydum □ Bilgim yok

**SORU43:** TRUVA ATI (TROJEN HORSE)

□Bilgi sahibiyim □Sadece duydum □ Bilgim yok

Ek-2(Devam). Online anket formu

**SORU44:** OLTALAMA (PHİSHİNG SALDIRILARI )

□Bilgi sahibiyim □Sadece duydum □ Bilgim yok

**SORU45**: SİBER ŞANTAJ VE TEHDİT

□Bilgi sahibiyim □Sadece duydum □ Bilgim yok

**SORU46:** SİBER KUMAR VE BAHİS

□Bilgi sahibiyim □Sadece duydum □ Bilgim yok

**SORU47:** SİBER DOLANDIRICILIK

□Bilgi sahibiyim □Sadece duydum □ Bilgim yok

**SORU48:** ÇOCUK PORNOGRAFİSİ

□Bilgi sahibiyim □Sadece duydum □ Bilgim yok

**SORU49:** Üniversitelerde teknolojik gelişmeler ve siber suçlarla ilgili konuların derslerde anlatılmasını ayrıca bu konularla ilgili

seminer düzenlenmesini istiyor musunuz?

□Evet □Hayır □Fikrim yok

# ÖZGEÇMİŞ

## Kişisel Bilgiler


| | |
|---|---|
| Soyadı, adı | : BİLEK, Burak Tunç |
| Uyruğu | : T.C. |
| Doğum tarihi ve yeri | : 1985, İzmir |
| Medeni hali | : Bekar |
| Telefon | : 0 (543) 533 94 94 |
| e-mail | : buraktunc@gmail.com |


## Eğitim

| Derece | Eğitim Birimi | Mezuniyet tarihi |
|---|---|---|
| Yüksek lisans | Gazi Üniversitesi /Bilgisayar Eğitimi | 2012 |
| Lisans | Kara Harp Okulu/ Sistem Mühendisliği | 2008 |
| Lise | Maltepe Askeri Lisesi | 2004 |

## İş Deneyimi

| Yıl | Yer | Görev |
|---|---|---|
| 2008- | J.Gn.K.lığı | Subay |

## Yabancı Dil

İngilizce

## Yayınlar

SARICA R., BİLEK B. T., Yanı Başımızdaki Tehlike: Sosyal Mühendislik, **Jandarma Dergisi**, Sayı:132, 22 (2012).