

**BİLİŞİM ÖĞRENCİLERİNİN SİBER SUÇ
FARKINDALIĞI: ERZURUM İLİ MESLEKİ VE
TEKNİK LİSELER ÖRNEĞİ**

Ömer Sıddık BUDAK

**Yüksek Lisans Tezi
Bilgisayar ve Öğretimi Teknolojileri Eğitimi
Ana Bilim Dalı
Prof. Dr. Aslan GÜLCÜ
2015
Her hakkı saklıdır**

T.C.
ATATÜRK ÜNİVERSİTESİ
EĞİTİM BİLİMLERİ ENSTİTÜSÜ
BİLGİSAYAR VE ÖĞRETİMİ TEKNOLOJİLERİ EĞİTİMİ
ANA BİLİM DALI

BİLİŞİM ÖĞRENCİLERİNİN SİBER SUÇ FARKINDALIĞI:
ERZURUM İLİ MESLEKİ VE TEKNİK LİSELER ÖRNEĞİ

(Cyber Crime Awareness of Informatics Students:
Erzurum Province Example of Vocational and Technical High School)

YÜKSEK LİSANS TEZİ

Ömer Sıddık BUDAK

Danışman: Prof. Dr. Aslan GÜLCÜ

ERZURUM
Temmuz, 2015

KABUL VE ONAY TUTANAĞI

Prof. Dr. Aslan GÜLCÜ danışmanlığında, Ömer Sıddık BUDAK tarafından hazırlanan “BİLİŞİM ÖĞRENCİLERİNİN SİBER SUÇ FARKINDALIĞI: ERZURUM İLİ MESLEKİ VE TEKNİK LİSELER ÖRNEĞİ” başlıklı çalışma / / tarihinde yapılan savunma sınavı sonucunda başarılı bulunarak jürimiz tarafından Bilgisayar ve Öğretimi Teknolojileri Eğitimi Anabilim Dalı’nda Yüksek Lisans Tezi olarak kabul edilmiştir.

Jüri Üyesi : Prof. Dr. Aslan GÜLCÜ

İmza:

Jüri Üyesi : Doç. Dr. Yüksel GÖKTAŞ

İmza:

Jüri Üyesi : Yrd. Doç. Dr. Özlem BAYDAŞ

İmza:

Yukarıdaki imzaların adı geçen öğretim üyelerine ait olduğunu onaylarım.

17/08/2015

Prof. Dr. H. Ahmet KIRKKILIÇ

Enstitü Müdürü

S. D.

TEZ ETİK VE BİLDİRİM SAYFASI

Yüksek Lisans Tezi olarak sunduğum “BİLİŞİM ÖĞRENCİLERİNİN SİBER SUÇ FARKINDALIĞI: ERZURUM İLİ MESLEKİ VE TEKNİK LİSELER ÖRNEĞİ” başlıklı çalışmanın, tarafımdan, bilimsel ahlak ve geleneklere aykırı düşecek bir yardıma başvurmaksızın yazıldığını ve yararlandığım eserlerin kaynakçada gösterilenlerden olduğunu, bunlara atıf yapılarak yararlanılmış olduğunu belirtir ve onurumla doğrularım.

Tezimin kâğıt ve elektronik kopyalarının Atatürk Üniversitesi Eğitim Bilimleri Enstitüsü arşivlerinde aşağıda belirttiğim koşullarda saklanmasına izin verdiğimi onaylarım.

Lisansüstü Eğitim-Öğretim yönetmeliğinin ilgili maddeleri uyarınca gereğinin yapılmasını arz ederim.

- ☒ Tezimin tamamı her yerden erişime açılabilir.
- ☐ Tezim sadece Atatürk Üniversitesi yerleşkelerinden erişime açılabilir.
- ☐ Tezimin yıl süreyle erişime açılmasını istemiyorum. Bu sürenin sonunda uzatma için başvuruda bulunmadığım takdirde, tezimin tamamı her yerden erişime açılabilir.

.... / / 2015

(İmza)

Ömer Sıddık BUDAK

ÖZET

YÜKSEK LİSANS TEZİ

BİLİŞİM ÖĞRENCİLERİNİN SİBER SUÇ FARKINDALIĞI: ERZURUM İLİ MESLEKİ VE TEKNİK LİSELER ÖRNEĞİ

Ömer Sıddık BUDAK

2015, 110 sayfa

Bu araştırmanın amacı Mesleki ve Teknik liselerdeki bilişim bölümü öğrencilerinin siber suç farkındalıklarını araştırmaktır. Betimsel tarama modeli kullandığımız bu araştırmada 2013-2014 eğitim-öğretim yılında Erzurum’da Mesleki ve Teknik Liselerin bilişim bölümlerinde okuyan toplam 269 öğrenciye yerli-yabancı kaynaklardan yararlanılarak ve uzman görüşlerine başvurularak oluşturulan “Ortaöğretim Kurumlarında Siber Suç Farkındalık Anketi” uygulanmıştır.

Araştırmada SPSS 16 kullanılarak frekans dağılımı incelenmiş olup bu sorulardan hareketle faktör analizi yapılmış dört faktör elde edilmiştir. Bu faktörler İnternetin kişisel değerlere karşı sakıncalarını algılama, kişi ve örgütlerin İnterneti kötü niyetle kullanabileceklerini algılama, İnternetteki rahatlık seviyesi ve İnternette alınan önlem seviyesi şeklinde adlandırılmıştır. Yapılan Bağımsız Grup t Testi ve Tek Yönlü Varyans Analizi (ANOVA) ile faktörlerin demografik özellikler ile arasında anlamlı farklılıklarının olup olmadığı araştırılmıştır.

Öğrencilerin siber farkındalık durumlarının sınıf durumu, İnterneti kullanma yılı ve İnternette saldırıya uğrama durumu ile anlamlı bir farklılık göstermediği ancak cinsiyet ile anlamlı bir farklılık gösterdiği görülmüştür. Öğrencilerin İnternetteki rahatlık seviyelerinin sınıf durumu ve İnterneti kullanma yılı ile anlamlı bir farklılık göstermediği ancak cinsiyet ve İnternette saldırıya uğrama durumu ile anlamlı bir farklılık gösterdiği görülmüştür. Öğrencilerin İnternette alınan önlem seviyelerinin sınıf durumu, İnterneti kullanma yılı ve İnternette saldırıya uğrama durumu ile anlamlı bir farklılık göstermediği ancak cinsiyet ile anlamlı bir farklılık gösterdiği görülmüştür.

Anahtar Sözcükler: Bilişim bölümü öğrencileri, Siber suçlar, Siber suç farkındalığı.

ABSTRACT

MASTER'S THESIS

CYBER CRIME AWARENESS OF INFORMATICS STUDENTS: ERZURUM PROVINCE EXAMPLE OF VOCATIONAL AND TECHNICAL HIGH SCHOOL

Ömer Sıddık BUDAK

2015, 110 Pages

In this research where we have used descriptive survey model, “The Survey of Cybercrime and its Perception in Secondary Schools” formed by benefiting from domestic and foreign resources and by consulting to expert opinions has been applied to totally 269 students in informatics departments of vocational and technical high schools in Erzurum in 2013-2014 - academic year.

In the research, frequency distribution has been examined by using SPSS 16 and factor analysis has been performed based on these questions and four factors have been obtained. These factors are called as the perception the dangers of the Internet against personal values, the perception that people and organizations can use the Internet maliciously, comfort level in the Internet and the level of measures taken for the internet. It has been investigated whether there is a significant difference between the independent Group t Test, One-Way Analysis of Variance (ANOVA) and demographic characteristics of factors.

It has been observed that there isn't significant difference between class state of the student's cyber awareness, the number of years of using the Internet and the state of being attacked on the Internet but a significant difference has been observed with the gender. It has been observed that there isn't significant difference between class states of the comfort level of the students on the internet but a significant difference has been observed between the gender and the state of being attacked on the Internet. It has been observed that there isn't significant difference between class state of the student's level of measures taken on the internet, the number of years of using the Internet and the state of being attacked on the Internet but a significant difference has been observed with the gender.

Key Words: Informatics department students, Cybercrimes, Cybercrime awareness.

ÖNSÖZ

Çalışmalarım boyunca bana destek olan danışmanım ve değerli hocam Sayın Prof. Dr. Aslan GÜLCÜ'ye, yardımlarını esirgemeyen sayın Doç. Dr. Yüksel GÖKTAŞ'a minnettarlığımı arz ederim.

Çalışmalarımın her safhasında yanımda olan değerli arkadaşlarım Öğr. Gör. Erol GEÇGİN'e, Öğr. Gör. Onur KAVAK'a ve diğer iş arkadaşlarıma teşekkürlerimi sunarım.

Hayatımın bütün aşamalarında olduğu gibi hazırladığım bu tez aşamasında da desteğini her zaman bana hissettiren değerli abim Mevlüt BUDAK'a şükranlarımı sunarım.

Son olarak bugünlere gelmemde çok büyük emekleri olan, dualarını üzerimden hiçbir zaman esirgemeyen annem ve babama, varlığıyla moral kaynağım olan dünyalar tatlısı oğlum Yusuf Adil'e ve hiçbir zaman benden desteğini esirgemeyen, bu çalışma süresince benimle aynı sıkıntıları çeken yol arkadaşım canım eşim Eda BUDAK'a en içten sevgi ve teşekkürlerimi sunuyorum. İyi ki hayatımda varsınız.

Erzurum-2015

Ömer Sıddık BUDAK

İÇİNDEKİLER

KABUL VE ONAY TUTANAĞI	i
TEZ ETİK VE BİLDİRİM SAYFASI	ii
ÖZET.....	iii
ABSTRACT.....	iv
ÖNSÖZ	v
TABLolar DİZİNİ	xii
KISALTMALAR DİZİNİ.....	xiv

BİRİNCİ BÖLÜM

1. GİRİŞ	1
1.1. Siber Suç İle İlgili Tanımlar.....	3
1.1.1. Bilişim Kavramı.....	3
1.1.1.1. Bilgisayar.....	3
1.1.1.2. İnternet.....	4
1.1.2. Bilişim Suçu	4
1.1.3. Siber Kavramı.....	5
1.1.4. Siber Suç.....	5
1.1.5. Suç Kavramı	7
1.2. Geleneksel Suç İle Siber Suç Arasındaki Farklar	7
1.3. Siber Suçun Tarihçesi	8
1.4. Siber Suçun Sınıflandırılması	10
1.4.1. Veri Suçları.....	10
1.4.1.1. Verilerin çalınması.....	10
1.4.1.2. Verilerin durdurulması	10
1.4.1.3. Verilerin bozulması	10
1.4.1.4. Verilerin değiştirilmesi	10
1.4.1.5. Verilerin silinmesi	10
1.4.2. Yetkisiz erişim suçları	11
1.4.2.1. Yetkisiz erişim	11
1.4.2.2. Yetkisiz dinleme	11
1.4.2.3. Hesap ihlali	11

1.4.2.4. Virüs bulaştırma.....	11
1.4.3. Ağ Suçları	12
1.4.3.1. Ağların sabotajı.....	12
1.4.3.2. Ağların engellenmesi	12
1.4.4. Bilgisayarla İlgili Diğer Suçlar	12
1.4.4.1. Bilgisayar aracılığıyla dolandırıcılık ve hırsızlık	12
1.4.4.2. Bilgisayar aracılığıyla sahtecilik.....	12
1.4.4.3. Bilgisayar sabotajı	13
1.4.4.4. Bilgisayar yazılımlarının kullanımı	13
1.4.4.4.1. Yazılımların kural dışı kullanılması	13
1.4.4.4.2. Yazılımların kural dışı çoğaltılması.....	13
1.4.4.4.3. Yazılımların kural dışı kiralanması	14
1.4.4.5. Yasadışı yayınlar	14
1.4.4.6. Terörist faaliyetler	14
1.4.4.7. Çocuk pornografisi	15
1.4.4.8. Satılması yasak ürünlerin ticareti.....	15
1.4.4.8.1. Kadın ticareti	15
1.4.4.8.2. Çocuk ticareti.....	15
1.4.4.8.3. Organ ticareti	16
1.4.4.8.4. Uyuşturucu ticareti	16
1.4.4.8.5. Silah ticareti	16
1.5. Siber Suçların İşleniş Şekilleri	17
1.5.1. Bilişim Korsanlığı.....	17
1.5.2. Gizli Kapılar	17
1.5.3. Ağ Solucanları	18
1.5.4. Truva Atı.....	18
1.5.5. Mantık Bombaları.....	18
1.5.6. Salam Tekniği.....	19
1.5.7. İstem Dışı Elektronik Postalar (Spam)	19
1.5.8. Çöpe Dalma	19
1.5.9. Tarama	19
1.5.10. Oltaya Gelme	20

1.6. Türk Ceza Kanununda Siber Suçlar	20
1.6.1. Yeni Türk Ceza Kanununda Belirtilen Siber Suçlar.....	20
1.6.1.1. “Bilişim alanındaki suçlar” başlığı altındaki kanun maddeleri	21
1.6.1.1.1. Bilişim sistemine girme (Madde 243)	21
1.6.1.1.2. Sistemi engelleme, bozma, verileri yok etme veya değiştirme (Madde 244)	21
1.6.1.1.3. Banka veya kredi kartlarının kötüye kullanılması (Madde 245)	22
1.6.1.1.4. Tüzel kişiler hakkında güvenlik tedbiri uygulanması (Madde 246)	23
1.6.1.2. Yeni Türk ceza kanununda belirtilen diğer siber suçlar	24
1.6.1.2.1. Çocukların cinsel istismarı (Madde 103).....	24
1.6.1.2.2. Müstehcenlik (Madde 226).....	24
1.6.1.2.3. Kişisel verilerin kaydedilmesi (Madde 135).....	24
1.6.1.2.4. Verileri hukuka aykırı olarak verme veya ele geçirme (Madde 136)....	25
1.6.1.2.5. Verileri yok etmeme (Madde 138)	25
1.6.1.2.6. Haberleşmenin engellenmesi (Madde 124)	25
1.6.1.2.7. Haberleşmenin gizliliğini ihlal (Madde 132).....	26
1.6.1.2.8. Kişiler arasındaki konuşmaların dinlenmesi ve kayda alınması (Madde 133)	26
1.6.1.2.9. Özel hayatın gizliliğini ihlal (Madde 134).....	27
1.6.1.2.10. Hakaret (Madde 125)	27
1.6.1.2.11. Nitelikli hırsızlık (Madde 142)	28
1.6.1.2.12. Nitelikli dolandırıcılık (Madde 158).....	28
1.6.1.2.13. Kumar oynanması için yer ve imkan sağlama (Madde 228)	29
1.6.1.2.14. Uyuşturucu veya uyarıcı madde kullanılmasını kolaylaştırma (Madde 190).....	29
1.6.1.2.15. Soruşturma Gizliliğinin ihlali (Madde 285)	29
1.6.1.2.16. Türk Milletini, Türkiye Cumhuriyeti Devletini, Devletin kurum ve organlarını aşağılama (Madde 301)	30
1.6.1.2.17. Siyasal veya askerî casusluk (Madde 328)	30
1.6.1.2.18. Diğer suçlar.....	31
1.6.2. Fikir ve Sanat Eserleri Kanununda Belirtilen Siber Suçlar	33
1.6.2.1. Maddi ve manevi haklara tecavüz (Madde 71).....	33

1.6.2.2. Koruyucu programları etkisiz kılmaya yönelik hazırlık hareketleri (Madde 72)	34
1.6.3. Elektronik İmza Kanununda Belirtilen Siber Suçlar	35
1.6.3.1. İmza oluşturma verilerinin izinsiz kullanımı (Madde 16)	35
1.6.3.2. Elektronik sertifikalarda sahtekârlık (Madde 17)	36
1.7. Dünyada Siber Suçlar.....	36
1.8. Siber Suç Farkındalığı.....	41
1.9. Problem Durumu.....	44
1.10. Alt Problemler.....	44
1.11. Araştırmanın Amacı.....	45
1.12. Araştırmanın Önemi.....	45
1.13. Sınırlılıklar	46
1.14. Varsayımlar	46
1.15. Tanımlar	46

İKİNCİ BÖLÜM

2. YÖNTEM.....	48
2.1. Araştırma Modeli	48
2.2. Evren ve Örneklem	48
2.3. Veri Toplama Araçları	49
2.4. Verilerin Toplanması	53
2.5. Verilerin Analizi.....	53

ÜÇÜNCÜ BÖLÜM

3. BULGULAR VE YORUM.....	54
3.1. Bilişim Bölümü Öğrencilerinin Demografik Özelliklerinin ve Ankete Verdikleri Yanıtların Genel Dağılımı İle İlgili Bulgular	54
3.2. Tespit Edilen Faktörlerin Demografik Özelliklere Göre Farklılaşması.....	65
3.2.1. “İnternetin Kişisel Değerlere Karşı Sakıncalarını Algılama” Faktörünün Cinsiyete Göre Farklılaşması	65
3.2.2. “Kişi ve Örgütlerin İnterneti Kötü Niyetle Kullanabileceklerini Algılama” Faktörünün Cinsiyete Göre Farklılaşması	66

3.2.3. “Öğrencilerin İnternetteki Rahatlık Seviyesi” Faktörünün Cinsiyete Göre Farklılaşması	67
3.2.4. “Öğrencilerin İnternette Aldıkları Önlem Seviyesi” Faktörünün Cinsiyete Göre Farklılaşması	67
3.2.5. “İnternetin Kişisel Değerlere Karşı Sakıncalarını Algılama” Faktörünün Sınıf Durumuna Göre Farklılaşması	68
3.2.6. “Kişi ve Örgütlerin İnterneti Kötü Niyetle Kullanabileceklerini Algılama” Faktörünün Sınıf Durumuna Göre Farklılaşması	69
3.2.7. “Öğrencilerin İnternetteki Rahatlık Seviyesi” Faktörünün Sınıf Durumuna Göre Farklılaşması	69
3.2.8. “Öğrencilerin İnternette Aldıkları Önlem Seviyesi” Faktörünün Sınıf Durumuna Göre Farklılaşması	70
3.2.9. “İnternetin Kişisel Değerlere Karşı Sakıncalarını Algılama” Faktörünün İnterneti Kullanma Yılına Göre Farklılaşması	71
3.2.10. “Kişi ve Örgütlerin İnterneti Kötü Niyetle Kullanabileceklerini Algılama” Faktörünün İnterneti Kullanma Yılına Göre Farklılaşması	72
3.2.11. “Öğrencilerin İnternetteki Rahatlık Seviyesi” Faktörünün İnterneti Kullanma Yılına Göre Farklılaşması	73
3.2.12. “Öğrencilerin İnternette Aldıkları Önlem Seviyesi” Faktörünün İnterneti Kullanma Yılına Göre Farklılaşması.....	74
3.2.13. “İnternetin Kişisel Değerlere Karşı Sakıncalarını Algılama” Faktörünün Siber Saldırıya Uğrama Durumuna Göre Farklılaşması.....	75
3.2.14. “Kişi ve Örgütlerin İnterneti Kötü Niyetle Kullanabileceklerini Algılama” Faktörünün Siber Saldırıya Uğrama Durumuna Göre Farklılaşması.....	75
3.2.15. “Öğrencilerin İnternetteki Rahatlık Seviyesi” Faktörünün Siber Saldırıya Uğrama Durumuna Göre Farklılaşması	76
3.2.16. “Öğrencilerin İnternette Aldıkları Önlem Seviyesi” Faktörünün Siber Saldırıya Uğrama Durumuna Göre Farklılaşması	77

DÖRDÜNCÜ BÖLÜM

4. SONUÇ VE ÖNERİLER.....	78
4.1. Sonuçlar	78
4.1.1. Bilişim Bölümü Öğrencilerinin Anket Sorularına Verdikleri Cevaplar İle Farkındalık Durum Sonuçları.....	79
4.1.2. Bilişim Bölümü Öğrencilerinin Cinsiyetleri ile Siber Suçları Algılama, İnternetteki Rahatlık Seviyesi ve İnternette aldıkları Önlem Seviyelerine İlişkin Sonuçlar	80
4.1.3. Bilişim Bölümü Öğrencilerinin Okudukları Sınıflar ile Siber Suçları Algılama, İnternetteki Rahatlık Seviyesi ve İnternette aldıkları Önlem Seviyelerine İlişkin Sonuçlar	81
4.1.4. Bilişim Bölümü Öğrencilerinin İnterneti Kullanma Yılları ile Siber Suçları Algılama, İnternetteki Rahatlık Seviyesi ve İnternette aldıkları Önlem Seviyelerine İlişkin Sonuçlar.....	81
4.1.5. Bilişim Bölümü Öğrencilerinin İnternette Saldırıya Uğrama Durumu İle Siber Suçları Algılama, İnternetteki Rahatlık Seviyesi ve İnternette Aldıkları Önlem Seviyelerine İlişkin Sonuçlar.....	81
4.2. Öneriler	82
KAYNAKÇA	83
EKLER.....	90
EK 1. İZİN BELGESİ.....	90
EK 2. ANKET FORMU	91
ÖZGEÇMİŞ.....	94

TABLÖLAR DİZİNİ

Tablo 2.1. Faktör Analizi.....	51
Tablo 3.1. Bilişim Bölümü Öğrencilerinin Demografik Özelliklerinin Frekans ve Yüzde Dağılımları	54
Tablo 3.2. Bilişim Bölümü Öğrencilerinin Likert Ölçekli Sorulara Verdikleri Cevapların Frekans ve Yüzde Dağılımları	57
Tablo 3.3. İnternetin Kişisel Değerlere Karşı Sakıncalarını Algılama Faktörünün Cinsiyete Göre Farklılaşması	65
Tablo 3.4. Kişi ve Örgütlerin İnterneti Kötü Niyetle Kullanabileceklerini Algılama Faktörünün Cinsiyete Göre Farklılaşması.....	66
Tablo 3.5. Öğrencilerin İnternetteki Rahatlık Seviyesi Faktörünün Cinsiyete Göre Farklılaşması	67
Tablo 3.6. Öğrencilerin İnternette Aldıkları Önlem Seviyesi Faktörünün Cinsiyete Göre Farklılaşması	67
Tablo 3.7. İnternetin Kişisel Değerlere Karşı Sakıncalarını Algılama Faktörünün Sınıf Durumuna Göre Farklılaşması	68
Tablo 3.8. Kişi ve Örgütlerin İnterneti Kötü Niyetle Kullanabileceklerini Algılama Faktörünün Sınıf Durumuna Göre Farklılaşması	69
Tablo 3.9. Öğrencilerin İnternetteki Rahatlık Seviyesi Faktörünün Sınıf Durumuna Göre Farklılaşması	69
Tablo 3.10. Öğrencilerin İnternette Aldıkları Önlem Seviyesi Faktörünün Sınıf Durumuna Göre Farklılaşması	70
Tablo 3.11. İnternetin Kişisel Değerlere Karşı Sakıncalarını Algılama Faktörünün İnterneti Kullanma Yılına Göre Farklılaşması	71
Tablo 3.12. Kişi ve Örgütlerin İnterneti Kötü Niyetle Kullanabileceklerini Algılama Faktörünün İnterneti Kullanma Yılına Göre Farklılaşması.....	72
Tablo 3.13. Öğrencilerin İnternetteki Rahatlık Seviyesi Faktörünün İnterneti Kullanma Yılına Göre Farklılaşması.....	73
Tablo 3.14. Öğrencilerin İnternette Aldıkları Önlem Seviyesi Faktörünün İnterneti Kullanma Yılına Göre Farklılaşması.....	74
Tablo 3.15. İnternetin Kişisel Değerlere Karşı Sakıncalarını Algılama Faktörünün Siber Saldırıya Uğrama Durumuna Göre Farklılaşması	75

Tablo 3.16. Kiři ve Örgütlerin İnterneti Kötü Niyetle Kullanabileceklerini Algılama Faktörünün Siber Saldırıda Uğrama Durumuna Göre Farklılaşması	75
Tablo 3.17. Öğrencilerin İnternetteki Rahatlık Seviyesi Faktörünün Siber Saldırıda Uğrama Durumuna Göre Farklılaşması	76
Tablo 3.18. Öğrencilerin İnternette Aldıkları Önlem Seviyesi Faktörünün Siber Saldırıda Uğrama Durumuna Göre Farklılaşması	77

KISALTMALAR DİZİNİ

ABD	: Amerika Birleşik Devletleri
BÖTE	: Bilgisayar ve Öğretim Teknolojileri Eğitimi
EİK	: Elektronik İmza Kanunu
FSEK	: Fikir ve Sanat Eserleri Kanunu
TCK	: Türk Ceza Kanunu
TEF	: Teknik Eğitim Fakültesi
TF	: Teknoloji Fakültesi
TDK	: Türk Dil Kurumu
ENIAC	: Electronic Numerical Integrator And Calculator
UNIVAC	: Universal Automatic Computer
ARPANET	: Advanced Research Projects Agency Network
www	: World wide web
http	: Hyper text transfer protocol
SSCB	: Sovyet Sosyalist Cumhuriyetler Birliği
IP	: İnternet Protokol
Spam	: Spiced park and ham
YTCK	: Yeni Türk Ceza Kanunu
BT	: Bilgisayar Teknolojisi
SPSS	: Sosyal Bilimler İçin İstatistik Programı

BİRİNCİ BÖLÜM

1. GİRİŞ

Geçmişten bu yana insan yaşamını birçok alanda kolaylaştıran teknolojik gelişmeler dün olduğu gibi bugün de önemini korumaya devam etmektedir. İnsanoğlu bir yandan karşılaştığı zorlukları yenmek amacıyla yeni teknolojilere ihtiyaç duyarken diğer yandan da bu teknolojilerin yarattığı sorunlarla da baş etmeyi öğrenmektedir. İnsan yaşamının her alanını derinden etkileyen bilgisayar teknolojisi de bu teknolojik araçlar arasında başta gelmektedir. 1950’lerde bir oda büyüklüğünde ve 30 ton ağırlığında olan bilgisayarlar zamanla evrilerek hızlanması sonucunda insanlar, kendi hayatlarını kolaylaştırmak için bilgisayar ve teknolojilerini nasıl daha üst düzeye çıkaracaklarının yolunu aramaya koyulmuşlardır. Bugün nihayetinde insanlık, bilgisayarı kendilerine bir yardımcı elemanmış gibi kullanarak;

- Klavye, fare, kamera faks, modem, tarayıcı, İnternet gibi unsurlarla bilgisayara veri girişi yapmışlardır.
- Sabit disk, disket, CD-ROM, DVD-ROM, gibi unsurlarla girilen verilerin saklanması sağlamışlardır.
- Merkezi işlem birimi (CPU) oluşturarak saklanan verilerin aynı zamanda işlenmesini sağlamışlardır.
- Ekran, yazıcı, çizici gibi unsurlarla da işlenen verinin bilgisayardan çıktısını alarak büyük bir iş yükünden kurtulmuşlardır (Akarslan, 2011).

Fakat zamanla insanların bilgisayardaki bu verileri başkaları ile paylaşma ihtiyacı gün yüzüne çıkmıştır. İnsanlar öncelikle yerel ve bölgesel ağlarla sınırlı sayıda bilgisayarı birbirine bağlayarak yerel ve bölgesel düzeyde bilgi paylaşımı sağlayabilmişlerdir. Bu yerel ve bölgesel ağlarla daha büyük bir ağ oluşturarak dünyadaki bütün bilgisayarların birbirine bağlanması amaçlanmıştır. Bu amaçla İnternet denen ulusal ağ ortaya çıkmıştır. 1960’lardan günümüze kadar hızla gelişen İnternet ABD’den dünyaya yayılmıştır. Bu yayılma diğer teknolojik buluşların yayılmasından daha hızlı bir şekilde gerçekleşmiştir. Bu teknolojiyle beraber toplum ihtiyaçlarının

giderilme yolları da oldukça kolaylaşmıştır. İletişimden alışverişe, bankacılık işlemlerinden eğitime kadar birçok ihtiyacımız İnternet ortamında giderilebilir hale gelmiştir. Yaşam şartları ağırlaşan dünyamızda insanoğlunun omuzlarına her geçen gün başka bir yük yüklendiği düşünülürse, bu yüklerin üstesinden gelmek için İnternet teknolojisi olmazsa olmazlarımızdandır. Ülkeler, yaşamımızdaki tüm olaylara müdahil olan İnternet ile e-yaşam standartlarına ulaşp bilgi toplumu haline dönüşmeyi hedeflemektedirler. Ancak İnternet teknolojisinin insanoğlu için avantajları kadar dezavantajlarının olduğu da bir gerçektir. İnternetin hayatımıza girmesinden önce normal hayatta karşımıza çıkan etik sorunlar, İnternetin hayatımıza girmesinden sonra sanal ortamda karşımıza çıkmıştır (Torun, 2007).

İnternet de diğer teknolojik gelişmeler gibi insanlık yararına kullanıldığı sürece faydalıdır. Fakat toplumda İnterneti insanlık yararına kullananların yanı sıra İnterneti insanlığa maddi-manevi zarar vermek için de kullananların olduğu bilinmektedir. Kötü niyetli insanlar da İnternet gibi teknolojik gelişmeleri takip ederler ve teknolojinin kolaylıklarından faydalanarak işleyeceği suçu daha kolay ve daha gizli bir şekilde gerçekleştirirler. Bu tip insanların teknolojiyi takip etmesi sonucu ortaya çıkan siber suç kavramı hızla tüm dünyaya yayılmaktadır. Bu suçların yayılması, İnternetin daha geniş perspektifte kullanılmasına engel olmaktadır (Broadhurst, 2006). Tabi ki İnternet ve bilgisayar dünyasındaki tüm olumlu gelişmelerde olduğu gibi siber suç konusu da, tüm dünyaya ABD'den yayılmıştır. Siber suç tarihi 1960'lara dayanır ki o zamanlarda teknolojinin derinlemesine işlenememesi siber suç kavramının da yüzeysel kalmasını sağlamıştır. 1980lere doğru bilgisayarlar sabote edilmiş, bilgisayar sistemleri illegal olarak kullanılmış ve korsan kişiler yavaş yavaş bilgisayar ve İnternet ortamına girmeye başlamışlardır. Teknolojinin hızla gelişmesi ile insanlar daha fazla kötülük işleyebileceği alanlar bulabilmektedirler (Duymaz, 2013). Dolayısıyla siber suçlar da gün geçtikçe daha değişik varyasyonlarla karşımıza çıkmaya başlamışlardır. Günümüzde siber suçlarla verilen zararlardan bahsederken milyar dolarların telaffuz edilmesi küresel bir sorunun habercisi olarak algılanmaktadır. Ülkelerin ekonomik kayıpların önüne geçmesi için devlet yatırımlarını siber güvenlik alanına da kaydırmaları gerekmektedir (Silva, 2013).

1.1. Siber Suç İle İlgili Tanımlar

1.1.1. Bilişim Kavramı

Kelime anlamı olarak “değişken bilgi” anlamına gelen bilişim sözcüğü Türkçe’ye Fransızca “informatique” kelimesinden esinlenerek girmiştir (Yenidünya ve Değirmenci, 2003). Bu sözcük, Fransa’da bilgi ve otomatik kavramlarının birleşmesiyle oluşmuştur. Otomatik olarak elde edilen bilgi yani otomatik bilgi demektir. Türkçeye enformasyon olarak geçen bu terim zamanla bilişim anlamında da kullanılmıştır. TDK’ya göre bilişim sözcüğünün genel anlamı; insanoğluna bilimsel olarak veya iletişim için gerekli bilgilerin elektronik cihazlar aracılığıyla düzenli ve uygun bir şekilde işlenmesidir (Nacar, 2010). Bilginin saklanması, saklanan bilgiye erişilmesi, istenildiği zaman başka bir yere aktarılması ve işlenmesi aşamaları bilişim olgusu kapsamında gerçekleşen olaylardır. Artık hayatımızda gerçekleşen çoğu toplumsal ve ekonomik olaylar bilişim alanı içerisinde gerçekleşmektedir. Bu alanı tek bilgisayarlar olarak ta düşünebiliriz, bilgisayarların toplu olarak bağlı oldukları bir ağ olarak ta düşünebiliriz (Akıncı, Alıç ve Er, 2004). Bu haliyle bilişimin temel unsurları olarak bilgisayar ve İnternet karşımıza çıkmaktadır.

1.1.1.1. Bilgisayar

Bilgisayar birçok aritmetiksel ve mantıksal işleme dayalı işleri önceden yüklenmiş programlara göre yapıp sonuçlandıran elektronik cihazlardır (Türkiye Dil Kurumu [TDK], 2014). Bilgisayar sadece verilen emirleri programlara dayalı olarak yerine getiren aletler değil aynı zamanda yüklenen bilgilerin depolanarak istenildiği zaman kullanıcıya tekrar geriye sunan aygıtlardır (Akarslan, 2012). Bilgisayar ilk olarak 1940’larda üretilmiştir ve boyutu yaklaşık olarak bir bina büyüklüğündedir. 1946 yılında Amerikan ordusu tarafından genel amaçlı kullanmak için üretilen ilk bilgisayarın ismi ENIAC’tır (Hennessy ve Patterson, 2007). 1951’de ilk ticari amaçlı üretilen bilgisayar olan UNIVAC üretilmiştir (Yazıcıoğlu, 1997). Sonraki yıllarda bilgisayarın fiziki ve yazılımsal unsurları geliştirilerek şu anki haline getirilmiştir.

Bilgisayarlar yazılım ve donanım elemanlarından oluşmaktadır. Bilgisayarın donanım elemanları; somut kavramlar olan, gözle görülebilen giriş çıkış birimleridir

(Topaloğlu, 1997). Ancak bilgisayar sadece bu donanım elemanları ile çalışamazlar. Bu donanım elemanlarının yönetilebilmesi gerekli olan yazılım programlarına ihtiyaç vardır. Yazılım programları, elektronik araçların donanım birimleri arasında veya elektronik cihazların kendi aralarındaki irtibatın sağlanması için verilen makine komutlarıdır (Topaloğlu, 1997).

1.1.1.2. İnternet

İnternet, dünyadaki insanların birbirleriyle iletişim kurmaları ve veri alışverişinde bulunmalarını sağlayan uluslar arası bir ağıdır. Kelime olarak “International Network” kelimelerinden türemiştir. 1950 yıllarında ABD ve SSCB arasındaki soğuk savaş esnasında Amerikan ordusu, askeri bilgilerin ana bilgisayar dâhilinde diğer bilgisayarlarda da görülmesi ve tüm birimlerin birbirleriyle kesintisiz iletişim kurabilmeleri için bir ağ geliştirmeye karar vermiştir (Lloyd, 2000). Deneme aşamasından sonra ARPANET uygulamaya konmuştur. Amerika daha sonra bu ağı sivil halkın kullanımına açmıştır. 1990’larda www teknolojisi ve bu teknolojinin dayandığı http protokolü geliştirildikten sonra ARPANET yaygın kullanım alanını kaybetmiştir (İçel, 2001). İnternete bağlanıp iletişim ve veri alışverişini sağlamak uluslar arası kabul görmüş bu http protokolleri sayesinde olur. Her İnternet sitesinin bağlı olduğu bir bilgisayar vardır ve bu bilgisayarın IP adresi vardır. IP adresleri aaa.bbb.ccc.ddd şeklinde dört gruptan oluşur. Bu sayı grupları 1 ‘den 250’ye kadar değişebilmektedir. İlk kısım bağlı olunan network adresi, son kısım ise bağlı olunan bilgisayar hakkında bilgi vermektedir (Ergün, 2008). Bir İnternet sayfasına girmemize imkân sağlayan çeşitli sağlayıcılar vardır. Bu sağlayıcıları biz görmeyiz ama bu sağlayıcılar sayesinde İnternet’e ulaşabiliriz. Bu sağlayıcılar; sitelerin içeriğini belirleyen içerik sağlayıcılar, başkalarına ait bilgilerin İnternete aktarılmasını sağlayan erişim sağlayıcılar ve başkalarına ait verilerin depolanabileceği bilgisayarlara sahip olan servis sağlayıcılardır (Kurt, 2005)

1.1.2. Bilişim Suçu

Bilişim suçları ülkemizde değişik isimlerle bilinmektedir. İnternet suçları, bilgisayar suçları, dijital suçlar, siber suçlar gibi kavramlar bilişim suçları kapsamındaki

suçları ifade etmek için kullanılırlar. Avrupa’da ise genel olarak “cyber crime” olarak kullanılmaktadır (Pocor, 2004). Avrupa Ekonomik Topluluğu Uzmanlar Komisyonunu tarafından 1983 yılı Mayıs ayında Paris’te yapılan toplantıda bilişim suçları şu şekilde tanımlanmıştır; “Bilgilerin otomatik olarak işleme tabi tutulduğu veya verilerin nakline yarayan bir sistemde gayri kanuni, gayri ahlaki veya yetki dışı gerçekleştirilen her türlü davranıştır.” Bilişim suçları, bilişim sistemleri ile işlenen veya bilişim sistemlerinin hedef alındığı suçlardır (Durmaz, 2006). Yani bilişim suçları ikiye ayrılır: Birincisi bilişim sistemlerini araç olarak kullanıp işlenen suçlardır. Bu suçlar bilişim sistemleri aracılığıyla yapılan taciz, tehdit, şantaj, hırsızlık, dolandırıcılık, hakaret, fuhuş, kumar oynanması için yer ve imkân sağlama, müstehcenlik, cinsel istismar, intihara yönlendirme gibi suçlardır. İkincisi bilişim sistemlerinin direk hedef tahtasına konulduğu suçlardır. Bu tür suçlarda bilişim sistemlerindeki veriler izinsiz olarak kaydedilir, değiştirilir, silinir veya kullanılır.

1.1.3. Siber Kavramı

Siber sözcüğü, İngilizce “cyber” kelimesinden Türkçeye girmiştir. Türkçede genellikle siber ile bilişim sözcükleri aynı anlamda kullanılmaktadır. Kelime anlamı olarak bilgisayar ve İnternetle ilgili olan anlamına gelmektedir. Çoğu zaman siber ile bilişim kelimeleri aynı anlamda kullanılsa da aralarında farklılık vardır (Çakmak ve Demir, 2009). Peker’e (2010) göre; “Siber, bilgisayar ve buna bağlı elektronik sistemlerin bulunduğu ortam; bilişim ise bu ortamdan etkin olarak faydalanma ve bu ortam aracılığıyla bilgi üretilmesidir.”

1.1.4. Siber Suç

Siber suç terimi de bilişim suçu gibi farklı isimler ile anılabilmektedir. Sanal suç, İnternet suçu, bilgisayar suçu, bilişim suçu bunlardan bazılarıdır. Ama siber suç terimi bu suç tiplerinin tamamını kapsayıcı niteliktedir (Yazıcıoğlu, 2002). Zaten uluslararası literatürde de genel olarak “ciber crime” yani “siber suç” terimi kullanılmaktadır. Bizim yaptığımız bu çalışmada bilgisayar suçları, bilişim sistemlerinin hedef olarak seçildiği suçlar, bilişim sistemlerinin aracılığıyla işlenen suçlar, İnternet

suçları ve bilgisayara bağlı elektronik sistemlerde gerçekleşen suçları incelediğimiz için kapsayıcı bir terim olan “siber suç” kavramı kullanılmıştır.

Yazıcıoğlu’na (2002) göre; bilgisayar ve bilgisayar ağıları aracılığıyla siber uzayda yapılan hukuk dışı eylemler siber suçun tanımını oluşturmaktadır. Akyazı, Dilmen ve Kara ise (2008) siber suçun tanımını şöyle yapmışlardır:” Yapılan herhangi bir kanunsuz eylemde bilgisayar veya bilgisayara bağlı elektronik sistemlerin araç veya hedef olarak seçilmesi siber suçtur.” Siber suç kavramını ülkemizdeki mevcut yasa maddeleri ile örneklendirecek olursak;

- İntihara yönlendirme (TCK madde 84)
- Çocukları cinsel istismarı (TCK madde 103)
- Cinsel taciz (TCK madde 105)
- Tehdit (TCK madde 106)
- Şantaj (TCK madde 107)
- Haberleşmenin engellenmesi (TCK madde 124)
- Hakaret (TCK madde 125)
- Haberleşmenin gizliliğini ihlal (TCK madde 132)
- Kişiler arasındaki konuşmaların dinlenmesi ve kayda alınması (TCK madde 133)
- Özel hayatın gizliliğini ihlal (TCK madde 134)
- Kişisel verileri kaydedilmesi (TCK madde 135)
- Verileri hukuka aykırı olarak verme veya ele geçirme (TCK madde 136)
- Nitelikli hırsızlık (TCK madde 142)
- Nitelikli dolandırıcılık (TCK madde 158)
- Müstehcenlik (TCK madde 226)
- Fuhuş (TCK madde 227)
- Kumar oynanması için yer ve imkân sağlama (TCK madde 228)
- Maddi-manevi haklara tecavüz (FSEK madde 71)
- Bilgisayar koruma programlarını etkisizleştirmeye yönelik eylemler (FSEK madde 72)
- İmza oluşturma verilerine habersiz ulaşım (EİK madde 16)

- Elektronik ortamda verilen sertifikalarda yapılan sahtekârlık (EİK Madde 17)

siber suç sınıfına giren suç çeşitlerinden bazılarıdır.

1.1.5. Suç Kavramı

Suç, topluma ve muhatabı olduğu kişilere zararının olduğu kanunlarla onaylanmış hareket ve fiillerdir (Dönmezer, 1981). Diğer bir deyişle kanun koyucunun yasakladığı fiillerin insanlar tarafından gerçekleştirilmesidir (Bostancı, 2011). Yapılan fiilin suç olabilmesi için yapılan eylemle sonucun arasında bir neden sonuç ilişkisinin olması gerekir. Ayrıca yapılan fiil ile yapan kişi arasında manevi bir unsurun olması gerekir. Yapılan fiilin kusurlu olması fiil ile kişi arasındaki manevi boyutu belirler. Son olarak yapılan fiilin, kanunlarda suç sayılan fiiller arasına girmesi gerekir (Gözübüyük, 1988).

1.2. Geleneksel Suç İle Siber Suç Arasındaki Farklar

Geleneksel suçlarla siber suçlar arasında yoğunlaşılan nokta, suçluların ortaya çıkarılması, zaman ve mekân kavramlarına tabi olmaları, işleniş biçimleri, cezaları açısından birçok farklılık vardır.

- Geleneksel suç olayında suçluyu bulup ortaya çıkarma eğilimli bir çalışma yapılır siber suç olayında ise asıl dikkatlerin yoğunlaştığı nokta suçtur (Peker, 2010).
- Suçluların ortaya çıkarılması açısından geleneksel suç olayında olayı ortaya çıkaracak personel için çok fazla teknik bilgiye gerek yokken siber suç olayında suçu inceleyen personelin yeteri kadar teknik bilgiye sahip olmaması durumunda suçluların ortaya çıkarılması zordur.
- Siber suçlarda mağdurların gerekli mercilere başvurması, geleneksel suçlara göre daha azdır. Geleneksel suçlarda suçlunun ortaya çıkarılma ümidi daha fazladır, insanlar yasalara daha fazla güvenirler ve dolayısıyla şikâyetçi olma konusunda siber suç mağdurlarına göre daha isteklidirler (Akarslan, 2012).
- Suçun işlenmesinden sonra bırakılan iz konusunda geleneksel suçlarda genelde yeteri kadar iz bulunurken, siber suçlarda suçu işleyen kişiler genelde iz bırakmazlar zaten bıraksalar bile bırakılan bu izlere ulaşmak çok zordur.

- Geleneksel suçlar siber suçlara göre daha eski bir tarihe sahip oldukları için geleneksel suçlarda suç kavramları ve ceza oranları oturmuş iken siber suçlarda bir belirsizlik vardır.
- Geleneksel suçlarda zaman, mekân kavramları konusunda net veriler elde edilirken siber suçlarda zaman ve mekân konusu net değildir. Kıtalar ötesinden zaman kavramı fazla önemsenmeden siber suç olgusu gerçekleşebilir (Peker, 2010).
- Geleneksel suçların maddi boyutu genellikle fazla yüksek değildir. Ama siber suçların maddi boyutu geleneksel suçlara göre daha fazladır.
- Siber suçların mağduru geleneksel suçlara göre daha fazladır. Toplumun tamamı bile bazen gerçekleşen bir siber suçun mağduru olabilmektedir (Akarslan, 2012).
- Geleneksel suçlara göre siber suçların geçmişi çok eski tarihlere dayanmamaktadır. Siber suçlar son otuz yılda teknolojinin hızlı bir şekilde gelişmesiyle yaygınlaşmıştır.
- Siber suçların maddi ve manevi etkilerinin yüksek olabilme potansiyelinden dolayı verilen cezalar farklıdır.
- Siber suçların işlenmesi geleneksel suçlara göre daha kolay bir şekilde olur (Demircan, 2007).
- Siber suçlar gelişen teknolojiyle arttığı için hızla artan bir yapısı vardır. Dolayısıyla geleneksel suçlara göre siber suçlarla mücadele etmek daha fazla zorlaşmaktadır.
- Geleneksel suçlardan mağdur olan kesim tüm halktır. Ama siber suçlardan mağdur olan kesim teknolojiyi sıklıkla kullanan kesimdir. Bilişim sistemlerine uzak olan ülke ve topluluklar siber suçlardan fazla etkilenmeyecektir (Akarslan, 2012).

1.3. Siber Suçun Tarihçesi

Siber suç, bilgisayarın ve İnternetin dünyada yaygınlaşması ile ortaya çıkmış bir suç türüdür. Dünya’da gerçekleşen ilk siber suç 1966 yılında Amerika’da gerçekleşmiştir. Banka hesabında tahrifat yapan bir bilgisayar uzmanı siber suç işleyen ilk kişi olarak kayıtlara geçmiştir (Aydın, 1992). Yine 1973 yılında ABD’nin Los Angeles eyaletinde yapılan dolandırıcılık olayında altmış dört bin adet sahte müşteri

kaydı yapılarak o zamana kadar yapılan en büyük siber suç gerçekleştirilmiştir (Johnson, 2005). 1995 yıllarında Amerika’da siber savaş komutanları yetiştirilmeye başlanmıştır. Siber suçların en hızlı bir şekilde arttığı ülkelerden biri olan ABD’ de siber suçlara karşı alınan önlemlerde de en ön saftadır. Bunun en önemli örneği, savunma bakanlığını siber saldırılara karşı korumak ve gerektiği zaman siber operasyonlar yapmak amacıyla Siber komutanlığın (CYBERCOM) kurulmasıdır (Yayla, 2013). Siber suçların yaygınlaşması dünya ülkelerini tedbirler almaya zorlamıştır. ABD ve Avrupa Konseyi üye ülkeleri yaptıkları yasal değişiklikler ve düzenlemeler ile yaşanan sıkıntıların önüne geçmek istemişlerdir. Hazırlanan sözleşmeler ile uluslar arası boyut kazanan siber suç kavramına karşı tüm ülkelerin ortak bir payda da buluşmaları amaçlanmıştır. 2001 yılında Avrupa Konseyi bünyesinde hazırlanan “Avrupa Siber Suç Sözleşmesi” Avrupa nezdinde hazırlanmış en kapsamlı siber suç sözleşmesidir. NATO’da ise Estonya’nın 2007’de maruz kaldığı saldırıdan sonra “NATO Siber Savunma Politikası” kabul edilmiş ve Lizbon’da yapılan zirve sonrası siber savunma konusunun gündemde sürekli olarak tutulması kararı alınmıştır (Yayla, 2013). Türkiye’de siber suçla mücadelede üyesi olduğu kuruluşların kararlarını baz alıp kendi mevzuatındaki eksiklikleri gidermekle başlamıştır (Akbulut, 1999). İlk olarak 1991 yılında TCK’ya bazı siber suçları ihtiva eden “Bilişim Alanında Suçlar” bölümü eklenmiştir (Kurt, 2005). Yine 1995 yılında Fikir ve Sanat Eserleri Kanunu siber suçların bir bölümünü kapsayacak şekilde değiştirilmiştir (Dülger, 2004). Elektronik İmza Kanunu ile de 2004 yılında çeşitli siber suçlara karşı önlem alınmaya çalışılmıştır. 2007’de kabul edilen İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun ile siber suç sayılabilecek yayınlara karşı önlem alınmaya çalışılmıştır (Horozgil, 2012). 2008’de çıkarılan Elektronik Haberleşme Kanunu ile Siber Güvenlik Kurulu ve görevlerine atıfta bulunulmuştur (Uz, 2013).

1.4. Siber Suçun Sınıflandırılması

1.4.1. Veri Suçları

Verilere yönelik suçlar verilerin çalınması, durdurulması, bozulması, değiştirilmesi ve silinmesi şeklinde olmaktadır. Veri sahipleri en büyük mağduriyeti verilerin bozulması değiştirilmesi ve silinmesi suçlarında görürler.

1.4.1.1. Verilerin çalınması

Bilişim sistemindeki verilerin haksız kazanç sağlayarak çalan kişiye veya üçüncü bir kişiye menfaat sağlanması için veya veri sahibinin mağduriyet yaşayacak şekilde verinin kullanılması şeklinde işlenen bir suçtur (Kurt, 2005).

1.4.1.2. Verilerin durdurulması

Bilişim sistemindeki verilerin aktarılması esnasında hak sahibini mağdur edecek şekilde veri aktarımının engellenmesi şeklinde işlenen suçtur.

1.4.1.3. Verilerin bozulması

Verilerin aktarılması esnasında veya muhafaza edildiği yerde tahrip edilerek kullanılamayacak hale getirilmesi şeklinde işlenen suçtur.

1.4.1.4. Verilerin değiştirilmesi

Verilerin aktarılması esnasında veya muhafaza edildiği yerde hukuka aykırı bir şekilde değiştirilerek hak sahibi kişilerin mağdur edilmesi şeklinde işlenen suçtur (Turhan, 2006).

1.4.1.5. Verilerin silinmesi

Bilişim sistemindeki verilerin veri sahibini veya üçüncü kişileri mağdur edecek şekilde bilişim sisteminden silinmesi şeklinde işlenen suçlardır. Verilerin silinmesi, veri sahibi kişilerin çok büyük kayıplara uğramasına neden olan veri suçlarından birisidir.

1.4.2. Yetkisiz erişim suçları

Herhangi bir bilişim sistemine izinsiz ve hukuka aykırı bir şekilde tamamına, bir bölümüne veya verilerin olduğu kısma erişilmesi şeklinde işlenen suçlardır. Bilişim sistemlerine yetkisiz erişim, yetkisiz dinleme, virüs bulaştırma ve hesapların ihlal edilmesi bu kapsamda işlenen suçlardır.

1.4.2.1. Yetkisiz erişim

Bir bilişim sistemine yetkisi olmayan kişiler tarafından giriş yapılarak bilişim sistemindeki verilere izinsiz ve hukuka aykırı bir şekilde ulaşmak yetkisiz erişim suçudur (Nacar, 2010). Kişiler bilişim sistemlerine mekân ve zaman kavramlarına bağlı kalmaksızın erişim sağlayabilirler.

1.4.2.2. Yetkisiz dinleme

Bilişim sistemlerinin haberleşmede de kullanılması dünya genelinde iyice yaygınlaşmıştır. Ayrıca çoğu haberleşme cihazlarının bilgisayar ve bilişim sistemleri ile entegre bir şekilde çalışmaları yetkisiz dinleme suçunu yaygınlaştırmıştır. Ayrıca ortam dinleme cihazları yardımıyla herhangi bir iletişim aracı kullanmaksızın bile yetkisiz dinleme suçu gerçekleştirilmektedir. Genellikle telekomünikasyon sistemi ile iletişim halinde olan kişilerin veri alışverişlerinin takibi şeklinde işlenen suçlardır (Kurt, 2005).

1.4.2.3. Hesap ihlali

Kişilerin bilişim sistemlerindeki hesaplarına kişilerin rızası ve haberi olmadan erişilmesi şeklinde işlenen suçlardır. Kişilerin Facebook, Twitter ve diğer sosyal paylaşım hesaplarının ihlal edilmesi en çok yaygın olan erişim suçlarından.

1.4.2.4. Virüs bulaştırma

Bilişim sistemlerine zarar vermek amaçlı oluşturulan zararlı programların oluşturularak bilişim sistemlerine değişik yollarla bulaştırılması şeklinde işlenen suçlardır. Sonuçları itibari ile suç boyutu belli edilir. Genel olarak geniş toplumsal kitleleri etkileyebilecek bir suç türüdür (Kurt, 2005).

1.4.3. Ağ Suçları

Bilişim sistemleri arasındaki veri aktarımını sağlamak amacıyla kurulan ağları hedef alan suç türleridir (Beceni ve Uçkan, 2004). Ağların sabotajı ve ağların engellenmesi şeklinde gerçekleşir.

1.4.3.1. Ağların sabotajı

Söz konusu ağların fiziksel olarak değiştirilip zarar verilmesi sonucu kullanılamaz hale getirilmesi şeklinde işlenen suçlardır (Beceni ve Uçkan, 2004).

1.4.3.2. Ağların engellenmesi

Bilgisayarlara yönlendirilmiş sistemlere sürekli veri gönderimi yapılarak söz konusu sistemlere diğer kişilerin girmesini engelleme şeklinde işlenen suçlardır (Turhan, 2006). Web sitelerine erişimin engellenmesi veya hack olayları en çok görülen ağ engellenmesi suçlarıdır.

1.4.4. Bilgisayarla İlgili Diğer Suçlar

1.4.4.1. Bilgisayar aracılığıyla dolandırıcılık ve hırsızlık

Bilişim sistemleri üzerinde yapılacak veri değişikliği, veri hırsızlığı yollarıyla mağdurun büyük maddi kayıplara uğratılması şeklinde işlenen suçlardır. Sahte siteler oluşturularak kişinin gerçek sitede yaptığı işlemlerin bu sahte sitede yapılmasını sağlayan suçlular, mağdurun tüm bilgilerini öğrenip mağduru dolandırma yoluna gitmektedirler. Genelde bilişim sistemleri aracılığıyla yapılan mali işlerde dolandırıcılık ve hırsızlık söz konusu olabilmektedir. Kredi kartı bilgilerinin alınması, hesap bilgilerinin alınması, sahte maillerle mağdura maddi kayıplar yaşatacak eylemlerin yaptırılması bilgisayar aracılığıyla yapılan dolandırıcılık suçuna örnektir.

1.4.4.2. Bilgisayar aracılığıyla sahtecilik

Bilişim sistemleri aracılığıyla web sitelerinin, sanal belgelerin, maillerin, hesapların aslına benzer bir şekilde benzerini yapıp bu öğelerin asıl sahiplerini mağdur

etmek veya maddi manevi kazanç sağlamak suçluların asıl hedefidir (Akıncı vd, 2004). Sahtecilik suçu, teknolojinin ilerlemesiyle oldukça yaygın ve profesyonelce işlenen bir suç haline dönüşmüştür.

1.4.4.3. Bilgisayar sabotajı

Bilgisayar sabotajı suçundan suçlular hem bilişim sistemleri ve ağlarını kullanarak hem de direk bilgisayarın donanımsal unsurlarına fiziksel müdahale ile bilgisayardaki verilere zarar verebilirler. Burada önemli olan fiziksel malın gördüğü zarar değil içerikte bulunan verilerin gördüğü zarardır (Burden ve Palmer, 2003).

1.4.4.4. Bilgisayar yazılımlarının kullanımı

Telif hakkı başkalarında olan ürünlerin kopyalanarak çoğaltılması, kullanılması, satılması, dağıtılması şeklinde işlenen suçlardır (Demircan, 2007). FSEK ile devlet bu tür suçların önüne geçmek istemektedir. Yazılımların izinsiz kullanılması ve kopyalanması en yaygın işlenen siber suçlardan bir tanesidir. Ürünlerinin orijinallerinin yüksek fiyatlardan satılması korsan ürünlerin satışını artıran nedenlerin başında gelmektedir. Ayrıca insanların korsan ürünlere kolayca ulaşabilmeleri korsan ürünlerin günlük hayatta kullanımını artırmıştır (Bilek, 2012). Bu suçun üç değişik şekilde işlenmesi söz konusudur.

1.4.4.4.1. Yazılımların kural dışı kullanılması

Lisanslı bir şekilde alınan yazılımların birden çok bilgisayarda kullanılmasının yasak olduğu sözleşmesinde belirtilmesine rağmen sözleşmeye bağlı olarak kullanılmaması şeklinde işlenen suçlardır (Turhan, 2006).

1.4.4.4.2. Yazılımların kural dışı çoğaltılması

Herhangi bir yazılım ve eserin lisans sözleşmesinde söz konusu eseri alan kişinin birden fazla çoğaltamayacağı yazmaktadır. Eserlerin ve yazılımların birden fazla çoğaltılması söz konusu kişiyi suçlu duruma düşürmektedir (Koç ve Kaynak, 2009). Yazılım ve eserlerin kural dışı çoğaltılması ile mağdurların büyük maddi kayıpları söz

konusu olur. Mağdurların maddi kayıplarının yanında manevi olarak ta üretim yapma heveslerinin kırılması gibi bir durumla karşı karşıya kalırlar.

1.4.4.4.3. Yazılımların kural dışı kiralınması

Yazılım ve eserlerin lisans sözleşmelerine aykırı bir şekilde kiralınması olarak karşımıza çıkmaktadır. En yaygın şekli oyun ve film eserlerinin kurallarına uymadan kiralınmasıdır.

1.4.4.5. Yasadışı yayınlar

Kanun koyucu tarafından yayınlanması, dağıtılması yasaklanmış her türlü yayının bilişim sistemleri ve ağları aracılığıyla yayınlanması şeklinde işlenen suçlardır. Web siteleri, mail hesapları, forumlar aracılığıyla bu yasadışı yayınlar yayınlanabilmektedir. Genel olarak terörist grupların bu yolla bağlı oldukları terörist faaliyetlerin propagandasını yapmaya çalıştıkları görülmektedir (Tulum, 2006). Normal şartlarda yapmaya zorlandıkları propaganda eylemini bu yasa dışı yayınlarla daha kolay yapabilmektedirler.

1.4.4.6. Terörist faaliyetler

Terör örgütlerinin propaganda, haberleşme, saldırı gibi faaliyetlerini gerçekleştirirken bilişim sistemleri ve ağlarını kullanması siber suçun bir çeşidi olarak karşımıza çıkmaktadır. Terör örgütleri normal hayatta yaptıkları illegal faaliyetlerin hemen hemen hepsini siber ortamda da yapabilmektedirler. Terör örgütü için yardım toplamak, terör örgütüne eleman sağlamak, örgüt içi haberleşmeyi sağlamak, kişileri tehdit etmek, devleti karalayarak haksız davalarını haklıymış gibi göstermek, baskı ve iftiralarla isyan ve düzene karşı başkaldırıya teşvik etmek, eylem emri vermek gibi birçok yasadışı faaliyet terör örgütü tarafından bilişim sistemlerinin vasıtasıyla yapılır (Atıcı ve Gümüş, 2003). Terör örgütleri özellikle şehir merkezlerindeki haberleşme faaliyetlerini gerçekleştirirken bilişim sistemlerini kullanırlar. Bu yasadışı işlerin gerçekleştirilmesi esnasında suçluların kolay bir şekilde bulunamaması için İnternet kafeler tercih edilir. Yapılan terörist saldırılarda bireyler hedef alınacağı gibi kitlelerde hedef alınabilmektedir (Zarplı, 2008).

1.4.4.7. Çocuk pornografisi

Daha kendi karar verecek yaşa gelmemiş kişilerin müstehcen bir şekilde fotoğraf çektilirerek veya videolarının çekilmesiyle yöntemiyle uygunsuz görüntülerinin bilişim sistemleri ve ağları yardımıyla yayınlanması veya dağıtılması siber suç kapsamına girmektedir. 15 yaşını geçmemiş kişilerin pornografik video ve resimlerinin yayınlanması çocuk pornografisi olarak adlandırılmaktadır (Bilek, 2012). Bu siber suç çeşidi, uluslar arası pazarda büyük paraların döndüğü (Seigfried-Spellar, Lovely ve Rogers, 2011) ve genelde örgütlerin rağbet gösterdiği bir piyasadır (Özbek, 2002). Teknolojinin gelişmesiyle insanların ahlaki açıdan sınır tanımayan arzuları fırsatlara dönüşebilmektedir. Teknolojik gelişmelerin verdiği imkânlarla insanlar istediği resim ve videoları istediği anda sisteme yükleyebilir, yayınlatabilir ve izleyebilirler. Dolayısıyla çocukların masumiyetini koruyabilmek amacıyla bu tür insanların yakalanıp adalet önüne çıkarılması çok önemlidir.

1.4.4.8. Satılması yasak ürünlerin ticareti

Bilişim sistemleri ve ağları kullanılarak normal hayatta satışı yasak veya kontrollü olan ürünlerin satışı kolaylıkla yapılabilmektedir. Kadın ticareti, çocuk ticareti, uyuşturucu ticareti, organ ticareti, silah ticareti İnternette daha kolay yapılabilmesinden dolayı çoğu zaman siber suçları konusu olmuştur.

1.4.4.8.1. Kadın ticareti

Görsel iletişimde rahatlıkla yapılabileceği sanal ortam kadın ticareti yapmak isteyenlerin uğrak yeri olmuştur. Fuhşa sürüklenen kadınlara İnternet ortamında chat yaptırılıp, fotoğraf ve video yükletilmesi yoluyla müşteri bulmaları sağlanmaktadır (Csonka, 2000).

1.4.4.8.2. Çocuk ticareti

Dilendirilmek ve organlarına sahip olabilmek amacıyla kaçırılan çocukların takibi ve bebek sahibi olamayan ailelerin bilişim sitemleri ve ağları aracılığıyla durumu

iyi olmayan ailelerin çocuklarını satın almaları şeklinde gelişen suçlardır. Üçüncü sınıf ülkelerde rastlanan bir siber suç çeşididir.

1.4.4.8.3. Organ ticareti

Özellikle maddi durumu iyi olmayan insanların organlarını bilişim sistemlerini kullanarak para karşılığında başkalarına satmak, almak veya aracı olmak siber suç çeşididir. Çeşitli İnternet sitelerinde, forum sitelerinde veya sosyal paylaşım sitelerinde organların pazarlanması söz konusu olmaktadır. Bu suçun muhatapları ya durumları iyi olmayan kişiler veyahut kaçırılmış çocukların ve fakir insanların organlarını satan simsarlardır.

1.4.4.8.4. Uyuşturucu ticareti

Gençlerin en büyük düşmanı olan uyuşturucu ile mücadele bütün devletlerin sürdürdüğü politikaların başında gelmektedir. Emniyet olarak narkotik masanın baktığı bu suçlar alınan tedbirlerin ardından yapılması zor bir hale gelmiştir. Uyuşturucu ticareti yapan suç örgütleri alınan tedbirlere karşılık sanal alemini kullanarak daha rahat bir hareket alanı bulmuşlardır. Özellikle iletişim ve pazarlama konusunda bilişim sistemlerini kullanan uyuşturucu örgütleri e-ticareti kendi sektörlerine rahatlıkla uyarlamışlardır. Aynı şekilde uyuşturucu kullanıcıları da uyuşturucu temini için riskin daha az olduğu sanal ortamları tercih etmektedirler.

1.4.4.8.5. Silah ticareti

Bilişim sistemlerinin kullanılması ile kayıt dışı silah satışının gerçekleştirilmesi siber suçtur. Silah satışı normal de devlet denetimi altında taşıma ve bulundurma ruhsatları ile satılmakta ve takip edilmektedir. Ama sanal ortamda yapılan silah satışlarının herhangi bir kaydı yoktur. Devlet tarafından bu silahların takibi yapılamamaktadır. Normal yollardan silah alamayan kişiler bu şekilde illegal yollara başvurumaktadırlar. Suç örgütlerinin de bu şekilde silah temin etmesi gayet kolaydır.

1.5. Siber Suçların İşleniş Şekilleri

Kendilerini bilişim konusunda geliştirmiş kötü niyetli insanlar bu kötü niyetlerini değişik yöntemlerle siber ortama yansıtmaktadırlar. Bu kişilerin başvurduğu belli başlı yöntemler şunlardır:

1.5.1. Bilişim Korsanlığı

Bilişim sistemine yetkisi olmayan kişilerin girip verilerin kontrol edilip, değiştirilip veya ele geçirilmesi yoluyla siber suçun işlenmesidir. Bu işi yapan kişiler hacker veya bilişim korsanı olarak adlandırılır. Yaptıkları iş ise hackleme olarak adlandırılır. Bilişim korsanları sisteme girdikleri zaman ya varlıklarını hissettirmeden veri kontrolü yaparlar yada sisteme girip verileri değiştirerek sistemi ele geçirirler. Karşıt görüşlü kişilerin karşılıklı birbirlerinin sitelerini hacklemeleri sıkça görülen bir olaydır. Hacker gruplar genelde genç yaşta kişilerden oluşur ve bu işi çoğu zevk için yapar. Diğer siber suç işleniş şekillerinden ayıran tarafı işin bizzat bilişim korsanı olarak adlandırılan kişi tarafından yapılmasıdır. Bilişim korsanlarının yarısına yakın bir bölümünü bilişim alanında çalışan kişiler oluşturur (Yazıcıoğlu, 1997). Bilişim korsanları hedeflerini belirledikten sonra ilk yaptıkları iş hedefleri hakkında bilgi toplamaktır. Daha sonra saldıracakları hedeflerin zayıf noktalarını belirlemeye çalışırlar. Yöntemin belirlenmesiyle beraber bilişim korsanları sisteme girerler. Sisteme giren bilişim korsanının ilk hedefi sistemde olduğunu fark ettirmeden sistemde kalmaya devam etmektir. Hedefine ulaşan bilişim korsanı daha sonra arkasında iz bırakmadan sistemden çıkmak ister. Sistemden çıkmadan önce sisteme girdiğini gösteren bütün belirtileri yok eder (Akarslan, 2012).

1.5.2. Gizli Kapılar

Sistemi oluşturan yazılımcıların sisteme uzaktan veya güvenlik önlemlere takılmadan girebilmesi için koyduğu açık kapılardır. Bu açık kapılar sadece sistemi oluşturan kişi tarafından bilinir (Yazıcıoğlu, 1997). Bu kapılara gizli kapı veya arka kapı adı da verilmektedir. Kötü niyetli kişiler bu gizli kapıları keşfetmeleri ile sisteme rahatlıkla girebilirler.

1.5.3. Ağ Solucanları

Ağ solucanları herhangi bir programa gerek duymadan sistemden sisteme, dosyadan dosyaya kendini aktaran yazılımlardır. Sisteme veya bilgisayara bir kez girmesi yeterlidir daha sonra kendi yolunu bularak çoğalır. Ağ solucanlarının en büyük handikabı hızlı bir şekilde çoğalmasındır (Kurt, 2005). Sisteme girdikten sonra hızlı bir şekilde çoğalır ve sistemi yavaşlatır hatta sistemi çökertme seviyesine bile getirebilir. Ağ solucanları virüslerden farklı olarak komutsuz hareket edebilmektedirler. Solucanlar sisteme girdikten sonra komut beklemezler aynı şekilde sistemden diğer sistemlere ilerlemek içinde komut beklemezler (Akarslan, 2012)

1.5.4. Truva Atı

Sistemin arka planında yararlı bir dosya gibi görünüp asıl yazılımcısı tarafından bilgisayarın yönetilmesini sağlar. Masum bir programın açılmasından bilgisayarımıza aktarılabilir. İnternette bilgisayarımıza indirdiğimiz programlardan da giriş yapabilir. Bilgisayara animasyon veya değişik program şeklinde girdikten sonra asıl kendisini oluşturan kullanıcının emrinde çalışır. Kendi kullanıcısının emriyle aktarıldığı bilgisayardaki verileri silebilir, değiştirebilir, yönetildiği bilgisayara verileri ve şifreleri aktarabilir. Bu yapılan işlemler aktarılan bilgisayarın kullanıcısı tarafından anlaşılmaz. Çünkü bu Truva atı yazılımı her açıldığında masum yazılımlar gibi işlevini görür (Değirmenci, 2002). Solucanlardan farklı olarak çoğalma ve yayılma durumları söz konusu değildir.

1.5.5. Mantık Bombaları

Sisteme girdikten sonra Truva atı gibi zararsızmış gibi görünüp belirli bir tarihten sonra sisteme tamamen zarar vermek amaçlı çalışan bir yazılım türüdür. Mantık bombaları yıkıcı ve zararlı yazılımlardır. Kurulum programları veya diğer masum programlarla beraber sisteme girerler. Mantık bombaları gibi tavşanlarda sistemi yavaşlatan saldırı türüdür (Berry, 2003). 1999 Çernobil virüsü bir mantık bombası mantığında hareket etmiş ve kısa zamanda çoğu dünya ülkesine ulaşmıştır. Her sene 26 Nisan'da aktif hale gelen bu mantık bombası sisteme işlemez bir hale sokmaktadır.

1.5.6. Salam Tekniđi

Truva atı yazılımları kullanılarak banka sistemlerindeki çok küçük miktardaki işlem kusuratlarının başka bir banka hesabında biriktirilmesi ve bu olayın birçok işlemde tekrarlanması ile failler söz konusu hesaplarında hiçte azımsanmayacak miktarda para birikimi yaparlar (Alaca, 2008).

1.5.7. İstem Dışı Elektronik Postalar (Spam)

Deđişik yollarla elde edilen mail adreslerine zararlı olmayan spamların karřıdakinin kişinin isteđi olmadan zoraki bir şekilde gönderilmesidir. Bu spamların içeriğinde ticari reklam amaçlı ürünlerin tanıtımı veya pornografik reklamlar olabilir. Bu spamlar yardımıyla reklam yapmak isteyen kişiler çok geniş kitlelere ulaşabilirler. Spamlar sistemleri yoktan yere meşgul etmekte ve servis sağlayıcıları için ekstra maddi külfet oluşturmaktadırlar (Özdilek, 2002). Bu spamların içeriğinde yasalara aykırı herhangi bir propaganda yapılması veya spamların yoğunluğundan dolayı sistemin kullanılamaz hale gelmesi durumlarında sistemin engellenmesi gündeme getirilerek buna göre işlem yapılmaktadır (Kurt, 2005).

1.5.8. Çöpe Dalma

Çöpe dalma, gerek donanım birimlerinin gerekse yazılım birimlerinin işlem yapmalarından sonra geride kalan artık verilerin toplanması yoluyla işlenen siber suç çeşitleridir. Yazıcıdan alınan çıktıların üzerinde olan veriler veya sistemdeki çöp kutusuna gönderilmiş verilerin üst düzey yöntemlerle geri getirilerek elde edilmesi işlemi söz konusudur (Yazıcıođlu, 1997).

1.5.9. Tarama

Tarama sistemleri aracılığıyla IP numaralarını taraması yapıp bilişim sitemlerine bađlı bilgisayarların bu yolla bulunması yöntemidir. Aynı yöntem giriş şifrelerinin bulunması içinde kullanılabilir (Kurt, 2005).

1.5.10. Oltaya Gelme

Oltaya gelme yöntemi, gerçek hayatta balıkçıların oltaya yem takıp balığı beklemesi olayına benzetildiği için bu ismi almıştır. Suçluların sahte maillerle veya gerçeklerine tıpa tıp benzer İnternet sayfaları ile mağdurları beklemesi söz konusudur. Suçlular özellikle banka hesap numaraları ve şifreleri gibi işlerine yarayacak bilgileri sahte maillerle elde etmeye çalışırlar. Ayrıca yüksek benzerlikli İnternet sayfaları sayesinde mağdurların şüphelerini çekmeden işlerini yürütürler (Akarslan, 2012).

1.6. Türk Ceza Kanununda Siber Suçlar

İnternet ve İnternet suçlarının hızla yayılması tüm dünyada olduğu gibi ülkemizde de yankı bulmuştur. Bu hızlı yayılmanın bir sonucu olarak ortaya çıkan siber suçlar, hukuk sistemine yeni bir kavram sokmuştur. Bu yeni kavramın hukuk sistemine entegrasi kanun koyucular tarafından yapılmaktadır. Ülkemiz siber suç olgusuyla diğer ülkelere göre daha geç tanıştığı için hukuksal olarak diğer ülke mevzuatlarından faydalanarak siber suçlarla mücadele altyapısını oluşturmuştur (Dülger, 2004). 5237 sayılı Yeni Türk Ceza Kanununda (YTCK), 5846 sayılı Fikir ve Sanat Eserleri Kanununda (FSEK) ve 5070 sayılı Elektronik İmza Kanununda (EİK) düzenlenen maddelerle siber suç sayılabilecek fiillerin önüne geçilmek istenmiştir. 1 Haziran 2005 tarihinde yürürlüğe giren Yeni TCK'da da “Bilişim Alanında Suçlar” başlığı altında toplanan kanun maddeleri düzenlenmiş ve siber suçlar konusu ele alınmıştır. Bu maddelerin yanı sıra YTCK 'da ki diğer bazı kanun maddelerinin de bilişim sistemleri ile işlenme olasılığı vardır. Ama bu suçlar sadece siber suç olarak adlandırılmazlar (Dülger, 2004). Bu maddelerde belirtilen suçların işlenmesi aşamasında bilişim sistemlerinin doğrudan veya dolaylı olarak kullanılması söz konusudur.

1.6.1. Yeni Türk Ceza Kanununda Belirtilen Siber Suçlar

Yeni Türk Ceza Kanunda siber suçlar “Topluma Karşı İşlenen Suçlar” kısmının 10. bölümünde bulunan “Bilişim Alanındaki Suçlar” başlığı altında belirtilmiştir. Bu bölümdeki kanun maddeleri belirtildikten sonra bilişim sistemleri ile işlenebilecek suçları içeren diğer kanun maddeleri de belirtilecektir.

1.6.1.1. “Bilişim alanındaki suçlar” başlığı altındaki kanun maddeleri

1.6.1.1.1. Bilişim sistemine girme (Madde 243)

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

(2) Yukarıdaki fıkrada tanımlanan fiillerin bedeli karşılığı yararlanılabilen sistemler hakkında işlenmesi halinde, verilecek ceza yarı oranına kadar indirilir.

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

Bu madde ile kişilerin bilişim sistemine hukuka aykırı bir şekilde girmesi, sistemdeki verilerin değiştirilmesi, silinmesi, tahrip edilmesi gibi şartlar aranmaksızın suç kabul edilmiştir (İlbaş, 2009). Suçun sonucunda ortaya çıkacak durumlara bakılmadan suç işlenmiş sayılacaktır (Soyaslan, 2005). Suçun sonucunda ortaya çıkan ve ceza gerektiren diğer durumlar için ayrıca ceza verilecektir (Dülger, 2004). Bunun yanı sıra kişilere sisteme girişleri için verilen sürenin ihlal edilmesi de bu kanun maddesi kapsamında suç sayılmaktadır (Meran, 2008). Avrupa ve dünyada siber suç kavramını hukuk mevzuatlarına entegre eden ülkelerin hemen hemen tamamı bilişim sistemine girme eylemini suç kabul etmiştir. Teknolojinin gelişmesiyle özel hayatın, sırların ve kişisel verilerin bilişim sistemine aktarılması gerçekleşmiş böylelikle başkasının bilişim sistemine girme eylemi özel hayata müdahale anlamına gelmiştir (Akarslan, 2012). Sisteme girilerek öğrenilen bilgi ve sırlar, muhatap kişi ve kurumlara maddi olarak zarar vermektedir. Dolayısıyla bu kanun maddesi ile kişi ve kurumların maddi kayıpları da önlenmek istenmiştir (Ketizmen, 2008).

1.6.1.1.2. Sistemi engelleme, bozma, verileri yok etme veya değiştirme (Madde 244)

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

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

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

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

Bu maddede kişilerin sisteme girerek kendilerine ait olmayan sistem verileri değiştirip veya bozmak kaydıyla sisteme erişimin engellenmesi söz konusudur. Kanun maddesinde belirtilen fiillerin herhangi birinin gerçekleştirilmesi suçun meydana gelmesi için yeterli bir sebeptir (Alacakaptan, 1975). Kişiler hazırladıkları virüslerle sistemin işleyişini değiştirirler. Yine bu virüslerle sistemdeki verilerin üzerinde istedikleri eylemi gerçekleştirebilirler. Bu kanun maddesi ile bilgisayar sabotajlarının engellenerek sistemin çalışmasına herhangi bir engel çıkarılmaması hedeflenmiştir (Parlar ve Hatipoğlu, 2008). Kişiler sistemi engelleyerek, verileri silip tahrip ederek muhatap kişi ve kurumların elde edecekleri maddi yararları sınırlandırabilirler (Kardaş, 2003). Bu kanun maddesi ile bunun önüne geçilmek istenmiştir.

1.6.1.1.3. Banka veya kredi kartlarının kötüye kullanılması (Madde 245)

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

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

(3) Sahte oluşturulan veya üzerinde sahtecilik yapılan bir banka veya kredi kartını kullanmak suretiyle kendisine veya başkasına yarar sağlayan kişi, fiil daha ağır

cezayı gerektiren başka bir suç oluşturmadığı takdirde, dört yıldan sekiz yıla kadar hapis ve beşbin güne kadar adlî para cezası ile cezalandırılır.

(4) Birinci fıkra da yer alan suçun;

a) Haklarında ayrılık kararı verilmemiş eşlerden birinin,

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

c) Aynı konutta beraber yaşayan kardeşlerden birinin,

Zararına olarak işlenmesi hâlinde, ilgili akraba hakkında cezaya hükmolunmaz.

(5) Birinci fıkra kapsamına giren fiillerle ilgili olarak bu kanunun malvarlığına karşı suçlara ilişkin etkin pişmanlık hükümleri uygulanır.”

Banka ve kredi kartlarının art niyetli insanlar tarafından ele geçirilmesi veya sahte kartların basılması yoluyla muhatap kişiye yüklü miktarda maddi zarar verilebilmektedir. Ayrıca var olmayan bir hesap veya kart oluşturularak bankaların maddi kayba uğratılması da söz konusu olabilmektedir (Dülger, 2004). Sahte kartlar basılırken iki değişik yol izlenebilmektedir. Ya gerçek kişiler üzerine sahte kartlar yada sahte kimlikler üzerine sahte kartlar basılır. Basılan bu sahte kartlar alınan birçok önleme rağmen bankaları yanıltılabilmektedir (Nuhoğlu, 2002). Sahte kartların oluşturulması, asıl kartların ele geçirilerek kullanılmasından farklı düşünülmektedir (Parlar ve Hatipoğlu, 2008). Kredi ve banka kartlarının kopyalanması eyleminde; yapan kişilerin herhangi birinde uzmanlık olup olmadığına bakılmaktadır (Taşkın, 2008). Aynı aileden kişilerin birbirlerinin banka ve kredi kartlarını habersizce kullanması ceza gerektirmez (Dönmezer, 2001). Ama dışarıdan bir kişinin iştiraki o kişinin ceza almasına engel değildir.

1.6.1.1.4. Tüzel kişiler hakkında güvenlik tedbiri uygulanması (Madde 246)

“(1) Bu bölümde yer alan suçların işlenmesi suretiyle yararına haksız menfaat sağlanan tüzel kişiler hakkında bunlara özgü güvenlik tedbirlerine hükmolunur.”

Bu madde ile tüzel kişiliklerin söz konusu kanun maddeleri ile muhatap olması durumu belirtilmiştir.

1.6.1.2. Yeni Türk ceza kanununda belirtilen diğer siber suçlar

1.6.1.2.1. Çocukların cinsel istismarı (Madde 103)

“(1) Çocuğu cinsel yönden istismar eden kişi, üç yıldan sekiz yıla kadar hapis cezası ile cezalandırılır.”

1.6.1.2.2. Müstehcenlik (Madde 226)

“(1) Bir çocuğa müstehcen görüntü, yazı veya sözleri içeren ürünleri veren ya da bunların içeriğini gösteren, okuyan, okutan veya dinleten kişi altı aydan iki yıla kadar hapis ve adli para cezası ile cezalandırılır.”

Bu kanun maddeleri YTCK’da çocuk pornografisini önlemek için yerini almış kanun maddeleridir. 103. Maddede geçen çocuk kelimesinden 15 yaşını henüz doldurmamış veya doldurmuş olmasına rağmen yapılan fiillerin hukukiliğini ve hukuki sonuçlarını algılayamayan çocuklar kastedilmektedir. Çocukların bilişim sistemleri aracılığıyla müstehcen görüntü ve yayınlarının yayınlanması veya yayınlanması için aracılık edilmesi bu kanun maddeleri gereği cezalandırılmaktadır (Erbaşı, 2007). Ayrıca çocukları cinsel açıdan istismar eden kişiler, bilişim sistemleri aracılığıyla sözel istismar, teşhircilik, röntgencilik fiillerini de gerçekleştirebilmektedirler (Turla ve Özkanlı, 2006).

1.6.1.2.3. Kişisel verilerin kaydedilmesi (Madde 135)

“(1) Hukuka aykırı olarak kişisel verileri kaydeden kimseye bir yıldan üç yıla kadar hapis cezası verilir.”

Kişilerin, herhangi bir kurum, kuruluş veya bir site aracılığıyla bilgilerinin izinsiz kaydedilmesi ve bu bilgilerin başka kişilerin ellerine geçmesi muhatap kişiyi maddi ve manevi kayıplarla yüz yüze bırakabilmektedir. Bilgilerin ait olduğu kişinin rızasının olmaması ve yasal bir dayanağın olmaması söz konusu eylemi suç haline getirmektedir (Karagülmez, 2009).

1.6.1.2.4. Verileri hukuka aykırı olarak verme veya ele geçirme (Madde 136)

“(1) Kişisel verileri, hukuka aykırı olarak bir başkasına veren, yayan veya ele geçiren kişi, iki yıldan dört yıla kadar hapis cezası ile cezalandırılır.”

Hukuka uygun bir şekilde kaydedilmiş olan kişisel verilerin bilişim sistemleri aracılığıyla 3. şahıslara iletilmesi siber suç olarak kabul edilmektedir (Taşkın, 2008). Aynı şekilde kişilerin çeşitli sitelere istekleri ile verdikleri bilgilerin hukuka aykırı bir şekilde ele geçirilmesi siber suç sayılmaktadır (Dülger, 2004). Zararın oluşup oluşmadığına bakılmaksızın söz konusu fiillerin gerçekleşmesi ceza için yeterli sebeptir (Dülger, 2004).

1.6.1.2.5. Verileri yok etmeme (Madde 138)

“(1) Kanunların belirlediği sürelerin geçmiş olmasına karşın verileri sistem içinde yok etmekle yükümlü olanlara görevlerini yerine getirmediklerinde bir yıldan iki yıla kadar hapis cezası verilir.”

Kişilerin çeşitli nedenlerle kurum veya kuruluşlara kişisel bilgilerini vermelerinden sonra belirlenen süreler boyunca bu bilgilerin kaydı tutulabilir. Bu verilere her zaman ulaşılabilirliğin olmaması için belirlenen süreler sonunda veriler yok edilmelidir (İlbaş, 2009). Bu türde bir suç, kamu davası ile görülmektedir. Yani kişinin rızasının olup olmaması suçun oluşması için önemli değildir (Dülger, 2004).

1.6.1.2.6. Haberleşmenin engellenmesi (Madde 124)

“(1) Kişiler arasındaki haberleşmenin hukuka aykırı olarak engellenmesi halinde, altı aydan iki yıla kadar hapis veya adli para cezasına hükmolunur.

(2) Kamu kurumları arasındaki haberleşmeyi hukuka aykırı olarak engelleyen kişi, bir yıldan beş yıla kadar hapis cezası ile cezalandırılır.

(3) Her türlü basın ve yayın organının yayınının hukuka aykırı bir şekilde engellenmesi halinde, ikinci fıkra hükmüne göre cezaya hükmolunur.”

Teknolojinin gelişmesiyle kişilerin haberleşme için kullandıkları araçlarda değişme göstermektedir. Bilişim sistemlerinin haberleşmeyi kolaylaştırma konusunda

büyük katkısı olmuştur (Dülger, 2004). Ama diğer haberleşme araçlarında olduğu gibi bilişim sistemleri ile yapılan haberleşmede de kişiler çeşitli engellemelerle karşı karşıya kalabiliyorlar. Kişilerin e-postalar, telekonferanslar ve değişik çoklu ortam programları ile yaptıkları haberleşmenin hukuka aykırı bir şekilde engellenmesi suç oluşturur (Kurt, 2005).

1.6.1.2.7. Haberleşmenin gizliliğini ihlal (Madde 132)

“(1) Kişiler arasındaki haberleşmenin gizliliğini ihlal eden kimse, bir yıldan üç yıla kadar hapis cezası ile cezalandırılır. Bu gizlilik ihlali haberleşme içeriklerinin kaydı suretiyle gerçekleşirse, verilecek ceza bir kat artırılır.

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

Kişilerin haberleşme araçları ile yaptıkları haberleşme kişilerin özeldir. Herhangi bir şüphe olmadan ve gerekli mahkemelerden gerekli izinler alınmadan kişilerin yaptıkları haberleşmeler dinlenemez, gün yüzüne çıkarılamaz ve 3. şahıslara aktarılamaz (Akarslan, 2012). Kanun koyucu, söz konusu kanun maddesi ile kişilerin yaptıkları haberleşmenin gizliliğini ihlal edenleri cezalandırmaktadır. Bilişim sistemleri ile yapılan haberleşmenin gizliliğini ihlal ederek siber suç işleyen kişiler bu kanun maddesi ile cezalandırılmaktadır.

1.6.1.2.8. Kişiler arasındaki konuşmaların dinlenmesi ve kayda alınması (Madde 133)

“(1) Kişiler arasındaki aleni olmayan konuşmaları, taraflardan herhangi birinin rızası olmaksızın bir aletle dinleyen veya bunları bir ses alma cihazı ile kaydeden kişi, iki yıldan beş yıla kadar hapis cezası ile cezalandırılır.

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

Son yıllarda gittikçe yaygınlaşan ortam dinlemeleri, kişi ve kurumları maddi ve manevi yönden oldukça etkilemektedir. Bilgisayarlarda yapılan bu ortam dinlemelerinde doğrudan veya dolaylı olarak kullanılmaktadırlar (Akarslan, 2012).

Kişilerin çeşitli ortamlara koydukları dinleme cihazlarını bilişim sistemleri ile entegre bir şekilde kullanıp ortamdaki kişilerin konuşmalarını dinlemeleri ve kayıt altına almaları siber suç oluşturmaktadır.

1.6.1.2.9. Özel hayatın gizliliğini ihlal (Madde 134)

“(1) Kişilerin özel hayatının gizliliğini ihlal eden kimse, bir yıldan üç yıla kadar hapis cezası ile cezalandırılır. Gizliliğin görüntü veya seslerin kayda alınması suretiyle ihlal edilmesi halinde, verilecek ceza bir kat artırılır.

(2) Kişilerin özel hayatına ilişkin görüntü veya sesleri hukuka aykırı olarak ifşa eden kimse iki yıldan beş yıla kadar hapis cezası ile cezalandırılır. Ifşa edilen bu verilerin basın ve yayın yoluyla yayımlanması halinde de aynı cezaya hükmolunur.”

Kişilerin özel hayatlarına ait görüntü veya videolar, bilişim sistemleri aracılığıyla çok rahat bir şekilde ifşa edilebilmektedir (Akarslan, 2012). Özellikle İnternet siteleri bu amaçla kullanılabilir. Bahse konu görüntülerin kişinin rızası olmadan çeşitli bilişim sistemleri aracılığıyla yayımlanması siber suç olarak sayılmaktadır (Taşkın, 2008).

1.6.1.2.10. Hakaret (Madde 125)

“(1) Bir kimseye onur, şeref ve saygınlığını rencide edebilecek nitelikte somut bir fiil veya olgu isnat eden veya sövmek suretiyle bir kimsenin onur, şeref ve saygınlığına saldıran kişi, üç aydan iki yıla kadar hapis veya adlî para cezası ile cezalandırılır.

(2) Fiilin, mağduru muhatap alan sesli, yazılı veya görüntülü bir iletiyle işlenmesi halinde, yukarıdaki fıkrada belirtilen cezaya hükmolunur.”

Söz konusu kanun maddesinin 2. fıkrasında da belirtildiği gibi çeşitli görüntü ve ses kayıtlarıyla 3. kişilere hakaret edilmesi siber suç sayılmaktadır. Kişilerin haysiyet ve şerefleri, bilişim sistemleri aracılığıyla yapılan yayınlarla zedelenebilmektedir (Dülger, 2004). Kanun koyucu bu tür suçlarla mücadele için ilgili kanun maddesini yürürlüğe sokmuştur.

1.6.1.2.11. Nitelikli hırsızlık (Madde 142)

“(2) Hırsızlık suçunun;

e) Bilişim sistemlerinin kullanılması suretiyle,

işlenmesi hâlinde, üç yıldan yedi yıla kadar hapis cezasına hükmolunur.”

Hukuk literatüründe hırsızlık fiilinin kamu kurumu, ibadethane gibi özel kurumlarda gerçekleşmesi veya kamu malı gibi özel eşyalar üzerinde gerçekleşmesi veya bilişim sistemleri, resmi bir unvan kullanılarak gerçekleşmesi durumlarında “Nitelikli Hırsızlık” terimi kullanılmaktadır. Dolayısıyla bilişim sistemlerinin kullanılması aracılığıyla yapılan hırsızlık nitelikli hırsızlık sınıfına girer ve siber suç sayılır. Söz konusu maddenin 2. bendinin “e” fıkrasında bu durum belirtilmiştir (Noyan, 2005). Bilişim sistemleri hırsızlık olaylarında doğrudan veya dolaylı olarak kullanılabilir. Kişiler bilişim sistemlerini kullanarak banka hesaplarını doğrudan boşaltabilmektedirler. Ayrıca yine kişiler, güvenlik alarmlarını bilişim sistemleri aracılığıyla devre dışı bırakarak hırsızlık yapabilmektedirler.

1.6.1.2.12. Nitelikli dolandırıcılık (Madde 158)

“(1) Dolandırıcılık suçunun;

f) Bilişim sistemlerinin, banka veya kredi kurumlarının araç olarak kullanılması suretiyle işlenmesi halinde, iki yıldan yedi yıla kadar hapis ve beşbin güne kadar adli para cezasına hükmolunur. Ancak, (e), (f), (j) ve (k) bentlerinde sayılan hâllerde hapis cezasının alt sınırı üç yıldan, adli para cezasının miktarı suçtan elde edilen menfaatin iki katından az olamaz.”

Dolandırıcılık suçunun da bilişim sistemleri aracılığıyla yapılması “Nitelikli Dolandırıcılık” olarak adlandırılmıştır. Bu durum söz konusu maddenin 1. bendinin “f” fıkrasında belirtilmiştir. Bilişim sistemleri aracılığıyla çeşitli hileli uygulamalar gerçekleştirilip kişi veya kurumların dolandırılması siber suç sınıfına girmektedir. Bilişim sistemleri kullanılarak daha kapsamlı ve daha çözülmesi zor dolandırıcılık vakaları gerçekleşebilmektedir (Akarslan, 2012). Bununla birlikte bilişim sistemleri ile yapılan dolandırıcılıkların maddi kaybı da fazla olmaktadır. Günümüzde e-ticaretin

yaygınlaşması ile bilişim yoluyla yapılan dolandırıcılık vakaları da artmıştır (Nacar, 2010).

1.6.1.2.13. Kumar oynanması için yer ve imkan sağlama (Madde 228)

“(1) Kumar oynanması için yer ve imkan sağlayan kişi, bir yıla kadar hapis ve adli para cezası ile cezalandırılır.”

Teknolojinin gelişmesi ile kumar oynanan yerlerde bu değişimden nasibini almışlardır. Bilişim sistemleri ile bahis ve kumar oynamak isteyen kişiler yer ve imkan bulmakta zorlanmamaktadırlar. Siber uzayın büyüklüğü bu kişiler için avantaj sağlamaktadır. Aynı şekilde bahis ve kumar oynatmak isteyen kişiler de, denetimin az olduğu siber ortamdaki sitelerle bu emellerini çok rahat bir şekilde gerçekleştirebilmektedirler. Genelde yurt dışından yönetilen bu siteler sayesinde failler rahat bir şekilde hareket edebilmektedirler (Akarslan, 2012). Bu konuda ülkelerin işbirliği yaparak evrensel boyutta önlemler almaları gerekmektedir.

1.6.1.2.14. Uyuşturucu veya uyarıcı madde kullanılmasını kolaylaştırma (Madde 190)

“Uyuşturucu veya uyarıcı madde kullanılmasını alenen özendiren veya bu nitelikte yayın yapan kişi, iki yıldan beş yıla kadar hapis cezası ile cezalandırılır.”

Çeşitli İnternet siteleri aracılığıyla kişilerin uyuşturucu ve uyarıcı madde kullanmaları için özendirici resim, ses ve görüntü yayınlamaları siber suç oluşturmaktadır. Gençlerin sanal ortamda fazlaca vakit geçirmeleri, en büyük düşmanları olan uyuşturucu ve uyarıcı maddeler ile de bu ortamda tanışmalarına neden olabilmektedir.

1.6.1.2.15. Soruşturma Gizliliğinin ihlali (Madde 285)

“(1) Soruşturmanın gizliliğini alenen ihlal eden kişi, bir yıldan üç yıla kadar hapis veya adli para cezası ile cezalandırılır.”

Kişiler, bilişim sistemleri aracılığıyla çeşitli ses kayıtları, görüntü ve videolar yayınlarak soruşturma ve kavuşturma aşamasında Türk bağımsız mahkemelerini

etkileyebilmektedirler. Özellikle çeşitli haber sitelerinde bitmemiş soruşturma ve kavuşturma aşamasındaki davalar hakkında yapılan haberler siber suç sayılmaktadır. Kanun koyucu çeşitli yasa maddeleri ile bu şekilde işlenebilecek siber suçların önüne geçmek istemiştir.

1.6.1.2.16. Türk Milletini, Türkiye Cumhuriyeti Devletini, Devletin kurum ve organlarını aşağılama (Madde 301)

“(1) Türk Milletini, Türkiye Cumhuriyeti Devletini, Türkiye Büyük Millet Meclisini, Türkiye Cumhuriyeti Hükümetini ve Devletin yargı organlarını alenen aşağılayan kişi, altı aydan iki yıla kadar hapis cezası ile cezalandırılır.

(2) Devletin askerî veya emniyet teşkilatını alenen aşağılayan kişi, birinci fıkra hükmüne göre cezalandırılır.”

Özellikle devletin bölünmez bütünlüğüne karşı olan kişi ve örgütler tarafından devlet kurum ve kişilerinin aşağılanması söz konusu olabilmektedir. Kişi ve örgütlerin bu amaç doğrultusunda bilişim sistemleri aracılığıyla çeşitli ses ve görüntü üretip yayınlamaları siber suç oluşturmaktadır.

1.6.1.2.17. Siyasal veya askerî casusluk (Madde 328)

“(1) Devletin güvenliği veya iç veya dış siyasal yararları bakımından, niteliği itibarıyla, gizli kalması gereken bilgileri, siyasal veya askerî casusluk maksadıyla temin eden kimseye on beş yıldan yirmi yıla kadar hapis cezası verilir.”

Son zamanlarda ülkemizde ve tüm dünyada gündemde olan bu suç, ülkeler için iç ve dış güvenlik sorunu, ekonomik istikrarsızlık gibi sorunlara neden olabilmektedir. Ülkelerin askeri ve siyasi politika konularında gizli kalması gereken bilgilerinin çeşitli İnternet siteleri aracılığıyla tüm dünya ülkelerine servis edilmesi çok tehlikeli bir siber suç oluşturabilmektedir. Bilgiler, bilişim sistemleri aracılığıyla çok kısa zamanda çok geniş kitlelere ulaştırılabilmektedir. Buda ülkelerin gizli kalması gereken bilgilerinin kısa zamanda geniş kitleler tarafından öğrenilmesi anlamına gelmektedir ki bu ülkeler için büyük bir handikaptır.

1.6.1.2.18. Diğer suçlar

YTCK’da belirtilen suçlardan bazılarını kişiler bilişim sistemleri aracılığıyla doğrudan veya dolaylı olarak işleyebilmektedirler. Günümüz şartlarında en çok karşımıza çıkan siber suç çeşitleri yukarıda belirtilmiştir. Bunun yanı sıra bilişim sistemlerinin kullanılması yoluyla işlenebilecek diğer suçlar kanun maddeleri ile beraber aşağıda belirtilmiştir.

- İnsan ticareti (Madde 80)
- İntihara yönlendirme (Madde 84)
- Organ veya doku ticareti (Madde 91)
- Tehdit (Madde 106)
- Şantaj (Madde 107)
- Nefret ve ayrımcılık (Madde 122)
- Kişilerin huzur ve sükûnunu bozma (Madde 123)
- Haksız fiil nedeniyle veya karşılıklı hakaret (Madde 129)
- Kişinin hatırasına hakaret (Madde 130)
- Şirket veya kooperatifler hakkında yanlış bilgi (Madde 164)
- Bozulmuş veya değiştirilmiş gıda veya ilaçların ticareti (Madde 186)
- Kişilerin hayatını ve sağlığını tehlikeye sokacak biçimde ilaç yapma veya satma (Madde 187)
- Uyuşturucu veya uyarıcı madde imal ve ticareti (Madde 188)
- Resmi belgede sahtecilik (Madde 204)
- Özel belgede sahtecilik (Madde 207)
- Suç işlemeye tahrik (Madde 214)
- Suçu ve suçluyu övme (Madde 215)
- Halkı kin ve düşmanlığa tahrik veya aşağılama (Madde 216)
- Kanunlara uymamaya tahrik (Madde 217)
- Suç işlemek amacıyla örgüt kurma (Madde 220)
- Fuhuş (Madde 227)
- Fiyatları etkileme (Madde 237)

- Ticarî sır, bankacılık sırrı veya müşteri sırrı niteliğindeki bilgi veya belgelerin açıklanması (Madde 239)

- Tefecilik (Madde 241)
- Görevi kötüye kullanma (Madde 257)
- Göreve ilişkin sırrın açıklanması (Madde 258)
- Yargı görevi yapanı, bilirkişiyi veya tanığı etkilemeye teşebbüs (Madde 277)
- Suç delillerini yok etme, gizleme veya değiştirme (Madde 281)
- Cumhurbaşkanı hakaret (Madde 299)
- Devletin egemenlik alametlerini aşağılama (Madde 300)
- Devlete karşı savaşa tahrik (Madde 304)
- Halkı askerlikten soğutma (Madde 318)
- Askerleri itaatsizliğe teşvik (Madde 319)
- Savaşta yalan haber yayma (Madde 323)
- Devletin güvenliğine ilişkin belgeler (Madde 326)
- Devletin güvenliğine ilişkin bilgileri temin etme (Madde 327)
- Devletin güvenliğine ve siyasal yararlarına ilişkin bilgileri açıklama (Madde

329)

- Gizli kalması gereken bilgileri açıklama (Madde 330)
- Uluslararası casusluk (Madde 331)
- Devlet sırlarından yararlanma, Devlet hizmetlerinde sadakatsizlik (Madde

333)

- Yasaklanan bilgileri temin (Madde 334)
- Yasaklanan bilgilerin casusluk maksadıyla temini (Madde 335)
- Yasaklanan bilgileri açıklama (Madde 336)
- Yasaklanan bilgileri siyasal veya askerî casusluk maksadıyla açıklama

(Madde 337)

- Devlet güvenliği ile ilgili belgeleri elinde bulundurma (Madde 339)
- Yabancı devlet bayrağına karşı hakaret (Madde 341)

1.6.2. Fikir ve Sanat Eserleri Kanununda Belirtilen Siber Suçlar

FSEK kanun koyucu tarafından fikir ve sanat eserlerinin korunması amacıyla oluşturulmuş bir kanundur. 07.06.1995 tarihinde yapılan değişiklikle bilişim sistemleri ve bilgisayarlarda kullanılan programlar da kanun maddesinde belirtilen eserler kapsamına alınmıştır (Karagülmez, 2009). Kişi veya kurumların emek vererek hazırladığı bilgisayar programlarının maddi ve manevi hak ihlalleri siber suç sayılmış ve FSEK'in 71 ve 72. maddelerinde bu haklar korunmuştur.

1.6.2.1. Maddi ve manevi haklara tecavüz (Madde 71)

“Bu Kanunda koruma altına alınan fikir ve sanat eserleriyle ilgili manevi, mali veya bağlantılı hakları ihlal ederek:

1. Bir eseri, icrayı, fonogramı veya yapımı hak sahibi kişilerin yazılı izni olmaksızın işleyen, temsil eden, çoğaltan, değiştiren, dağıtan, her türlü işaret, ses veya görüntü nakline yarayan araçlarla umuma ileten, yayımlayan ya da hukuka aykırı olarak işlenen veya çoğaltılan eserleri satışa arz eden, satan, kiralamak veya ödünç vermek suretiyle ya da sair şekilde yayan, ticarî amaçla satın alan, ithal veya ihraç eden, kişisel kullanım amacı dışında elinde bulunduran ya da depolayan kişi hakkında bir yıldan beş yıla kadar hapis veya adlî para cezasına hükmolunur.

2. Başkasına ait esere, kendi eseri olarak ad koyan kişi altı aydan iki yıla kadar hapis veya adlî para cezasıyla cezalandırılır. Bu fiilin dağıtmak veya yayımlamak suretiyle işlenmesi hâlinde, hapis cezasının üst sınırı beş yıl olup, adlî para cezasına hükmolunamaz.

3. Bir eserden kaynak göstermeksizin iktibasta bulunan kişi altı aydan iki yıla kadar hapis veya adlî para cezasıyla cezalandırılır.

4. Hak sahibi kişilerin izni olmaksızın, alenileşmemiş bir eserin muhtevası hakkında kamuya açıklamada bulunan kişi, altı aya kadar hapis cezası ile cezalandırılır.

5. Bir eserle ilgili olarak yetersiz, yanlış veya aldatıcı mahiyette kaynak gösteren kişi, altı aya kadar hapis cezası ile cezalandırılır.

6. Bir eseri, icrayı, fonogramı veya yapımı, tanınmış bir başkasının adını kullanarak çoğaltan, dağıtan, yayan veya yayımlayan kişi, üç aydan bir yıla kadar hapis veya adlî para cezasıyla cezalandırılır.

Bu Kanunun ek 4 üncü maddesinin birinci fıkrasında bahsi geçen fiilleri yetkisiz olarak işleyenler ile bu Kanunda tanınmış hakları ihlâl etmeye devam eden bilgi içerik sağlayıcılar hakkında, fiilleri daha ağır cezayı gerektiren bir suç oluşturmadığı takdirde, üç aydan iki yıla kadar hapis cezasına hükmolunur.

Hukuka aykırı olarak üretilmiş, işlenmiş, çoğaltılmış, dağıtılmış veya yayımlanmış bir eseri, icrayı, fonogramı veya yapımı satışa arz eden, satan veya satın alan kişi, kovuşturma evresinden önce bunları kimden temin ettiğini bildirerek yakalanmalarını sağladığı takdirde, hakkında verilecek cezadan indirim yapılabileceği gibi ceza vermekten de vazgeçilebilir.”

Bu kanun maddesi ile kişilerin manevi haklarına yapılan saldırılara karşı önlem alınmaktadır. Ayrıca yukarıda belirtilen eylemler doğrultusunda kişinin maddi yönden zarara uğratılması söz konusu olabilir (Dülger, 2004). Bu kanun maddesi kapsamında kişilerin, eser sahibinin isteği dışında eserlerinin çoğaltması, değiştirmesi veya yayınlaması suç oluşturmaktadır (Karagülmez, 2009). Ayrıca eserlerin çalınıp kendi eserleriymiş gibi göstermeleri de kişiler için suç oluşturmaktadır. Eser sahibi kişilerin ölmesi durumunda 70 yıllık bir süreç vardır. Bu süreçte eserlere karşı yukarıda belirtilen eylemler gerçekleştirilirse mirasçıların şikâyeti söz konusu olabilir (Taşkın, 2008). Bu kanun maddesindeki eylemlerin takibinin yapılıp suç sayılabilmesi için mağduriyet yaşayan eser sahiplerinin veya mirasçılarının şikâyetinin olması gerekir (Nacar, 2010). Bilişim eserlerinin hak ihlali sonucu maddi ve manevi yönden kişilerin zarara uğratılması siber suç oluşturmaktadır.

1.6.2.2. Koruyucu programları etkisiz kılmaya yönelik hazırlık hareketleri (Madde 72)

“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.”

Kişilerin Madde 71’deki eylemleri gerçekleştirebilmesi için eser sahiplerinin koyduğu çeşitli güvenlik duvarlarını yıkmaları gerekir. Çeşitli ilave programlarla oluşturulan bu güvenlik duvarlarını yıkmak için program ve donanım üreten kişiler siber

suç işlemiş olurlar (Karagülmez, 2009). Bu kanun maddesi ile eser sahibi kişilerin eserleri için oluşturdukları koruyucu programlar koruma altına alınmıştır (Taşkın, 2008).

1.6.3. Elektronik İmza Kanununda Belirtilen Siber Suçlar

EİK, elektronik imza ve elektronik sertifikaların Avrupa Birliği standartları doğrultusunda güvenliklerinin, yetki ve sorumluluklarının belirlenebilmesi amacıyla oluşturulmuştur (Ergün, 2008). Avrupa Birliği'nin e-ticaret ve e-imza uygulamalarının yaygınlaştırılması ve güvenilirliklerinin sağlanması üzerinde durması, üye ülkelerin ve üyelik için aday olan ülkelerin bu konuyla daha fazla ilgilenmelerine sebep olmuştur (Sağlam, 2007). Ülkemizin de Avrupa Birliğine üyelik çalışmaları süresince gerçekleştirdiği uyum süreci doğrultusunda 15.01.2004 tarihinde TBMM tarafından Elektronik İmza Kanunu kabul edilmiştir. EİK'nun 16 ve 17. maddesi, e-imza ve e-sertifikaların oluşturulmasında hileli davranışların ortaya çıkmasına karşı alınmış tedbirlerdir. Bu hileli davranışlar, siber suç oluşturmaktadır. Bu kanun maddelerinde geçen terimlerin kanunda belirtilen tanımlarını verecek olursak;

Elektronik İmza: “Başka bir elektronik veriye eklenen veya elektronik veriyle mantıksal bağlantısı bulunan ve kimlik doğrulama amacıyla kullanılan elektronik veridir.”

Elektronik Sertifika: “İmza sahibinin imza doğrulama verisini ve kimlik bilgilerini birbirine bağlayan elektronik kayıdır.”

İmza Oluşturma Verisi: “İmza sahibine ait olan, imza sahibi tarafından elektronik imza oluşturma amacıyla kullanılan ve bir eşi daha olmayan şifreler, kriptografik gizli anahtarlar gibi verilerdir.”

İmza Oluşturma Aracı: “Elektronik imza oluşturmak üzere, imza oluşturma verisini kullanan yazılım veya donanım aracıdır.”

1.6.3.1. İmza oluşturma verilerinin izinsiz kullanımı (Madde 16)

“(1) 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 elli günden az olmamak üzere adli para cezasıyla cezalandırılırlar.

(2) Yukarıdaki fıkra da belirtilen suçlar elektronik sertifika hizmet sağlayıcısı çalışanları tarafından işlenirse bu cezalar yarısına kadar artırılır.”

Elektronik imza ile hazırlanmış belgeler ıslak imzalıymış gibi kabul edilir ve sorumluluk imza sahibine aittir (Orta, 2005). Yukarıdaki kanun maddesinde belirtilen hileli eylemler elektronik imza konusunda çeşitli mağduriyetler oluşturabilmektedir (Akarslan, 2012). Yapılan bu hileli eylemlerin tespiti ancak teknik incelemeler sonunda ortaya çıkarılabilmektedir (Acar, 2013). Genel olarak elektronik imza oluşturmak için gerekli aletlerin ve elektronik imzanın hukuk dışı kullanılması tüm kamuda güveni sarsabilmektedir (Dülger, 2004). Ayrıca elektronik imza ile hazırlanan belgeler konusunda kişiler belgede sahtecilik fiilini gerçekleştirebilmektedirler (Artuk, Gökçen ve Yenidünya, 2012).

1.6.3.2. Elektronik sertifikalarda sahtekârlık (Madde 17)

“(1) Tamamen veya kısmen sahte elektronik sertifika oluşturanlar veya geçerli olarak oluşturulan elektronik sertifikaları taklit veya tahrif edenler ile bu elektronik sertifikaları bilerek kullananlar, iki yıldan beş yıla kadar hapis ve yüz günden az olmamak üzere adli para cezasıyla cezalandırılır.

(2) Yukarıdaki fıkra da belirtilen suçlar elektronik sertifika hizmet sağlayıcısı çalışanları tarafından işlenirse bu cezalar yarısına kadar artırılır.”

16. maddede elektronik imza ile ilgili belirtilen siber suç olgusu bu maddede elektronik sertifikalar çerçevesinde belirtilmiştir. Özellikle bilişim sistemleri aracılığıyla kullanılan elektronik sertifikaların üzerinde yapılan hileli hareketler siber suç oluşmasında etkili olan eylemlerdir (Akarslan, 2012).

1.7. Dünyada Siber Suçlar

Narkotik ve Asayiş suçları gibi artık siber suçlar da ulus ötesi bir hal almıştır (Hunton, 2011). Özellikle 1990’larda iyice yaygınlaşan ve dünyayı kasıp kavuran İnternet furyası uluslar arası platformda devletler için güvenlik zafiyeti yaratmaya

başlamıştır (Özcan, 2004). İnternetin keşfedilmesi ve gelişmesi konusunda büyük bir rol alan ABD siber endişeyi de en fazla hisseden ülkelerin başında gelmektedir (Griffin, 2012). Devletlerin resmi sitelerine hacker gruplar tarafından yapılan saldırılar ve akabinde elde edilmek istenen devlet sırları, bu konunun ne kadar önemli olduğunu göstermektedir. Ülkelerin varlığını tehdit eden terör örgütlerinin başka ülkelerdeki İnternet siteleri tarafından yönetildiği, gerekli talimatların İnternet aracılığıyla verildiği düşünülürse bu suçun sadece ülke sınırları içerisinde değil evrensel sınırlar içerisinde düşünülmesi gerçeği önümüze çıkmaktadır. Siber suç zanlıları, teknolojinin karmaşıklığının yanı sıra ülkeler arasındaki hukuksal farklılıklardan da yararlanmışlardır (Ghernaouti, 2013). Bu açıklardan yararlanan zanlılar büyük kayıplı siber saldırıların sonunda rahatlıkla izlerini kaybettirebilmişlerdir (Clough, 2011). Saldırıları birçok ülkeyi rahatsız etmiş ve bu rahatsızlıktan dolayı birçok ülke Avrupa Sanal Suçlarla Mücadele sözleşmesini imzalamıştır. Böylelikle yasal boşluklardan yararlanıp rahat hareket eden siber suç zanlıları eskisi gibi rahat hareket etme ortamı bulamamışlardır.

Siber suçlar konusunda kimi ülkeler yeni kanun maddeleri çıkararak, kimi ülkeler ise mevcut kanun maddeleri üzerinde düzenleme yaparak önlem almaya çalışmışlardır. Karşılaştırmalı hukukta dünya ülkelerinin siber suçlara karşı kanun düzenlemelerine bakıldığında; Anglosakson Hukuk Sistemini uygulayan İngiltere, İrlanda ve ABD gibi ülkeler siber suçlarla mücadele için; kendi ceza kanunlarından bağımsız bir şekilde siber suçlarla ilgili olarak özel düzenlemelere başvurmuşlardır. Kıta Avrupası Hukuk Sistemi'ni uygulayan Fransa, Almanya, İtalya, Kanada, Lüksemburg gibi ülkeler ise siber suçlarla mücadele için; genel olarak kendi mevcut ceza kanunlarında yaptıkları değişiklikler sonucu ortaya çıkan ceza maddeleri ile siber suç kavramlarını ilişkilendirmiş ve bu alanda düzenlemeler yapmışlardır (Yazıcıoğlu, 1997). Siber suçların mukayeseli hukukta kapsam içerisine nasıl sokulduğunu ve hangi konuların bu kapsam çerçevesinde düşünüldüğünü görebilmek için çeşitli Avrupa Birliği ülkeleri ve teknoloji alanında hızlı ilerleyen dünya ülkelerinin siber suçlara yaklaşımı incelenmiştir.

Amerika Birleşik Devletleri bilgisayar teknolojisinin ilk girdiği ülkelerin başında gelmektedir. Dolayısıyla bu teknoloji ile beraber gelen siber suçlar da ilk olarak A.B.D.'de ortaya çıkmıştır (Kurt, 2005). A.B.D. yaygın olan siber suçlara çeşitli kanun

maddeleri ile önlemler almaya çalışmıştır. Hala yürürlükte olan bu kanun maddeleri şunlardır (Çeken, 2002):

- Bilgisayar Sahtekârlığı ve Bilgisayarların Kötüye Kullanılması Yasası
- Çocuk Pornografisinin Önlenmesi Yasası
- Çocukların Online Yayınlardan Korunması Yasası
- İnternet’te Kumarın Önlenmesi Yasası
- Elektronik Haberleşmenin Gizliliği Yasası
- İletişim Ahlak Yasası
- Antiterör Yasası
- Kimlik Hırsızlığı Yasası

Almanya’da siber suçların önlenmesi amacıyla Kıta Avrupası Hukuk Sistemi dahilinde çeşitli düzenlemeler yapılmıştır (Kurt, 2005). Bu düzenlemeler kapsamında;

- Bilgisayar sistemlerine izinsiz şekilde girilerek verilerin ele geçirilmesi
- Bilgisayar sistemleri aracılığıyla yapılan sahtekârlık ve dolandırıcılıklar

(Değirmenci, 2002)

- Verilerin silinip yok edilmesi, değiştirilmesi ve bilgisayarların sabotajı ile veri aktarım sürecinin engellenmesi

konularında çeşitli düzenlemeler yapılarak Teleservisler kanunu ve Telekomünikasyon kanunlarında çeşitli değişiklikler yapılmıştır (Karagülmez, 2009).

İsviçre’de siber suçlar, Federal Ceza Yasası ve Haksız Rekabet yasaları ile önlenmek istenmektedir. Federal Ceza Kanunlarında yapılan değişikliklerle bilişim sistemlerine girilerek verilerin değiştirilmesi, çalınması, yok edilmesi ve dolandırıcılıkların yapılması gibi siber suçlar kapsam içerisine sokulmuştur. Haksız rekabet yasaları ise ticari açıdan ihlallerin yapılması ile ortaya çıkan siber suçları içeren bir düzenleme ile yürürlüğe konulmuştur (Ergün 2008).

Fransa’da da ülkemizde olduğu gibi yeni oluşturulan ceza kanunu ile siber suçlar kapsam içerisine alınmıştır. Yeni ceza kanunu ile birlikte;

- Sisteme yetkisiz erişim ile verilen tahrip edilmesi, silinmesi, çalınması (Pallı, 2008)
- Banka ve kredi kartlarının kötüye kullanılması (Karagülmez, 2009)

- Çocuklar kullanılarak veya çocukların görmesine imkan verecek şekilde cinsel içerikli yayınların veya mesajların yayınlanması (Ünver, 2001)
- Görüntü ve ses kayıtlarında montaj yapılarak bu kayıtların kişinin rızası olmadan yayınlanması (Kangal, 2001)
- Bilişim sistemlerinin kullanılarak dolandırıcılık, hırsızlık gibi suçların işlenmesi ve bu suçların örgütlü bir şekilde işlenmesi (Dülger, 2004)

durumları yeni ceza kanunu ile siber suç kavramı içerisinde değerlendirilmeye başlamıştır.

Anglo Sakson hukuk sistemine göre hukuk sistemini düzenleyen İngiltere’de siber suçlar özel kanunlarla düzenlenmiştir. Computer Misuse Act kanunu ile yetkisiz erişim, verilerin yok edilmesi veya değiştirilmesi gibi fiiller önlenmeye çalışılmıştır (Akıncı vd, 2004). Yine bunun yanında müstehcen yayınlar ve pornografinin önüne geçilebilmesi için Müstehcen Yayınlar Kanunu ve Telekomünikasyon Kanunlarında çeşitli düzenlemeler yapılmıştır (Dülger, 2004). Çocukların Korunması Kanununda da buna paralel olarak çeşitli değişiklikler yapılmıştır (Mahmutoğlu, 2001).

İtalya, ceza kanun maddelerinde yaptığı çeşitli düzenlemeler ve eklerle siber suçlar konusunda adımlar atmıştır. Diğer ülkelerde olduğu gibi İtalya’da da bilişim sistemlerine yetkisiz erişim, siber suçların en önemli konusu olmuştur. Bilişim sistemine girip verileri silmek, değiştirmek ve verilere ulaşımın engellenmesi bu kapsamda önlenmek istenen suçlardır (Ünver, 2001). Çocukların pornografik içerikli görüntü ve videolarla istismar edilmesi en çok üzerinde durulan siber suçtur (Sınar, 2001). Bunların yanı sıra ;

- İletişimin engellenmesi veya yetkisiz bir şekilde dinlenmesi
 - Bilişim sistemleri aracılığıyla hırsızlık, dolandırıcılık ve kumar oynanmasına imkân sağlama
 - Virüs bulaştırmak yoluyla sistemlere erişimin engellenmesi
 - Devlet sırlarının bilişim sistemleri kullanılarak açıklanması
- gibi durumlar siber suç kapsamında değerlendirilmiştir.

Japonya da teknolojik gelişmelerin hızlı yol aldığı ülkelerden birisidir. Bu hızlı değişimle beraber gelen siber suç kavramı için Japon yasa koyucular çeşitli

düzenlemeler yapmışlardır. Ceza hukuku alanında yapılan düzenlemelerle normal suçlarla mücadele edilmesi için oluşturulan yasalarla siber suçları da kapsayacak şekilde değiştirilmiştir. Bunun yanı sıra “İnternete Haksız Girmenin Yasaklanması Hakkındaki Kanun” yürürlüğe sokulmuştur. Fakat Japonya da farklı olarak; sistemdeki veriler tahrip edilip satılmadığı takdirde sisteme izinsiz girmek suç sayılmamaktadır (Ünver, 2001).

Rusya’da siber suçlarla mücadele konusunda; G-8 ülkelerinin içişleri bakanlarının katıldığı toplantıda Ulusal Temas Noktaları oluşturulmasına karar verilmiş böylece siber suçlar konusunda diğer ülkelerle adli ve yargı bağlantı kurulmuştur (Ünver, 2001). Rusya ceza kanununa göre bilişim sistemlerinin kullanılarak iletişim özgürlüğünün kısıtlanması veya engellenmesi en önemli siber suçlardan biri olarak görülmektedir. Bunun yanı sıra;

- Pornografik içerikli yayınların bilişim sistemleri aracılığıyla hukuk dışı çoğaltılması ve yayınlanması (bu konuda Rus kanun koyucular çocuk veya yetişkin ayrımı yapmamıştır)

- Verilerin elde edilmesi veya kullanılması için sistemlere hukuk dışı erişim
- İnsan ve çocuk ticaretinin yapılması

konularında yapılan fiiller siber suç kapsamına sokulmuştur.

İsrail, siber suçlarla mücadele için “Bilgisayar Kanunu” adında yeni kanun maddeleri yürürlüğe sokmuştur. Bu kanun maddelerinin yanı sıra siber suçlarla mücadele anlamında birçok ülke ile ortak çalışma yoluna gidilmiştir (Akarslan, 2012).

Kanada devleti mevcut yasalarda yapılan değişikliklerle siber suçların kapsam içerisine alınmasını sağlamış ve bu şekilde siber suçlara karşı önlem almaya çalışmıştır (Akıncı vd, 2004). Çeşitli elektronik aletlerle sistemin kesintiye uğratılması veya sisteme girişin tamamen engellenmesi, Kanada’da yasa koyucular tarafından önemsenen en önemli konulardan bir tanesidir (Kurt, 2005).

Malezya teknolojik gelişmelerin yoğun yaşandığı ülkelerden birisidir. Bu yüzden çeşitli yasalarla bu teknolojik gelişmelerin olumsuz sonuçlarından korunmaya çalışmaktadır (Kurt, 2005). Bu yasalardan bazıları şöyledir:

- Dijital İmza Yasası
- Mültimedya Yakınsama Yasası

- Bilgisayar Suçları Yasası
- Ayrıca bu yasalarla beraber gündeme gelen çeşitli siber suç konuları şunlardır;
 - Telif, marka ve ticari sırların korunması
 - İnternette yapılan hırsızlık, dolandırıcılık, tehdit, şantaj, taciz, korku yayma fiilleri
 - Sisteme ve bilgisayarlara izinsiz giriş yapma veya sisteme giriş şifrelerini elde etme
 - Singapur da diğer ülkeler gibi siber suçların yaygınlaştığını görüp buna tedbir almak amacıyla çeşitli yasa maddeleri çıkarmıştır (Kurt, 2005). Bunlar;
 - Bilgisayarların kötüye kullanılması ile ilgili yasa ve
 - Elektronik işlemlerle ilgili olan yasadır.
 - Bu yasaların içeriği aşağıda belirtilen siber suç çeşitlerini kapsamaktadır.
 - Verileri çeşitli eylemlere maruz bırakmak amacıyla yetkisiz erişim
 - Sistemin bir bölümünün veya tamamının kullanılamaz hale getirilmesi veya erişimin engellenmesi
 - Sisteme giriş için gerekli olan kullanıcı adı veya şifrelerin ele geçirilmesi ve ifşa edilmesi

1.8. Siber Suç Farkındalığı

Diğer birçok ülke gibi bizim ülkemizde 1990'lı yıllardan sonra hızla esen İnternet rüzgârından etkilenmeye başlamıştır. Ülkemizde İnternet kullanımı özellikle 2000-2010 yılları arasında aşırı bir ilerleme kat ederek %1650 oranında artmıştır (Dijle ve Doğan, 2011). Buna bağlı olarak siber suç oranları ve nitelikleri de yükselen bir ivmeyle artış göstermiştir. Emniyet Genel Müdürlüğü Kaçakçılık ve Organize Suçlarla Mücadele Daire Başkanlığının yayınladığı raporlara göre 2000, 2001 ve 2002 yıllarında kayıtlara geçen siber suç sayısı oldukça azdır. Ama 2003 yılı sonrası siber suçlar her yıl bir önceki yılın iki katından daha fazla artış göstermiştir (Dicle ve Doğan, 2011). Bu artış, İnternetin yaygınlaştıkça bilinçsiz ve amacı dışında kullanıldığını göstermektedir. Kötü niyetli insanlar İnternetin sağladığı kolaylıkları kendilerinin illegal işlerinde kullanmaktadırlar. Yapılan siber suç çeşitlerine bakıldığında zanlıların hedeflerine

ulaşmak için İnternetin sunduğu her türlü imkânı kullandıkları görülmektedir. Özellikle “Banka ve Kredi Kartı Dolandırıcılığı”, “Bilişim Sistemlerine Girme, Sistemi Engelleme, Sistemi Bozma, Verileri yok etme, Verileri Değiştirme”, “İnternet Aracılığıyla Yapılan Dolandırıcılık” suçları ön plana çıkmaktadır. 2009 yılında İnternet ve bilgisayar aracılığıyla yapılan 1511 tane “Banka ve Kredi Kartı Dolandırıcılığı” olayında 2176 tane şüpheli, 353 tane “Bilişim Sistemlerine Karşı İşlenen Suç” olayında 534 tane şüpheli ve 412 tane “İnternet Aracılığıyla Nitelikli Dolandırıcılık” olayında 731 tane şüpheli yakalanmıştır (Şen, 2011). Ayrıca 2010 yılında da 1132 tane “Banka ve Kredi Kartı Dolandırıcılığı” olayında 1005 tane şüpheli, 975 tane “Bilişim Sistemlerine Karşı İşlenen Suç” olayında 1351 tane şüpheli ve 71 tane “İnternet Aracılığıyla Nitelikli Dolandırıcılık” olayında 115 tane şüpheli yakalanmıştır (Şen, 2011).

Siber suç zanlıları normal zanlılardan daha kolay bir şekilde izini kaybettirebilirler. Gerek jandarma gerekse polis teşkilatımızın, bilişim suçu zanlılarıyla baş edebilmeleri için en az onlar kadar bilişim altyapılarının olması gereklidir (Dülger, 2004). Siber suçların gün geçtikçe hızla artmasına karşın güvenlik birimlerinde bilişim üzerine kendini yetiştirmiş eleman sayısı sınırlıdır (Şeker, 2003). Dolayısıyla siber suç konuları kapsamında yürütülen kovuşturma sayısı siber suç sayısına nispeten çok azdır (Wall, 2008). Bu yüzden bilişim suçu zanlıları için; güvenlik görevlilerinin, suç işlendikten sonra değil de suç işlenmeden önce önlem almaları çok önemlidir (Grabosky ve Smith, 2001). Bu noktada siber suç farkındalığı ortaya çıkmaktadır. Siber suç farkındalığı, insanların siber suç hakkında bilinçlilik düzeyleridir. Şüpheliler yaptıkları işin sanal ortamda olması nedeniyle sonuçlarını tahmin edememektedirler. En basitinden örnek verecek olursak; sosyal paylaşım ortamlarında duyarsızca paylaşılan mesajların belki milyonlar tarafından okunacağı ve ne şekilde anlaşılabileceği paylaşan kişi tarafından tahmin edilememektedir. Bunun gibi sanal ortamdaki birçok işlemin nelere mal olacağı, yapılan eylemin muhataplarına karşı maddi-manevi zararı, kişiler tarafından düşünülmemektedir. İnsanlar sanal ortamdaki sorumluluklarının farkına varmakta sıkıntı yaşamaktadırlar. Kişilerin siber suçlara karşı farkındalığını ölçmek için Dijle ve Doğan (2011), üniversite öğrencileri ve öğretim görevlileri üzerinde bir araştırma yapmıştır. Yapılan bu araştırmada katılımcıların % 35,6’sının bilişim (siber) suç kavramını daha önce duymadıkları tespit edilmiştir. Yine aynı araştırmada

katılımcıların % 29,6'sının İnternette film ve müzik gibi dosyaları indirmenin suç olduğunu bilmediğini, ayrıca katılımcıların % 42,2'sinin yeterli bilgi ve birikime sahip olmaları halinde hackerlık (bilgisayar korsanlığı) yapabilecekleri sonucu elde edilmiştir. Bilişim suçları genelde 16 – 35 yaşları arası gençler tarafından işlenmektedir. Kendini bazı kesimlere karşı ispat etmek isteyen ve yaptığı işin yasal olup olmadığını bilmeyen gençler bu işe daha çok meyillidir (Demirbaş, 2005). Martin ve Rice (2011), tarafından yapılan bir araştırmaya göre özellikle genç ve okul çağındaki kişiler tarafından kabadayılık için bilgisayarın kötü amaçlarla kullanılması toplumda derin endişelere neden olmaktadır. Bilek (2012), Türkiye'nin değişik üniversitelerinde bulunan BÖTE bölümü öğrencilerinin bilişim teknolojilerini kullanma durumları ve bilişim suçları konusunda ki bilgi düzeyleri ile tutumlarını ölçmek için bir araştırma yapmıştır. Yapılan araştırmaya katılanların % 25'i yakalanmayacağını düşündüğü için bilgisi olsa hackerlık yapabileceğini söylemiştir. Yine aynı araştırmada öğrencilerin % 34'ü bilgisayarlarında lisanssız işletim sistemi kullandığını belirtmişlerdir. Ayrıca yapılan bu araştırmanın en göze çarpan tarafı üniversite öğrencilerinin % 95 gibi büyük bir oranının bilişim suçları ile ilgili bilgilendirilmek istemeleridir. İlbaş (2009), Başkent Üniversitesi öğrencileri ve akademik çalışanları üzerinde bilişim suçlarının sosyo-kültürel seviyelere göre algı analizini ölçmek için bir araştırma yapmıştır. Yapılan bu araştırmada; katılımcılara göre sırasıyla “çocuk pornografisi” ve “bilgisayar aracılığıyla banka hesaplarına ulaşıp yapılan hırsızlık” en ağır bilişim suçları olarak gösterilmiştir. Aynı araştırmada öğretim elemanı, öğrenci gruplarında ki en belirgin algı farklılığı plagiarizm olarak da bilinen akademik aşırı macılık fiilinde tespit edilmiştir. Akademik aşırı macılık öğretim elemanları için ağır bir bilişim suçu olarak kabul edilmesine rağmen aynı suçun öğrenciler için o kadarda önemsenmeyen bir bilişim suçu olmadığı anlaşılmıştır. Türkoğlu, Özdemir, Kalkan, Varol ve Tokdemir (2013), Elazığ'da Fırat Üniversitesi T.E.F. Bilgisayar bölümü ile T.F. Yazılım Mühendisliği bölümünde ve lise öğrencileri üzerinde bir araştırma yapmıştır. Yapılan bu araştırmada lise öğrencilerinin % 21'i, üniversite öğrencilerinin % 11'i bilişim suçları ile ilgili herhangi bir bilgiye sahip olmadıklarını belirtmişlerdir. Yine aynı araştırmada lise öğrencilerinin %57'si, üniversite öğrencilerinin % 77'si medya aracılığıyla bilişim suçları hakkında birtakım bilgiler edindiğini söylemiş; lise öğrencilerinin % 40'ı, üniversite öğrencilerinin % 36'sı öğretmenleri aracılığıyla bilişim suçları hakkında birtakım bilgiler öğrenmiş; lise

öğrencilerinin % 30'u, üniversite öğrencilerinin % 22'si güvenlik güçleri aracılığıyla bilişim suçları hakkında bazı bilgiler öğrendiklerini belirtmişlerdir.

1.9. Problem Durumu

Bu araştırmada mesleki ve teknik liselerdeki bilişim bölümü öğrencilerinin siber suçlara karşı farkındalık durumları incelenmiştir.

Problem Cümlesi: Mesleki ve teknik liselerdeki bilişim bölümü öğrencilerinin siber suçlara karşı farkındalık düzeyleri nedir?

1.10. Alt Problemler

- Mesleki ve teknik liselerdeki bilişim bölümü öğrencilerinin demografik özelliklerine göre siber suçları algılama düzeyleri nedir?
- Cinsiyet değişkeni ile İnternetin kişisel değerlere karşı sakıncalarını algılama, kişi ve örgütlerin İnterneti kötü niyetle kullanabileceklerini algılama, İnternetteki rahatlık seviyesi ve İnternette alınan önlem seviyesi arasında anlamlı fark var mıdır?
- Sınıf değişkeni ile İnternetin kişisel değerlere karşı sakıncalarını algılama, kişi ve örgütlerin İnterneti kötü niyetle kullanabileceklerini algılama, İnternetteki rahatlık seviyesi ve İnternette alınan önlem seviyesi arasında anlamlı fark var mıdır?
- İnterneti kullanma yılı ile İnternetin kişisel değerlere karşı sakıncalarını algılama, kişi ve örgütlerin İnterneti kötü niyetle kullanabileceklerini algılama, İnternetteki rahatlık seviyesi ve İnternette alınan önlem seviyesi arasında anlamlı fark var mıdır?
- Siber saldırıya uğrama durumu ile İnternetin kişisel değerlere karşı sakıncalarını algılama, kişi ve örgütlerin İnterneti kötü niyetle kullanabileceklerini algılama, İnternetteki rahatlık seviyesi ve İnternette alınan önlem seviyesi arasında anlamlı fark var mıdır?

1.11. Araştırmanın Amacı

Siber suçun gençler arasında yaygınlaşması siber suç vakalarında hızla artışa neden olmaktadır. Kendilerini kanıtlama peşinde olan gençler, ABD Savunma Bakanlığı Pentagon'a siber saldırı düzenleyecek kadar cesaret sahibidirler (Özcan, 2004). Aradıkları özgür ortamı İnternette bulan ortaöğretim seviyesindeki gençler siber ortamda istedikleri her şeyi yapabileceklerini zannetmektedirler (Turhan, 2006). Hukuk kurallarını tam olarak idrak edemeyen gençler siber ortamda yaptıkları eylemlerin hukuksal boyutunu ve sonuçlarını algılamakta sıkıntı çekebilmektedirler. Bu araştırmanın amacı Mesleki ve Teknik Liselerdeki Bilişim Bölümü öğrencilerinin siber suç farkındalık düzeylerinin belirlenerek demografik özelliklere göre anlamlı farklılıkların ortaya çıkarılmasıdır.

1.12. Araştırmanın Önemi

Ülkemizde ve dünyada siber suç olayları hızla artmaktadır. Ülkeler, ulusal ve uluslararası ortamda siber suçlara karşı birçok önlem almaktadırlar (Peker, 2010). Teknolojinin baş döndürücü bir şekilde değiştiği düşünülürse ülkelerin de siber suçlara karşı mücadele için sürekli kendilerini yenilemeleri gerekmektedir (Özcan, 2004). Fakat yasal önlemlerin siber suçları önleme konusunda tek başına yeterli etkiye sahip olmadıkları görülmektedir (Dülger, 2012). Siber suç vakalarının hızlı ilerleyişinin önüne geçebilmek için; siber suçlarla en çok anılan kesim olan gençlerin siber suçla ilişkileri incelenmelidir (Bayram ve Sayılı, 2013). Aileler, çocuklarının belli bir yaştan sonra bilgiye hızlı ve etkin bir şekilde ulaşmaları için siber imkânlardan faydalanmalarını istemektedirler (Canberk ve Sağıroğlu, 2007). Ama siber ortamın sağladığı denetimsizlik hali, gençlerin sonuçlarını düşünmeden rahat hareket etmelerine sebep olmaktadır. Özellikle bilgisayar ile daha fazla içli dışlı olan gençler siber ortama rahatça uyum sağlarlar. Bu rahatlık, siber ortamın denetimsizliğiyle birleşince gençlerin siber suçla tanışması kaçınılmaz olmaktadır. Yapılan bu çalışmada derslerinin çoğunu bilgisayar ortamında işleyen mesleki ve teknik liselerin bilişim bölümü öğrencilerinin siber suçlarla ilgili farkındalık durumlarının belirlenmesi amaçlanmıştır. Bu farkındalığın durumunun belirlenmesi alınacak önlemler açısından önemlidir. Çalışmada problem ve alt problemlere alınacak cevaplarla siber suçların en çok

muhatapı olan gençlerin siber suçların ne kadar farkında oldukları anlaşılabilecektir. Böylelikle siber suçlara karşı alınacak önlemlerin belirlenmesinde sorunun kökenine inilerek daha objektif tedbirler alınabilecektir.

Siber suçların, teknolojik gelişmelerle çeşitlilik kazandığı düşünülürse yapılan bu araştırmanın güncelliği günümüz şartlarındaki siber suçları gün yüzüne çıkararak bireysel ve devlet nezdinde alınacak tedbirler için fikir vermektedir.

Siber suçların diğer suç tiplerine göre yeni olması ve kendini sürekli yenilemesi yasal boşlukların ortaya çıkmasına neden olabilmektedir. Bu yasal boşluklar kanun koyucu tarafından doldurularak maddi ve manevi kayıplar önlenmek istenmektedir. Dolayısıyla konu hakkında çıkarılan yasa ve yasa değişikliklerinin ayrıntılı bir şekilde derlenmesi gelecekteki çalışmalar için yararlı olacaktır.

1.13. Sınırlılıklar

Araştırma 2013-2014 eğitim-öğretim yılı Erzurum ili merkez ilçelerinde bulunan Mesleki ve Teknik Liselerin bilişim sınıfı öğrencileri ile sınırlıdır.

Araştırma, veri toplama aracı olarak kullanılan “Ortaöğretim Kurumlarında Siber Suç Farkındalık Anketi” isimli anket formunun genel sınırlılıkları ile sınırlıdır.

1.14. Varsayımlar

Araştırma dâhilinde anket yapılan öğrenciler, anket sorularını okuyarak ve anlayarak cevaplamışlardır.

Bilişim bölümü öğrencilerinin siber suçlar konusunda belirli bir farkındalık düzeyine sahip oldukları kabul edilmektedir.

Bilişim bölümü öğrencilerinin derslerinin çoğunu bilgisayar ortamında işledikleri kabul edilmektedir.

1.15. Tanımlar

Siber Suç: Bilgisayar ve bilgisayar ağıları aracılığıyla siber uzayda yapılan hukuk dışı eylemler siber suçun tanımını oluşturmaktadır (Yazıcıoğlu, 1997).

Siber Suç Farkındalığı: İnsanların siber suç hakkında bilinçlilik düzeyidir.

Siber Ortam: Bilişim sistemleri ve bu sistemlere bağlı bilgisayarların oluşturduğu ağlar üzerine kurulmuş, sınırsız, denetimi zor olan sanal bir ortamdır (Özpehlivan, 2006).

Bilişim Bölümü: Mesleki ve Teknik Liselerin bilgisayar teknolojileri, bilgisayar yazılım-donanım bilgileri ve bilgisayar ağları üzerine yoğunlaşmış bölümüdür.

İKİNCİ BÖLÜM

2. YÖNTEM

Bu bölümde araştırmamızda kullanılan model, araştırmamızın evren ve örnekleme, verileri toplama araçları ve verilerin toplanmasına yer verilmiştir.

2.1. Araştırma Modeli

Araştırma modeli, araştırmanın asıl amacı doğrultusunda belirlenen bir yol haritasıdır (Yıldırım ve Şimşek, 2005). Çeşitli yaklaşımlar ile araştırmacı için bir plan ortaya konulmaktadır. Bu araştırmada bizim kullandığımız araştırma modeli betimsel tarama modelidir.

Tarama modellerinde var olan bir durumu değiştirmeden betimlemek asıl amaçtır (Karasar, 2011). Tarama araştırmalarında; literatür taraması sonucu elde edilecek bilgiler araştırmacının gözlemleri ile harmanlanmaktadır.

2.2. Evren ve Örneklem

Mesleki ve teknik liselerdeki bilişim bölümü öğrencileri, derslerinin çoğunu bilgisayar laboratuvarlarında işlediklerinden dolayı diğer öğrencilere göre daha fazla bilgisayar ve İnternet kullanıcısı olmaktadır. Dolayısıyla yapılan bu araştırmada; bilgisayarla iç içe olan bilişim bölümü öğrencilerinin siber suç farkındalığı araştırılmıştır. Bu araştırmamızda araştırmamızın evrenini Erzurum İlindeki mesleki ve teknik liselerin bilişim bölümü öğrencileri oluşturmaktadır. Örneklem ise; araştırma yaptığımız evreni temsil edebilmesi için kolay örnekleme yöntemi ile seçilen mesleki ve teknik liselerde okuyan bilişim bölümü öğrencilerden oluşmaktadır. Merkez Yakutiye ilçesine bağlı Atatürk Mesleki ve Teknik Anadolu Lisesi, Hamidiye Mesleki ve Teknik Anadolu Lisesi ve merkez Palandöken ilçesine bağlı Kazım Karabekir Mesleki ve Teknik Anadolu Lisesinde 2013-2014 eğitim-öğretim yılında okuyan bilişim bölümü öğrencileri örneklemimizi oluşturmaktadır.

2.3. Veri Toplama Araçları

Çalışmada veriler, yerli ve yabancı kaynaklardan yararlanılarak oluşturulan “Ortaöğretim Kurumlarında Siber Suç Farkındalık Anketi” ile toplanmıştır. Ayrıca söz konusu anket maddelerinin oluşturulması esnasında uzman görüşlerine başvurulmuştur. Hazırlanan anket taslağı yukarıdaki okullardan seçilen üç sınıfta uygulandıktan sonra güvenilirlik geçerlilik testi yapılmıştır. Anketin iç tutarlılık katsayısı Cronbach-Alpha yöntemiyle hesaplanmış $\alpha=0.776$ bulunmuştur. Ölçeğimizin güvenilir olduğu anlaşılmıştır (Kalaycı, 2010). Güvenilirlik-geçerlilik testinden geçen anket formu ile veriler toplanmıştır. Anketimizde demografik soruların yanı sıra likert ölçekli sorular sorularak öğrencilerin görüşlerine ulaşmak amaçlanmıştır. Oluşturulan ankette beşli dereceleme ölçeği kullanılmıştır. Anketi cevaplayanlar görüş ve değerlendirmelerini “Kesinlikle Katılıyorum”, “Katılıyorum”, “Kararsızım”, “Katılmıyorum”, “Hiç Katılmıyorum” ölçütlerinden birini seçerek belirtmeleri istenmiştir. Likert tipi ölçme yönteminde seçenekler 1, 2, 3, 4, 5 biçiminde derecelendirilmiştir. Anket sorularını hazırlarken örneklem grubunu etik açıdan şüpheye düşürecek herhangi bir soru yöneltilmemeye çalışılmıştır.

Söz konusu anketimizdeki likert ölçekli sorular arasındaki ilişkilerden yararlanarak farklı olguları ortaya çıkarıp ve bu olguların verilerini elde edilmek amacıyla faktör analizi yapılmıştır. Faktör analizi, var olan çok sayıdaki değişkenleri ortak özelliklerine göre toplayarak, daha anlamlı ve sayıca daha az olan yeni değişkenlerin ortaya çıkması ya da faktörler ile vizyonları arasındaki ilişkileri sunan çok değişkenli bir istatistiktir (Büyüköztürk, Çakmak, Akgün, Karadeniz ve Demirel, 2012). Açımlayıcı ve doğrulayıcı olarak ikiye ayrılan faktör analizlerinden Açımlayıcı Faktör Analizi, belli faktörler altında toplanan verilerin kuramsal yapının birebir göstergeleri olup olmadığını ortaya çıkarmayı sağlar (Çokluk, Şekercioğlu ve Büyüköztürk, 2010). Faktör analizinin yapılış amaçları verilerin indirgenerek değişkenlerin sayısını azaltabilmek ve bu değişkenlerin arasında bulunan ilişkilerden faydalanarak yeni boyutlar ortaya çıkarabilmektir (Özdamar, 2010). Veri grubumuzun faktör analizi yapmaya uygunluğunun anlaşılabilmesi için Barlett Küresellik ve Kaiser-Meyer-Olkin (KMO) testleri uygulanmıştır. KMO, veri yapısının örneklem ile uygunluğunu, Barlett

Küresellik testi ise verilerin çok değişkenli (birbirleriyle ilişkili) bir yapıya sahip olup olmadığının bir göstergesidir (Çokluk vd, 2010).

Uygulanan faktör analizinde döndürme metodu (rotasyon) olarak varimax tekniği kullanılmıştır. Varimax tekniğinde yapının basite indirgenebilmesi için faktör yükleri matrisinin sütunları önemsenir, bütün sütunlarda bazı yük değerleri 1'e giderken, geriye kalan değerler 0'a gider (Büyüköztürk vd, 2012). Temel bileşenler yöntemi ve Varimax dönüştürme yöntemi kullanıldığından dolayı özdeğeri 1'in üzerinde olan, binişiklik sorunu göstermeyen, binişiklik durumunda ise iki faktör arasındaki korelasyon farkının en az .100 düzeyinde olması şartını sağlayan maddeler (Çokluk vd, 2010) ve faktör yük kabul düzeyi 0,32'nin altında olmayan maddelerden meydana gelen faktör yapıları tercih edilmiştir.

Bu şartlar altında 31 maddeli ölçeğe faktör analizi yapılmış ve B21. soru tek başına bir faktör oluşturduğu için anketten çıkarılarak kalan 30 maddeye tekrar faktör analizi uygulanmıştır. 30 maddeye uygulanan faktör analizi 9 faktör ortaya koymuştur; fakat B20,B2,B30,B12 ve B22 soruları da tek soru ile bir faktör oluşturdukları için teker teker anketten çıkarılmıştır. 25 maddeye uygulanan faktör analizi 7 faktör ortaya koymuştur; B16,B3, B4, B13 nolu maddeler binişiklik sorunu B28 ve B31 numaralı anket maddeleri ise .320'nin altında faktör yüküne sahip oldukları için analizden çıkarılmıştır. Kalan 19 maddeye tekrar uygulanan faktör analizi 6 faktör ortaya koymuştur; B15, B17 B1,B5 ve B28 nolu maddeler binişiklik sorunu olduğundan anketten çıkarılmış ve kalan 14 maddeye uygulanan faktör analizi 4 faktör ortaya koymuştur. Bu dört faktör, toplam varyansın % 52,001'nini açıklamaktadır. Analizde KMO örneklem yeterliliği ölçüsü %73,6 olarak hesaplanmış olup; Bartlett Küresellik testi anlamlı çıkmıştır ($p<,0001$). Bu iki ölçüt, veri setinin faktör analizine uygun olduğunu ve analize devam edilebileceğini göstermektedir. Bu test, aynı zamanda, maddeler arasında anlamlı korelasyonlar olduğu ve dolayısıyla veri setinin faktör analizine uygunluğuna da bir kanıt oluşturmaktadır (Kalaycı, 2006: 327). Faktör analizi sonucu Tablo 2.1'de görülmektedir.

Tablo 2.1.

Faktör Analizi

	Yükü	Özdeğeri	A.Varyans	Ortalama	Alfa
1.İnternetin kişisel değerlere karşı sakıncalarını algılama (4 madde)	1.963	14.021	1.7816	.644	
B11. Önemsediğim millî ve manevi değerlerimizi karalamak amacıyla yayın yapan web sitelerini kapatmak veya engellemek isterim.	.705				
B14. İnternette gezinirken her an müstehcen yayın içerikli bir site karşımıza çıkabilir	.641				
B6. İnternet üzerinden birçok suçun işlenebileceğine inanıyorum	.577				
B8. İnternette yapılan özel hayatı deşifre edici yayınlar kişileri toplum önünde küçük düşürülebilir.	.544				
2.Kişi ve örgütlerin İnterneti kötü niyetle kullanabileceklerini algılama (3 madde)	1.857	13.264	1.7410	.639	
B7. İnternette kötü niyetli insanların çok zararlı çalışmalar yaptığını düşünüyorum.	.790				
B9. Suç ve terör örgütleri çeşitli kurumların web sitelerini ve sistemlerini kendilerine hedef seçip buralara zarar verebilmektedir.	.713				
B10. Bireylerin yeni geliştirilen teknolojileri kullanırken güvende olabilmeleri için daha dikkatli olmaları gerekir.	.610				
3.Öğrencilerin İnternetteki rahatlık seviyesi (4 madde)	1.850	13.212	2.7584	.602	
B24. Bilgisayarımdaki bütün programların orijinal olması gerekmez	.724				
B19. Tanımadığım kişilerin İnternetini kullanırım.	.705				
B23. İnternette özgürlüğün sınırsız olması gerektiğini düşünüyorum	.664				
B18. Bilgisayarımda lisanssız yazılım kullanmaktan çekinmem	.566				

Tablo 2.1 (Devamı)

4.Öğrencilerin İnternette aldıkları önlem seviyesi (3 madde)	1.611	11.504	1.9071	.525
B25.İnternette gezinirken sitelerin beni yönlendirdiği değişik sitelere girmem.	.701			
B27.İnternette güvenli bulmadığım sitelere üye olmam	.688			
B26.İnternet şifrelerimin güvenlik seviyelerini önemserim.	.675			

Faktör çıkarma metodu: Temel bileşenler analizi; Döndürme metodu: Varimax

KMO Örneklem Yeterliliği: %.73.6 .; Bartlett's Küresellik Testi için X^2 : 568.031; sd: 91; $p < 0.0001$;

Açıklanan toplam varyans: %52.001;

Tablo 2.1'e göre ilk faktör, toplam varyansın % 14,021'ini açıklamakta ve 4 maddeden oluşmaktadır. Faktör analizinde “Önemsediğim millî ve manevi değerlerimizi karalamak amacıyla yayın yapan web sitelerini kapatmak veya engellemek isterim”, “İnternette gezinirken her an müstehcen yayın içerikli bir site karşımıza çıkabilir” “İnternet üzerinden birçok suçun işlenebileceğine inanıyorum” ve “İnternette yapılan özel hayatı deşifre edici yayınlar kişileri toplum önünde küçük düşürülebilir” maddelerinin bir araya gelmesiyle oluşan ilk faktöre “**İnternetin kişisel değerlere karşı sakıncalarını algılama**” adı verilmiştir.

İkinci faktör, toplam varyansın % 13,264'ünü açıklamakta ve 3 maddeden oluşmaktadır. Faktör analizinde “İnternette kötü niyetli insanların çok zararlı çalışmalar yaptığını düşünüyorum” ,”Suç ve terör örgütleri çeşitli kurumların web sitelerini ve sistemlerini kendilerine hedef seçip buralara zarar verebilmektedir” ve “Bireylerin yeni geliştirilen teknolojileri kullanırken güvende olabilmeleri için daha dikkatli olmaları gerekir” maddeleri bir araya gelmiştir. Bu maddelerin bir araya gelmesiyle oluşan ikinci faktöre “**Kişî ve örgütlerin İnterneti kötü niyetle kullanabileceklerini algılama**” adı verilmiştir

Üçüncü faktör, toplam varyansın % 13,212'sini açıklamakta ve 4 maddeden oluşmaktadır. Faktör analizinde “Bilgisayarındaki bütün programların orijinal olması gerekmez”, “Tanımadığım kişilerin İnternetini kullanırım”, “İnternette özgürlüğün sınırsız olması gerektiğini düşünüyorum” ve “Bilgisayarında lisanssız yazılım kullanmaktan çekinmem” maddeleri bir araya gelmiştir. Bu maddelerin bir araya

gelmesiyle oluşan üçüncü faktöre **“Öğrencilerin İnternetteki rahatlık seviyesi”** adı verilmiştir.

Dördüncü faktör, toplam varyansın % 11,504’ünü açıklamakta ve 3 maddeden oluşmaktadır. Faktör analizinde “İnternette gezinirken sitelerin beni yönlendirdiği değişik sitelere girmem.”, “İnternette güvenli bulmadığım sitelere üye olmam” ve “İnternet şifrelerimin güvenlik seviyelerini önemserim” maddeleri bir araya gelmiştir. Bu maddelerin bir araya gelmesiyle oluşan dördüncü faktöre **“Öğrencilerin İnternette aldıkları önlem seviyesi”** adı verilmiştir.

2.4. Verilerin Toplanması

Atatürk Üniversitesi Eğitim Bilimleri Enstitüsü aracılığıyla Erzurum İl Milli Eğitim Müdürlüğünden söz konusu anketin uygulanması için gerekli izinler alınmıştır. Alınan izin onay belgesi ile örnekleme belirttiğimiz okullarda anket uygulaması yapılarak veriler toplanmıştır.

Anket uygulaması esnasında alınan izin belgeleri okul yöneticilerine gösterilmiş ve gerekli bilgilendirmeler yapılmıştır. Araştırmacı tarafından ders hocaları ile iletişime geçilip anket uygulaması esnasında araştırmacı bizzat okullarda bulunmuştur.

2.5. Verilerin Analizi

Araştırma verileri SPSS 16 kullanılarak analiz edilmiştir. Frekans analizi bağımsız çift örneklem T- testi, Tek yönlü ANOVA testi kullanılmıştır.

T-testi, incelenen değişken (en az aralık seviyesinde ölçülmüş olması gerekli) için geçerli olan iki grup arasında istatistiksel açıdan herhangi bir anlamlı bir farklılığın tespitinde kullanılır (Altunışık, Coşkun, Bayraktaroğlu ve Yıldırım, 2012). Bağımsız çift örneklem T-testi için ise; karşılaştırılan bu grupların değişik evrenlerden rastgele seçilmesi ve gözlemlerinin birbirlerini etkilemeyecek şekilde gerçekleştirilmesi gerekmektedir. (Altunışık vd, 2012). Altunışık ve diğerlerine (2012) göre Anova testi, sadece gruplar arasındaki farklılıkların varlığına ilişkin bilgi sağlarken; Tek yönlü Anova Testi ise gruplar arasındaki farklılığa sebep olanın hangisi olduğu konusunda da bilgi vermektedir.

ÜÇÜNCÜ BÖLÜM

3. BULGULAR VE YORUM

3.1. Bilişim Bölümü Öğrencilerinin Demografik Özelliklerinin ve Ankete Verdikleri Yanıtların Genel Dağılımı İle İlgili Bulgular

Tablo 3.1.

Bilişim Bölümü Öğrencilerinin Demografik Özelliklerinin Frekans ve Yüzde Dağılımları

	(Frekans) N	(Yüzde) %
Cinsiyet		
Kadın	72	26.8
Erkek	197	73.2
Sınıf		
lise 1	2	0.7
lise 2	149	55.4
lise 3	87	32.3
lise 4	31	11.5
İnternete Girilen Yer		
Bağlanmıyorum	23	8.6
Evden	164	61
İnternet Kafeden	92	34.2
Cep telefonuyla	169	62.8
Okulda BT Sınıfından	73	27.1
Diğer	28	10.4

Tablo 3.1 (Devamı)

İnterneti Kullanım Yılları		
Kullanmıyorum	29	10.8
0-1 yıl	20	7.4
1-2 yıl	21	7.8
2-3 yıl	31	11.5
3 yıl üstü	168	62.5
Antivirüs Programı Kullanımı		
Evet	208	77.3
Hayır	61	22.7
İnterneti Kullanım Saati		
0-1 saat	94	34.9
1-2 saat	53	19.7
2-3 saat	42	15.6
3-4 saat	21	7.8
4 saat üstü	59	21.9
Kredi Kartı ile Alışveriş Yapma		
Evet	27	10
Hayır	242	90
Siber Saldırıya Uğrama		
Evet	50	18.6
Hayır	219	81.4

Araştırmaya katılan öğrencilerin % 26,8'si kadın iken % 73,2'si erkektir. Araştırmaya katılanların çoğunluğunu erkekler oluşturmaktadır. Araştırmaya katılan öğrencilerin % 0,7'sini lise 1. sınıf öğrencileri oluştururken, % 55,4'ünü lise 2. sınıflar,

% 32,3'ünü lise 3. sınıflar, 11,5'inide lise 4. sınıflar oluşturmuştur. Çalışmaya katılanların yarısından fazlasını lise 2. sınıflardan oluştuğu görülmüştür.

Araştırmaya katılan 269 katılımcıdan % 8,6'sı internete bağlanmadıklarını söylerken, % 61'i evden, % 34,2'si İnternet kafeden, % 62,8'i cep telefonundan, % 27,1'i okulda bilgisayar teknolojisi sınıfından, % 10,4'ü de diğer bağlantı araçlarını kullanarak İnternete bağlandıklarını söylemektedirler. Buradan da görüldüğü gibi öğrencilerin çoğu ya evden yada cep telefonlarından İnternete bağlanmaktadır.

Katılımcıların % 10,8'i İnterneti kullanmadıklarını söylerken, % 7,4'ü 0-1 yıldır kullandığını, % 7,8'i 1-2 yıl arasında kullandığını, % 11,5'i 2-3 yıl arasında kullandığını, % 62,5'i ise 3 yıl üstü süredir kullandığını söylemişlerdir. Görüldüğü gibi öğrencilerin çoğunun 3 yıl üstünde İnternet kullandıkları görülmüştür.

Araştırmaya katılan 269 kişiden % 77,3'ü antivirüs programı kullandıklarını söylerken % 22,7'si antivirüs programı kullanmadıklarını dile getirmişlerdir. Katılımcıların geneli antivirüs programının bilgisayarı koruduğunu bildiği görülmüştür.

Araştırmaya katılan 269 kişiden % 34,9'unun İnternet kullanımı günde 0-1 saat iken, % 19,7'sinin 1-2 saat arasında, % 15,6'sının 2-3 saat arasında, % 7,8'inin 3-4 saat arasında, % 21,9'unun ise İnternet kullanımı dört saatten fazla olduğu belirlenmiştir. Katılımcıların yarısından fazlasının İnternet kullanımı için günde bir saatten fazla zaman harcadıkları görülmüştür.

Araştırmaya katılan katılımcıların % 10'u ailelerine ait kredi kartı ile alışveriş yaparken, % 90'ı kredi kartı ile alışveriş yapmadıklarını belirtmişlerdir. Katılımcıların genel olarak kredi kartı ile alışveriş tecrübelerinin olmadıkları söylenebilir. Bunun sebebi olarak ailelerin öğrencilere kredi kartlarını vermemeleri gösterilebilir.

Katılımcılara İnternet ortamında sizi mağdur edecek bir olayla veya saldırıyla karşılaştınız mı sorusuna katılımcıların % 18,6'sı uğradıklarını söylerken, % 81,4'ü herhangi bir saldırıya uğramadıklarını belirtmişlerdir.

Tablo 3.2.

Bilişim Bölümü Öğrencilerinin Likert Ölçekli Sorulara Verdikleri Cevapların Frekans ve Yüzde Dağılımları

		Tamamen Katılıyorum	Katılıyorum	Kararsızım	Katılmıyorum	Hiç Katılmıyorum
1. İnterneti yaşamımın her alanında kullanırım.	N	107	90	40	27	5
	%	39.8	33.5	14.9	10	1.9
2. İnternet ve bilgisayar alanındaki teknolojik gelişmeleri takip ederim.	N	102	86	44	25	12
	%	37.9	32	16.4	9.3	4.4
3. Çevremde kendini hacker olarak tanıtan arkadaşlarım var.	N	57	68	44	43	57
	%	21.2	25.3	16.4	16	21.2
4. Bilgisayar ve İnternet her zaman özel ilgi alanıma girmiştir.	N	101	68	46	32	22
	%	37.5	25.3	17.1	11.9	8.2
5. Teknolojik gelişmelerin insanlara yararı olduğu kadar zararı da vardır.	N	147	82	21	11	8
	%	54.6	30.5	7.8	4.1	3
6. İnternet üzerinden birçok suçun işlenebileceğine inanıyorum.	N	158	73	23	10	5
	%	58.7	27.1	8.6	3.7	1.9
7. İnternette kötü niyetli insanların çok zararlı çalışmalar yaptığını düşünüyorum.	N	146	85	28	5	5
	%	54.3	31.6	10.4	1.9	1.9
8. İnternette yapılan özel hayatı deşifre edici yayınlar kişileri toplum önünde küçük düşürülebilir.	N	137	97	23	8	4
	%	50.9	36.1	8.6	3	1.4
9. Suç ve terör örgütleri çeşitli kurumların web sitelerini ve sistemlerini kendilerine hedef seçip buralara zarar verebilmektedir.	N	122	88	43	11	5
	%	45.4	32.7	16	4.1	1.9
10. Bireylerin yeni geliştirilen teknolojileri kullanırken güvende olabilmeleri için daha dikkatli olmaları gerekir.	N	141	90	22	10	6
	%	52.4	33.5	8.2	3.7	2.3
11. Önemsediğim millî ve manevî değerlerimizi karalamak amacıyla yayın yapan web sitelerini kapatmak veya engellemek isterim.	N	136	68	38	15	12
	%	50.6	25.3	14.1	5.6	4.5
12. İnternet aracılığıyla yaptığımız haberleşmenin engellenmesi ve gizliliğinin ihlali söz konusu olabilir.	N	92	76	53	25	23
	%	34.2	28.3	19.7	9.3	8.6
13. İnternette banka ve kredi kartı işlemlerinin yapılması tehlikeli buluyorum	N	120	76	40	22	11
	%	44.6	28.3	14.9	8.2	4.1
14. İnternette gezinirken her an müstehcen yayın içerikli bir site karşımıza çıkabilir.	N	123	88	36	14	8
	%	45.7	32.7	13.4	5.2	3

Tablo 3.2 (Devamı)

15. Bilgisayar ve İnternet aracılığıyla hırsızlık veya dolandırıcılık olayları daha kolay yapılır hale gelmiştir.	N	133	82	23	22	9
	%	49.4	30.5	8.6	8.2	3.3
16. Günümüzde kumar oynamak ve oynatmak isteyenler sanal ortamı kullanmaktadırlar.	N	121	78	39	16	15
	%	45	29	15.5	5.9	5.6
17. Her şeye rağmen İnternetin güvenli bir alan olduğunu düşünüyorum.	N	60	53	95	33	28
	%	22.3	19.7	35.3	12.3	10.4
18. Bilgisayarımda lisanssız yazılım kullanmaktan çekinmem.	N	59	63	62	42	43
	%	21.9	23.4	23	15.6	16
19. Tanımadığım kişilerin İnternetini kullanırım.	N	66	51	49	42	61
	%	24.5	19	18.2	15.6	22.7
20. İnternetin özgür bir iletişim platformu olduğunu düşünüyorum.	N	91	66	64	25	23
	%	33.8	24.5	23.8	9.3	8.6
21. Herhangi bir web sayfasına üye olurken kimlik numarası, telefon numarası veya adres bilgilerimi vermekten çekinmem.	N	47	47	35	50	90
	%	17.5	17.5	13	18.5	33.5
22. İnternetteki sitelerde oluşturduğum profillerde gerçek kimlik bilgilerimi kullanırım.	N	60	70	45	41	53
	%	22.3	26.1	16.7	15.2	19.7
23. İnternette özgürlüğün sınırsız olması gerektiğini düşünüyorum.	N	84	54	60	36	35
	%	31.2	20.1	22.3	13.4	13
24. Bilgisayarımdaki bütün programların orijinal olması gerekmez.	N	78	58	44	36	53
	%	29	21.6	16.4	13.4	19.7
25. İnternette gezinirken sitelerin beni yönlendirdiği değişik sitelere girmem.	N	116	78	38	22	15
	%	43.1	29	14.1	8.2	5.6
26. İnternet şifrelerimin güvenlik seviyelerini önemserim.	N	142	75	26	14	12
	%	52.8	27.9	9.7	5.2	4.5
27. İnternette güvenli bulmadığım sitelere üye olmam.	N	145	54	42	15	13
	%	53.9	20.1	15.6	5.6	4.8
28. Tanımadığım kişilerden gelen e-postaları açmadan silerim.	N	100	62	48	32	27
	%	37.6	22.7	17.8	11.9	10
29. Tanımadığım kişilerin arkadaşlık isteğini kabul etmem.	N	104	54	53	29	29
	%	38.7	20.1	19.7	10.8	10.8
30. İnternetteki yasaklı sitelere girmekten çekinirim.	N	121	63	36	20	29
	%	45	23.4	13.4	7.4	10.8
31. İnternetteki şifrelerimi tahmin edilmesi zor biçimde oluştururum.	N	152	62	29	16	10
	%	56.5	23	10.8	5.9	3.7

Mesleki ve Teknik Liselerin bilişim bölümü öğrencilerine İnterneti yaşamının her alanında kullanıp kullanılmadığı sorulmuş; öğrencilerin % 39,8'i bu soruya tamamen katıldıklarını, % 33,5'i katıldıklarını, % 14,9'u kararsız kalırken, % 10'u katılmadıklarını, % 1,9'u hiç katılmadıklarını belirtmişlerdir. Bilişim bölümü öğrencilerinin % 73,3'ünün İnterneti yaşamının her alanında aktif bir şekilde kullandıkları görülmüştür. Hatta bilişim bölümünde okumalarından dolayı günlerinin çoğu vaktini bilgisayar karşısında geçirmektedirler.

İnternet ve bilgisayar alanındaki teknolojik gelişmeleri takip edip etmediği sorulmuş katılımcıların % 37,9'u bu soruya tamamen katıldıklarını, % 32'si katıldıklarını, % 16,4'ü kararsız kalırken, % 9,3'ü katılmadıklarını, % 4,4 hiç katılmadıklarını belirtmişlerdir. Bilişim bölümü öğrencilerinin % 69,9'unun İnternet ve bilgisayar alanındaki teknolojik gelişmeleri yakından takip ettikleri görülmüştür.

Çevrelerinde kendini hacker olarak tanıtan arkadaşların olup olmadığı sorulmuş ve katılımcıların % 21,2'si bu soruya tamamen katıldıklarını, % 25,3'ü katıldıklarını, % 16,4'ü kararsız kalırken, % 16'sı katılmadıklarını, % 21,2'si hiç katılmadıklarını belirtmişlerdir. Bilişim bölümü öğrencilerinin % 46,5'inin hacker olarak tabir ettikleri kişilerle arkadaş olduğu % 37'sinin bu kişilerle arkadaş olmadığı görülmüştür.

Bilgisayar ve İnternet'in her zaman özel ilgi alanı olup olmadığı sorulmuş, katılımcıların % 37,5'i bu soruya tamamen katıldıklarını, % 25,3'ü katıldıklarını, % 17,1'i kararsız kalırken, % 11,9'u bu soruya katılmadıklarını, % 8,2'si hiç katılmadıklarını belirtmişlerdir. Araştırmaya katılan 269 bilişim bölümü öğrencisinden % 62,8'inin bilgisayar ve İnterneti kendileri için özel ilgi alanı olarak gördükleri % 21,1'lik kısmın ise bilişim bölümü öğrencisi olmalarına rağmen bilgisayar ve İnterneti özel ilgi alanı olarak görmedikleri anlaşılmıştır.

Teknolojik gelişmelerin insanlara yararı olduğu kadar zararı da vardır diye soru sorulmuş katılımcıların % 54,6'sı bu soruya tamamen katıldıklarını, % 30,5'i katıldıklarını, % 7,8'i kararsız kalırken, % 4,1'i bu soruya katılmadıklarını, % 3'ü hiç katılmadıklarını belirtmişlerdir. Bilişim bölümü öğrencilerinin % 85,1 gibi büyük bir kısmı, teknolojik gelişmelerin faydalarının yan sıra zararlarının da olduğunu farkındadırlar.

İnternet üzerinden birçok suçun işlenebileceğine inandıkları katılımcılara sorulmuş ve katılımcıların % 58,7'si bu soruya tamamen katıldıklarını, % 27,1'i katıldıklarını, % 8,6'si kararsız kalırken, % 3,7'si bu soruya katılmadıklarını, % 1,9'u hiç katılmadıklarını belirtmişlerdir. Araştırmaya katılan bilişim bölümü öğrencilerinin % 85,8'lik kısmı İnternet üzerinden bir çok suçun işlenebileceği algısı içerisinde.

İnternette kötü niyetli insanların çok zararlı çalışmalar yaptığını düşünüyor musunuz diye sorulmuş ve katılımcıların % 54,3'ü bu soruya tamamen katıldıklarını, % 31,6'sı katıldıklarını, % 10,4'ü kararsız kalırken, % 1,9'u bu soruya katılmadıklarını, % 1,9'u hiç katılmadıklarını belirtmişlerdir. Araştırmaya katılan öğrencilerin % 85,9'luk kısmı İnternette kötü niyetli insanların çok zararlı çalışmalar yaptığının farkındadır.

İnternette yapılan özel hayatı deşifre edici yayınlar kişileri toplum önünde küçük düşürülebilir mi diye sorulmuş ve katılımcıların % 50,9'u bu soruya tamamen katıldıklarını, % 36,1'i katıldıklarını, % 8,6'sı kararsız kalırken, % 3'ü bu soruya katılmadıklarını, % 1,4'ü hiç katılmadıklarını belirtmişlerdir. Araştırmaya katılan bilişim sınıfı öğrencilerinin % 87 gibi büyük bir çoğunluğu İnternette yapılan özel hayatı deşifre edici yayınların kişileri toplum önünde küçük düşürebileceği bilincine sahip oldukları görülmektedir.

Suç ve terör örgütleri çeşitli kurumların web sitelerini ve sistemlerini kendilerine hedef seçip buralara zarar verebilmektedir sorusuna katılımcıların % 45,4'ü bu soruya tamamen katıldıklarını, % 32,7'si katıldıklarını, % 16'sı kararsız kalırken, % 4,1'i bu soruya katılmadıklarını, % 1,9'u hiç katılmadıklarını belirtmişlerdir. Araştırmaya katılan öğrencilerin % 78,1 gibi büyük çoğunluğu suç ve terör örgütlerinin sanal ortamı etkin bir şekilde kullandığını ve bu ortamda çeşitli resmi kurumların web sitelerini, kullandıkları sistemlerini kendilerine hedef seçip buralara zarar verebileceklerini düşünmektedirler.

Bireylerin yeni geliştirilen teknolojileri kullanırken güvende olabilmeleri için daha dikkatli olmaları gerekir sorusuna katılımcıların % 52,4'ü bu soruya tamamen katıldıklarını, % 33,5'i katıldıklarını, % 8,2'si kararsız kalırken, % 3,7'si bu soruya katılmadıklarını, % 2,3'ü hiç katılmadıklarını belirtmişlerdir. Araştırmaya katılan öğrencilerin % 85,9'u yeni geliştirilen teknolojilerin güvenlik konusunda daha fazla dikkat istediğini düşünmektedirler. İnternet, bilgisayar gibi birçok teknolojiyi

kullanırken kişilerin güvende olabilmeleri için daha dikkatli olmaları gerektiği düşünülmektedir.

Önemsediğim milli ve manevi değerlerimizi karalamak amacıyla yayın yapan web sitelerini kapatmak veya engellemek isterim sorusu sorulmuş ve katılımcıların % 50,6'sı bu soruya tamamen katıldıklarını, % 25,3'ü katıldıklarını, % 14,1'i kararsız kalırken, % 5,6'sı bu soruya katılmadıklarını, % 4,5'i hiç katılmadıklarını belirtmişlerdir. Araştırmaya katılan öğrencilerin % 75,9'u milli ve manevi değerlerin korunması mevzu bahis olduğu zaman yasal olsun, olmasın bir şekilde müdahale edip söz konusu sitelerin kapatılması için uğraşabileceklerini belirtmişlerdir. Şimdiye kadar sorulan tüm sorularda öğrencilerin yüksek bir yüzdeyle siber suçlara karşı farkındalıklarının olduğu görülse de maddi ve manevi değerlerin söz konusu olduğu durumlarda öğrencilerin elindeki imkanları yetkilerini aşarak kullanabilecekleri görülmektedir.

İnternet aracılığıyla yaptığımız haberleşmenin engellenmesi ve gizliliğinin ihlali söz konusu olabilir sorusu sorulmuş ve katılımcıların % 34,2'si bu soruya tamamen katıldıklarını, % 28,3'ü katıldıklarını, % 19,7'si kararsız kalırken, % 9,3'ü bu soruya katılmadıklarını, % 8,6'sı hiç katılmadıklarını belirtmişlerdir. Araştırmaya katılan öğrencilerin % 62,5'i haberleşmenin ve gizliliğinin engellenebileceği görüşündedirler.

İnternette banka ve kredi kartı işlemlerinin yapılmasını tehlikeli buluyorum sorusuna katılımcıların % 44,6'sı bu soruya tamamen katıldıklarını, % 28,3'ü katıldıklarını, % 14,9'u kararsız kalırken, % 8,2'si bu soruya katılmadıklarını, % 4,1'i hiç katılmadıklarını belirtmişlerdir. Araştırmaya katılan öğrencilerin 72,9'u İnternette alışveriş konusuna tedbirli yaklaşmaktadırlar. Bu alışveriş türünün tehlikeli ve dikkat isteyen bir alışveriş türü olduğu görüşündedirler.

İnternette gezinirken her an müstehcen yayın içerikli bir site karşımıza çıkabilir sorusuna katılımcıların % 45,7'si bu soruya tamamen katıldıklarını, % 32,7'si katıldıklarını, % 13,4'ü kararsız kalırken, % 5,2'si bu soruya katılmadıklarını, % 3'ü hiç katılmadıklarını belirtmişlerdir. Araştırmaya katılan öğrencilerin % 78,4'ü İnternette normal herhangi bir sitede dolaşırken, tıklanan bir linkten müstehcen yayın içerikli bir siteyle karşılaşabileceklerini belirtmişlerdir.

Bilgisayar ve İnternet aracılığıyla hırsızlık veya dolandırıcılık olayları daha kolay yapılır hale gelmiştir sorusuna katılımcıların % 49,4'ü bu soruya tamamen katıldıklarını, % 30,5'i katıldıklarını, % 8,6'sı kararsız kalırken, % 8,2'si bu soruya katılmadıklarını, % 3,3'ü hiç katılmadıklarını belirtmişlerdir. Araştırmaya katılan öğrencilerin % 79,9'u hırsızlık ve dolandırıcılık olaylarının İnternet ve bilgisayar aracılığıyla daha risksiz ve daha kolay yapıldığı algısı içerisindeyler.

Günümüzde kumar oynamak ve oynatmak isteyenler sanal ortamı kullanmaktadırlar sorusuna katılımcıların % 45'i bu soruya tamamen katıldıklarını, % 29'u katıldıklarını, % 15,5'i kararsız kalırken, % 5,9'u bu soruya katılmadıklarını, % 5,6'sı hiç katılmadıklarını belirtmişlerdir. Araştırmaya katılan öğrencilerin % 74'ü günümüzde kumar oynamak ve oynatmak isteyenlerin İnterneti aktif bir şekilde kullandıkları düşüncesindedirler.

Her şeye rağmen İnternetin güvenli bir alan olduğunu düşünüyorum sorusuna katılımcıların % 22,3'ü bu soruya tamamen katıldıklarını, % 19,7'si katıldıklarını, % 35,3'ü kararsız kalırken, % 12,3'ü bu soruya katılmadıklarını, % 10,4'ü hiç katılmadıklarını belirtmişlerdir. Araştırmaya katılan öğrencilerin % 42'si İnternetin güvenli bir alan olduğunu düşünse de % 58'i İnternetin güvenli bir alan olduğuna onay vermemektedir. % 35,3'lük bir kısım İnternetin henüz güvenli veya güvensiz bir ortam olduğu konusunda karar verememiş kesimdir.

Bilgisayarımda lisanssız yazılım kullanmaktan çekinmem sorusuna katılımcıların % 21,9'u tamamen katıldıklarını, % 23,4'ü katıldıklarını, % 23'ü kararsız kalırken, % 15,6'sı bu soruya katılmadıklarını, % 16'sı hiç katılmadıklarını belirtmişlerdir. Araştırmaya katılan öğrencilerin % 45,3'ünün lisanssız bir yazılım kullanmaktan çekinmediği görülmüştür. Bu oran bize lisanssız yazılım kullanmanın bilişim bölümü öğrencileri arasında siber suç algısı oluşturmadığını anlatmaktadır.

Tanımadığım kişilerin İnternetini kullanırım maddesine katılımcıların % 24,5'i tamamen katıldıklarını, % 19'u katıldıklarını, % 18,2'si kararsız kalırken, % 15,6'sı bu soruya katılmadıklarını, % 22,7'si hiç katılmadıklarını belirtmişlerdir. Araştırmaya katılan öğrencilerin % 43,5'i tanımadıkları kişilerin İnternetini kullanma konusunda sıkıntı görmezken % 38,3'ü tanımadığı kişilerin İnternetini kullanma konusunda olumsuz görüş bildirmişlerdir.

İnternetin özgür bir iletişim platformu olduğunu düşünüyorum maddesine katılımcıların % 33,8'i tamamen katıldıklarını, % 24,5'i katıldıklarını, % 23,8'i kararsız kalırken, % 9,3'ü bu soruya katılmadıklarını, % 8,6'sı hiç katılmadıklarını belirtmişlerdir. Araştırmaya katılan öğrencilerin % 58,3'ünün İnterneti özgür bir iletişim platformu olarak algıladıkları görülmüştür.

Herhangi bir web sayfasına üye olurken kimlik numarası, telefon numarası veya adres bilgilerimi vermekten çekinmem maddesine katılımcıların % 17,5'i tamamen katıldıklarını, % 17,5'i katıldıklarını, % 13'ü kararsız kalırken, % 18,5'i bu soruya katılmadıklarını, % 33,5'i hiç katılmadıklarını belirtmişlerdir. Araştırmaya katılan öğrencilerin % 52'si herhangi bir web sayfasına üye olurken kimlik numarası, telefon numarası veya adres bilgilerini vermekten uzak durduklarını belirterek bunun tehlikeli bir iş olduğu algısını taşımaktadırlar.

İnternetteki sitelerde oluşturduğum profillerde gerçek kimlik bilgilerimi kullanırım maddesine katılımcıların % 22,3'ü tamamen katıldıklarını, % 26,1'i katıldıklarını, % 16,7'si kararsız kalırken, % 15,2'si bu soruya katılmadıklarını, % 19,7'si hiç katılmadıklarını belirtmişlerdir. Araştırmaya katılan öğrencilerin % 48,4'ü İnternetteki sitelerde oluşturdukları profillerde gerçek kimlik bilgilerini kullanmakta bir sakınca görmezken % 34,9'u gerçek bilgilerini kullanmaktan uzak durmaktadır.

İnternette özgürlüğün sınırsız olması gerektiğini düşünüyorum maddesine katılımcıların % 31,2'si tamamen katıldıklarını, % 20,1'i katıldıklarını, % 22,3'ü kararsız kalırken, % 13,4'ü bu soruya katılmadıklarını, % 13'ü hiç katılmadıklarını belirtmişlerdir. Araştırmaya katılan öğrencilerin % 51,3'ü İnterneti sınırsız bir alem olarak algılamakta bu sanal alemde özgürlüğün sınırlandırılmayacağı konusunda görüş bildirmişlerdir.

Bilgisayarındaki bütün programların orijinal olması gerekmez maddesine katılımcıların % 29'u tamamen katıldıklarını, % 21,6'sı katıldıklarını, % 16,4'ü kararsız kalırken, % 13,4'ü bu soruya katılmadıklarını, % 19,7'si hiç katılmadıklarını belirtmişlerdir. Araştırmaya katılan öğrencilerin % 50,6'sı bilgisayarında orijinal yazılımların kullanılmasını önemsememektedir % 33,1 ise bu konuda daha hassastır. Bu sorumuz anketimizin denetim sorusudur. Daha önceki maddelerde benzer soruya verilen

cevaplar ile bu sorumuza verilen cevaplarla aşağı yukarı aynıdır. Buda bize anketimizin gelişigüzel doldurulmadığını kanıtlamaktadır.

İnternette gezinirken sitelerin beni yönlendirdiği değişik sitelere girmem maddesine katılımcıların % 43,1'i tamamen katıldıklarını, % 29'u katıldıklarını, % 14,1'i kararsız kalırken, % 8,2'si bu soruya katılmadıklarını, % 5,6'sı hiç katılmadıklarını belirtmişlerdir. Araştırmaya katılan öğrencilerin % 72,1'i İnternette gezinirken sitelerin yönlendirdiği değişik sitelere girme konusunda olumsuz görüş bildirmiş ve bu konuda daha tedbirli olduklarını göstermişlerdir.

İnternet şifrelerimin güvenlik seviyelerini önemserim maddesine katılımcıların % 52,8'i tamamen katıldıklarını, % 27,9'u katıldıklarını, % 9,7'si kararsız kalırken, % 5,2'si bu soruya katılmadıklarını, % 4,5'i hiç katılmadıklarını belirtmişlerdir. Araştırmaya katılan öğrencilerin % 80,7'si İnternet şifrelerinin güvenlik seviyeleri konusunda oldukça tedbirli davrandıklarını ve bu konuyu önemsediklerini göstermişlerdir.

İnternette güvenli bulmadığım sitelere üye olmam maddesine katılımcıların % 53,9'u tamamen katıldıklarını, % 20,1'i katıldıklarını, % 15,6'sı kararsız kalırken, % 5,6'sı bu soruya katılmadıklarını, % 4,8'i hiç katılmadıklarını belirtmişlerdir. Araştırmaya katılan % 74 gibi büyük bir kısmı İnternette güvenli bulmadıkları veya güvenmedikleri sitelere üye olmadıklarını söyleyerek bu konuda tedbirli olduklarını göstermişlerdir.

Tanımadığım kişilerden gelen e-postaları açmadan silirim maddesine katılımcıların % 37,6'sı tamamen katıldıklarını, % 22,7'si katıldıklarını, % 17,8'i kararsız kalırken, % 11,9'u bu soruya katılmadıklarını, % 10'u hiç katılmadıklarını belirtmişlerdir. Katılımcıların % 60,3'ü tanımadıkları kişilerden gelen e-postaları virüs kaygısı veya başka kaygılardan dolayı açmadan sildiklerini belirtmişlerdir.

Tanımadığım kişilerin arkadaşlık isteğini kabul etmem maddesine katılımcıların % 38,7'si tamamen katıldıklarını, % 20,1'i katıldıklarını, % 19,7'si kararsız kalırken, % 10,8'i bu soruya katılmadıklarını, % 10,8'i hiç katılmadıklarını belirtmişlerdir. Araştırmaya katılan öğrencilerin % 58,8'i tanımadıkları kişilerden gelen arkadaşlık isteklerini uygun görmedikleri ve dolayısıyla kabul etmediklerini belirtmişlerdir.

İnternetteki yasaklı sitelere girmekten çekinirim maddesine katılımcıların % 45'i tamamen katıldıklarını, % 23,4'ü katıldıklarını, % 13,4'ü kararsız kalırken, % 7,4'ü bu soruya katılmadıklarını, % 10,8'i hiç katılmadıklarını belirtmişlerdir. Araştırmaya katılan öğrencilerin % 78,4'ü yasal olarak yasaklanan sitelere girme konusunda tedbirli davrandıkları ve bu sitelere girme konusunda ısrarcı olmadıklarını belirtmişlerdir.

İnternetteki şifrelerimi tahmin edilmesi zor biçimde oluştururum maddesine katılımcıların % 56,5'i tamamen katıldıklarını, % 23'ü katıldıklarını, % 10,8'i kararsız kalırken, % 5,9'u bu soruya katılmadıklarını, % 3,7'si hiç katılmadıklarını belirtmişlerdir. Araştırmaya katılan öğrencilerin % 79,5'i İnternetteki şifrelerini tahmin edilmesi zor biçimde oluşturduklarını belirtmişlerdir.

3.2. Tespit Edilen Faktörlerin Demografik Özelliklere Göre Farklılaşması

Katılımcıların bazı demografik özelliklerine göre, tespit edilen faktörler itibariyle ortalamaların farklılık gösterip göstermediğini anlamak için T-testi ve Anova yapılmıştır. Analiz sonuçları tablolarda gösterilmektedir. Buna göre dikkate alınan cinsiyet, sınıf, kaç yıldan beri İnternet kullanıldığı, siber saldırılara maruz kalınması gibi değişkenlerde farklılıklar tespit edilmektedir.

3.2.1. “İnternetin Kişisel Değerlere Karşı Sakıncalarını Algılama” Faktörünün Cinsiyete Göre Farklılaşması

Tablo 3.3.

İnternetin Kişisel Değerlere Karşı Sakıncalarını Algılama Faktörünün Cinsiyete Göre Farklılaşması

				Std.	t-	p-
	Cinsiyet	N	Ortalama	Sapma	değeri	değeri
İnternetin kişisel değerlere karşı sakıncalarını algılama	Bayan	72	1.5729	.66002	2.593	.010
	Erkek	196	1.8579	.84257		

Yapılan bağımsız çift örneklem T-testi analizi sonucunda cinsiyetin İnternetin kişisel değerlere karşı sakıncalarını algılama faktörü üzerinde farklılık yaratan bir değişken olduğunu ortaya koymuştur. Yapılan analiz sonucunda $p=0.010$ bulunmuş bu sonuç neticesinde ($p<.050$) olduğundan cinsiyet ile faktör arasında anlamlı bir farkın olduğu görülmüştür. Erkek katılımcıların kadın katılımcılara nispeten İnternetin kişisel değerlere karşı sakıncalarını algılamalarının daha yüksek olduğu görülmektedir.

3.2.2. “Kişi ve Örgütlerin İnterneti Kötü Niyetle Kullanabileceklerini Algılama” Faktörünün Cinsiyete Göre Farklılaşması

Tablo 3.4.

Kişi ve Örgütlerin İnterneti Kötü Niyetle Kullanabileceklerini Algılama Faktörünün Cinsiyete Göre Farklılaşması

	Cinsiyet	N	Ortalama	Std. Sapma	t- değeri	p- değeri
Kişi ve örgütlerin İnterneti kötü niyetle kullanabileceklerini algılama	Bayan	72	1.5602	.60469	2.267	.017
	Erkek	196	1.8071	.78968		

Yapılan bağımsız çift örneklem T-testi analizi sonucunda cinsiyetin Kişi ve örgütlerin İnterneti kötü niyetle kullanabileceklerini algılama faktörü üzerinde farklılık yaratan bir değişken olduğunu ortaya koymuştur. Yapılan analiz sonucunda $p=0.017$ bulunmuş bu sonuç neticesinde ($p<.050$) olduğundan cinsiyet ile faktör arasında anlamlı bir farkın olduğu görülmüştür. Erkek katılımcıların kadın katılımcılara nispeten İnternetin kişi ve örgütler tarafından kötü niyetle kullanabileceği algısı daha yüksek olduğu görülmektedir.

3.2.3. “Öğrencilerin İnternetteki Rahatlık Seviyesi” Faktörünün Cinsiyete Göre Farklılaşması

Tablo 3.5.

Öğrencilerin İnternetteki Rahatlık Seviyesi Faktörünün Cinsiyete Göre Farklılaşması

	Cinsiyet	N	Ortalama	Std. Sapma	t- değeri	p- değeri
Öğrencilerin İnternetteki rahatlık seviyesi	Bayan	72	2.9792	1.06211	2.273	.024
	Erkek	196	2.6777	.92487		

Yapılan bağımsız çift örneklem T-testi analizi sonucunda cinsiyetin Öğrencilerin İnternetteki rahatlık seviyesini ölçen faktör üzerinde farklılık yaratan bir değişken olduğu ortaya konmuştur. Yapılan analiz sonucunda $p=0.024$ bulunmuş bu sonuç neticesinde ($p<.050$) olduğundan cinsiyet ile faktör arasında anlamlı bir farkın olduğu görülmüştür. Bayan katılımcıların erkek katılımcılara nispeten İnternetteki rahatlık seviyelerinin daha yüksek olduğu görülmektedir.

3.2.4. “Öğrencilerin İnternette Aldıkları Önlem Seviyesi” Faktörünün Cinsiyete Göre Farklılaşması

Tablo 3.6.

Öğrencilerin İnternette Aldıkları Önlem Seviyesi Faktörünün Cinsiyete Göre Farklılaşması

	Cinsiyet	N	Ortalama	Std. Sapma	t- değeri	p- değeri
Öğrencilerin İnternette aldıkları önlem seviyesi	Bayan	72	1.7407	.76140	2.019	.045
	Erkek	196	1.9679	.83611		

Yapılan bağımsız çift örneklem T-testi analizi sonucunda cinsiyetin Öğrencilerin İnternette aldıkları önlem seviyesini ölçen faktör üzerinde farklılık yaratan bir değişken olduğu ortaya konmuştur. Yapılan analiz sonucunda $p=0.045$ bulunmuş bu sonuç

neticesinde ($p<.050$) olduğundan cinsiyet ile faktör arasında anlamlı bir farkın olduğu görülmüştür. Erkek katılımcıların kadın katılımcılara nispeten İnternetteki aldıkları önlem seviyelerinin daha yüksek olduğu görülmektedir.

3.2.5. “İnternetin Kişisel Değerlere Karşı Sakıncalarını Algılama” Faktörünün Sınıf Durumuna Göre Farklılaşması

Tablo 3.7.

İnternetin Kişisel Değerlere Karşı Sakıncalarını Algılama Faktörünün Sınıf Durumuna Göre Farklılaşması

	Sınıf	N	Ortalama	Std. Sapma	f- değeri	p- değeri
İnternetin kişisel değerlere karşı sakıncalarını algılama	1	2	1.1250	.12500		
	2	149	1.8121	.07245	.683	.563
	3	87	1.7816	.06800		
	4	31	1.6774	.15606		

Tek yönlü Anova analizi sonucunda katılımcıların İnternetin kişisel değerlere karşı sakıncalarını algılamalarının sınıflara göre istatistiksel olarak anlamlı bir şekilde farklılaştığı görülmemiştir. Yapılan analiz sonucunda $p=0.563$ bulunmuş bu sonuç neticesinde ($p>.001$) sınıf sırasının bilişim bölümü öğrencilerinin İnternetin kişisel değerlere karşı sakıncalarını algılama durumlarına etki etmediği anlaşılmıştır.

3.2.6. “Kişi ve Örgütlerin İnterneti Kötü Niyetle Kullanabileceklerini Algılama” Faktörünün Sınıf Durumuna Göre Farklılaşması

Tablo 3.8.

Kişi ve Örgütlerin İnterneti Kötü Niyetle Kullanabileceklerini Algılama Faktörünün Sınıf Durumuna Göre Farklılaşması

	Sınıf	N	Ortalama	Std. Sapma	f- değeri	p- değeri
Kişi ve örgütlerin İnterneti kötü niyetle kullanabileceklerini algılama	1	2	1.5000	.70711		
	2	149	1.7875	.78002	.866	.459
	3	87	1.7318	.69854		
	4	31	1.5591	.76200		

Tek yönlü Anova analizi sonucunda katılımcıların Kişi ve örgütlerin İnterneti kötü niyetle kullanabileceklerini algılamalarının sınıflara göre istatistiksel olarak anlamlı bir şekilde farklılaştığı görülmemiştir. Yapılan analiz sonucunda $p=0.459$ bulunmuş bu sonuç neticesinde ($p>.050$) sınıf sırasının bilişim bölümü öğrencilerinin kişi ve örgütlerin İnterneti kötü niyetle kullanabileceklerini algılama durumlarına etki etmediği anlaşılmıştır.

3.2.7. “Öğrencilerin İnternetteki Rahatlık Seviyesi” Faktörünün Sınıf Durumuna Göre Farklılaşması

Tablo 3.9.

Öğrencilerin İnternetteki Rahatlık Seviyesi Faktörünün Sınıf Durumuna Göre Farklılaşması

	Sınıf	N	Ortalama	Std. Sapma	f- değeri	p- değeri
Öğrencilerin İnternetteki rahatlık seviyesi	1	2	2.5000	.70711		
	2	149	2.9044	.94735	2.607	.052
	3	87	2.5603	1.00360		
	4	31	2.6290	.91940		

Tek yönlü Anova analizi sonucunda katılımcıların Öğrencilerin İnternetteki rahatlık seviyesi sınıflara göre istatistiksel olarak anlamlı bir şekilde farklılaştığı görülmemiştir. Yapılan analiz sonucunda $p=0.052$ bulunmuş bu sonuç neticesinde ($p>.050$) sınıf sırasının, bilişim bölümü öğrencilerinin İnternetteki rahatlık seviyesi durumlarına etki etmediği anlaşılmıştır.

3.2.8. “Öğrencilerin İnternette Aldıkları Önlem Seviyesi” Faktörünün Sınıf Durumuna Göre Farklılaşması

Tablo 3.10.

Öğrencilerin İnternette Aldıkları Önlem Seviyesi Faktörünün Sınıf Durumuna Göre Farklılaşması

	Sınıf	N	Ortalama	Std. Sapma	f- değeri	p- değeri
Öğrencilerin İnternette aldıkları önlem seviyesi	1	2	1.6667	.47140		
	2	149	1.8389	.75098	2.029	.110
	3	87	2.0805	.93726		
	4	31	1.7634	.76591		

Tek yönlü Anova analizi sonucunda katılımcıların Öğrencilerin İnternette aldıkları önlem seviyesi sınıflara göre istatistiksel olarak anlamlı bir şekilde farklılaştığı görülmemiştir. Yapılan analiz sonucunda $p=0.110$ bulunmuş bu sonuç neticesinde ($p>.050$) sınıf sırasının, bilişim bölümü öğrencilerinin İnternette aldıkları önlem seviyesine etki etmediği görülmüştür.

3.2.9. “İnternetin Kişisel Değerlere Karşı Sakıncalarını Algılama” Faktörünün İnterneti Kullanma Yılına Göre Farklılaşması

Tablo 3.11.

İnternetin Kişisel Değerlere Karşı Sakıncalarını Algılama Faktörünün İnterneti Kullanma Yılına Göre Farklılaşması

	İnterneti kullanma yılı	N	Ortalama	Std. Sapma	f- değeri	p- değeri
İnternetin kişisel değerlere karşı sakıncalarını algılama	Kullanmıyorum	29	2.0690	1.48939	1.535	.192
	0-1	20	1.5125	.42515		
	1-2	21	1.8214	.76989		
	2-3	31	1.7823	.68842		
	3+	168	1.7589	.68773		

Tek yönlü Anova analizi sonucunda katılımcıların İnternetin kişisel değerlere karşı sakıncalarını algılama düzeyi ile İnterneti kullanma yılları arasında istatistiksel olarak anlamlı bir şekilde farklılık görülmemiştir. Yapılan analiz sonucunda $p=0.192$ bulunmuş bu sonuç neticesinde ($p>.050$) İnterneti kullanma yılının, bilişim bölümü öğrencilerinin İnternetin kişisel değerlere karşı sakıncalarını algılama durumlarına etki etmediği görülmüştür.

3.2.10. “Kişi ve Örgütlerin İnterneti Kötü Niyetle Kullanabileceklerini Algılama” Faktörünün İnterneti Kullanma Yılına Göre Farklılaşması

Tablo 3.12.

Kişi ve Örgütlerin İnterneti Kötü Niyetle Kullanabileceklerini Algılama Faktörünün İnterneti Kullanma Yılına Göre Farklılaşması

	İnterneti kullanma yılı	N	Ortalama	Std. Sapma	f- değeri	p- değeri
Kişi ve örgütlerin İnterneti kötü niyetle kullanabileceklerini algılama	Kullanmıyorum	29	2.2069	1.19328	3.367	.010
	0-1	20	1.6500	.67082		
	1-2	21	1.7619	.73138		
	2-3	31	1.7419	.76357		
	3+	168	1.6678	.63550		

Tek yönlü Anova analizi sonucunda katılımcıların Kişi ve örgütlerin İnterneti kötü niyetle kullanabileceklerini algılama düzeyi ile İnterneti kullanma yılları arasında istatistiksel olarak anlamlı bir şekilde farklılık görülmüştür. Yapılan analiz sonucunda $p=0.010$ bulunmuş bu sonuç neticesinde ($p<.050$) İnterneti kullanma yılının, bilişim bölümü öğrencilerinin kişi ve örgütlerin İnterneti kötü niyetle kullanabileceklerini algılama düzeylerine etki ettiği görülmüştür.

3.2.11. “Öğrencilerin İnternetteki Rahatlık Seviyesi” Faktörünün İnterneti Kullanma Yılına Göre Farklılaşması

Tablo 3.13.

Öğrencilerin İnternetteki Rahatlık Seviyesi Faktörünün İnterneti Kullanma Yılına Göre Farklılaşması

	İnterneti kullanma yılı	N	Ortalama	Std. Sapma	f- değeri	p- değeri
Öğrencilerin İnternetteki rahatlık seviyesi	Kullanmıyorum	29	2.6934	1.04906	1.560	.185
	0-1	20	3.1375	.85353		
	1-2	21	2.6905	1.03653		
	2-3	31	2.9919	.91852		
	3+	168	2.7054	.96430		

Tek yönlü Anova analizi sonucunda öğrencilerin İnternetteki rahatlık seviyesi ile İnterneti kullanma yılları arasında istatistiksel olarak anlamlı bir şekilde farklılık görülmemiştir. Yapılan analiz sonucunda $p=0.185$ bulunmuş bu sonuç neticesinde ($p>.050$) İnterneti kullanma yılının, bilişim bölümü öğrencilerinin İnternetteki rahatlık seviyelerine etkisinin olmadığı anlaşılmıştır.

3.2.12. “Öğrencilerin İnternette Aldıkları Önlem Seviyesi” Faktörünün İnterneti Kullanma Yılına Göre Farklılaşması

Tablo 3.14.

Öğrencilerin İnternette Aldıkları Önlem Seviyesi Faktörünün İnterneti Kullanma Yılına Göre Farklılaşması

	İnterneti kullanma yılı	N	Ortalama	Std. Sapma	f- değeri	p- değeri
Öğrencilerin İnternette aldıkları önlem seviyesi	Kullanmıyorum	29	2.1264	.86563	1.192	.315
	0-1	20	1.6833	.66205		
	1-2	21	1.7143	.57044		
	2-3	31	1.9032	.66774		
	3+	168	1.9206	.87718		

Tek yönlü Anova analizi sonucunda Öğrencilerin İnternette aldıkları önlem seviyesi ile İnterneti kullanma yılları arasında istatistiksel olarak anlamlı bir şekilde farklılık görülmemiştir. Yapılan analiz sonucunda $p=0.315$ bulunmuş bu sonuç neticesinde ($p>.050$) İnterneti kullanma yılının bilişim bölümü öğrencilerinin İnternette aldıkları önlem seviyelerine etki etmediği anlaşılmıştır.

3.2.13. “İnternetin Kişisel Değerlere Karşı Sakıncalarını Algılama” Faktörünün Siber Saldırıya Uğrama Durumuna Göre Farklılaşması

Tablo 3.15.

İnternetin Kişisel Değerlere Karşı Sakıncalarını Algılama Faktörünün Siber Saldırıya Uğrama Durumuna Göre Farklılaşması

		İnternette saldırı	N	Ortalama	Std. Sapma	t- değeri	p- değeri
İnternetin kişisel değerlere karşı sakıncalarını algılama	Evet	50	1.7700	.58867	.151	.880	
	Hayır	219	1.7892	.85165			

Yapılan bağımsız çift örneklem T-testi analizi sonucunda öğrencilerin İnternette saldırıya maruz kalmalarının, İnternetin kişisel değerlere karşı sakıncalarını algılama faktörü üzerinde farklılık yaratan bir değişken olmadığı ortaya konulmuştur. Yapılan analiz sonucunda $p=0.880$ bulunmuş bu sonuç neticesinde ($p>.050$) olduğundan İnternette saldırıya maruz kalma durumu ile İnternetin kişisel değerlere karşı sakıncalarını algılama arasında anlamlı bir farkın olduğu görülmemiştir.

3.2.14. “Kişi ve Örgütlerin İnterneti Kötü Niyetle Kullanabileceklerini Algılama” Faktörünün Siber Saldırıya Uğrama Durumuna Göre Farklılaşması

Tablo 3.16.

Kişi ve Örgütlerin İnterneti Kötü Niyetle Kullanabileceklerini Algılama Faktörünün Siber Saldırıya Uğrama Durumuna Göre Farklılaşması

	İnternette saldırı	N	Ortalama	Std. Sapma	t- değeri	p- değeri
Kişi ve örgütlerin İnterneti kötü niyetle kullanabileceklerini algılama	Evet	50	1.7200	.74188	.263	.792
	Hayır	219	1.7512	.75668		

Yapılan bağımsız çift örneklem T-testi analizi sonucunda İnternette saldırıya maruz kalmanın, Kişi ve örgütlerin İnterneti kötü niyetle kullanabileceklerini algılama faktörü üzerinde farklılık yaratan bir değişken olmadığı ortaya koyulmuştur. Yapılan analiz sonucunda $p=0.792$ bulunmuş bu sonuç neticesinde ($p>.050$) olduğundan İnternette saldırı ile Kişi ve örgütlerin İnterneti kötü niyetle kullanabileceklerini algılama arasında anlamlı bir farkın olduğu görülmemiştir.

3.2.15. “Öğrencilerin İnternetteki Rahatlık Seviyesi” Faktörünün Siber Saldırıya Uğrama Durumuna Göre Farklılaşması

Tablo 3.17.

Öğrencilerin İnternetteki Rahatlık Seviyesi Faktörünün Siber Saldırıya Uğrama Durumuna Göre Farklılaşması

	İnternette			Std.	t-	p-
	saldırı	N	Ortalama	Sapma	değeri	değeri
Öğrencilerin	Evet	50	2.3800	.86785		
İnternetteki	Hayır	219	2.8525	.97041	3.163	.002
rahatlık seviyesi						

Yapılan bağımsız çift örneklem T-testi analizi sonucunda İnternette saldırıya maruz kalmanın, Öğrencilerin İnternetteki rahatlık seviyesi üzerinde farklılık yaratan bir değişken olduğu ortaya koyulmuştur. Yapılan analiz sonucunda $p=0.002$ bulunmuş bu sonuç neticesinde ($p<.050$) olduğundan İnternette saldırı ile öğrencilerin İnternetteki rahatlık seviyesi arasında anlamlı bir farkın olduğu görülmüştür. İnternette herhangi bir saldırıya maruz kalmayan öğrencilerin İnternetteki rahatlık seviyesi İnternette herhangi bir saldırıya maruz kalan öğrencilere göre daha fazladır.

3.2.16. “Öğrencilerin İnternette Aldıkları Önlem Seviyesi” Faktörünün Siber Saldırıya Uğrama Durumuna Göre Farklılaşması

Tablo 3.18.

Öğrencilerin İnternette Aldıkları Önlem Seviyesi Faktörünün Siber Saldırıya Uğrama Durumuna Göre Farklılaşması

	İnternette saldırı	N	Ortalama	Std. Sapma	t- değeri	p- değeri
Öğrencilerin	Evet	50	2.0333	.80601		
İnternette aldıkları önlem seviyesi	Hayır	219	1.8771	.82231	1.125	.225

Yapılan bağımsız çift örneklem T-testi analizi sonucunda İnternette saldırının, Öğrencilerin İnternette aldıkları önlem seviyesi üzerinde farklılık yaratan bir değişken olmadığı ortaya koymuştur. Yapılan analiz sonucunda $p=0.225$ bulunmuş bu sonuç neticesinde ($p>.050$) olduğundan İnternette saldırı ile Öğrencilerin İnternette aldıkları önlem seviyesi arasında anlamlı bir farkın olduğu görülmemiştir.

DÖRDÜNCÜ BÖLÜM

4. SONUÇ VE ÖNERİLER

Bilişim bölümü öğrencilerinin siber suçlara karşı farkındalık durumlarını belirlemek amacıyla yapılan bu araştırmada öğrencilerin İnternetin kişisel değerlere karşı sakıncalarını algılama düzeyleri, kişi ve örgütlerin İnterneti kötü niyetle kullanabileceklerini algılama seviyeleri, İnternetteki rahatlık seviyeleri ve İnternette aldıkları önlem seviyelerinin demografik özelliklere göre ilişkileri araştırılmıştır.

Araştırma, 2013-2014 eğitim-öğretim yılında Erzurum İlinde faaliyette olan Mesleki ve Teknik Liselerden kolay örnekleme yöntemi ile seçilen okullarda okuyan 72'si kız 197'si erkek toplamda 269 bilişim bölümü öğrencisi üzerinde yapılmıştır.

Çalışmada veriler, yerli-yabancı kaynaklardan yararlanılarak ve uzman görüşlerine başvurularak oluşturulan “Ortaöğretim Kurumlarında Siber Suç Farkındalık Anketi” ile toplanmıştır. Bu anket formunun genel sınırlılıkları ile sınırlı olan çalışmamızda öğrencilerin, anket sorularını okuyarak ve anlayarak cevapladıkları varsayılmıştır. Elde edilen bulgular, bize bilişim bölümü öğrencilerinin siber suç algı seviyeleri açısından bilgi vermektedir. Böylelikle siber suçlara karşı alınacak önlemlerin belirlenmesinde sorunun kökenine inilerek bireysel ve devlet nezdinde alınacak tedbirler için fikir edinilmektedir.

4.1. Sonuçlar

Bilişim bölümü öğrencilerinin siber suç farkındalık durumlarının belirlenmesi sonucu elde edilen bulgular, siber suçlara karşı alınacak önlemler konusunda değerlendirme yapmak, bilişim bölümü öğrencilerinin siber suçları algılama seviyeleri konusunda fikir sahibi olmak ve bu konuda çeşitli çalışmalar planlamak açısından çeşitli sonuçlar ortaya çıkarmıştır.

4.1.1. Bilişim Bölümü Öğrencilerinin Anket Sorularına Verdikleri Cevaplar İle Farkındalık Durum Sonuçları

Bilişim bölümü öğrencilerinin geneli, bilgisayar ile hayatını bütünleştirmiş, bilgisayarı hayatının her alanında kullanan, bilgisayara özel ilgi duyan ve bilgisayar ile bütünleşmiş kişilikler olarak karşımıza çıkmaktadırlar.

Bilişim bölümü öğrencilerinin % 81,7'sinin İnternetin kişisel değerlere karşı sakıncalarını algılayabildikleri görülmüştür. Yine bilişim bölümü öğrencilerinin % 83,3'ü kişi ve örgütlerin İnterneti kötü niyetle kullanabileceklerini algılayabildikleri görülmüştür. Türkoğlu vd. (2013) tarafından Elazığ Fırat Üniversitesi T.E.F. Bilgisayar bölümü ile T.F. Yazılım Mühendisliği bölümünde ve Meslek Liseleri Bilişim Teknolojileri Bölümlerinde yaptıkları araştırmada ortaöğretim bilişim bölümü öğrencilerinin bilişim suçları hakkında bilgi sahibi olma oranları % 45'dir. Siber suçların yazılı ve görsel medyada gün geçtikçe daha fazla yer alması ve toplum tarafından dillendirilmesi öğrencilerin bu konu hakkında bilgi sahibi olmasını sağlamaktadır. Fakat yine de bu oran yeterli değildir. Çünkü bu seviyede bilişim eğitimi alan öğrencilerin % 20'si siber suç konusunda bilgi sahibi değildir ve yaptığı işlerin yasal olup olmadığını bilmemektedir.

Yapılan araştırmada bilişim bölümü öğrencilerinin siber suçlara karşı farkındalıklarının % 80 üzerinde çıkmasına rağmen bölgenin milliyetçi bir yapıya sahip olmasından dolayı öğrencilerin milli ve manevi değerleri söz konusu olduğunda siber suçlara karşı farkındalığın % 25'lere kadar düştüğü görülmektedir.

Bilişim bölümü öğrencilerinin % 47,6'sının İnternette oldukça rahat tavırlar içerisinde olduğu görülmüştür. Türkoğlu vd. (2013) tarafından yapılan araştırmada öğrencilerin % 26'sı lisansız yazılım kullanma konusunda oldukça rahat iken bizim yaptığımız çalışmada öğrencilerin % 45,3'ü lisanssız yazılımları rahatça kullanabilmektedirler. Gün geçtikçe lisansız yazılımlara öğrencilerin rağbetinin arttığı görülmektedir. Ayrıca yaptığımız araştırmada öğrencilerin % 51,3'ü İnternet ortamında özgürlüğün sınırsız olması gerektiğini düşündüğünden özgürlüğün sınırının siber suçlara dayandığını fark edemedikleri görülmektedir.

Bilişim bölümü öğrencilerinin % 75,6'sının İnternetteki tehlikelere karşı üst seviye önlem aldıkları görülmektedir. Türkoğlu vd. (2013) tarafından yapılan

araştırmada öğrencilerin % 64'ü İnternetteki şifrelerinin güvenlik seviyelerini önemserken bizim araştırmamızda bu oran % 80,7'dir. İnternet teknolojisi ilerledikçe öğrencilerin bu ortamdaki tehlikelere karşı aldıkları önlemlerin arttığı görülmektedir.

4.1.2. Bilişim Bölümü Öğrencilerinin Cinsiyetleri ile Siber Suçları Algılama, İnternetteki Rahatlık Seviyesi ve İnternette aldıkları Önlem Seviyelerine İlişkin Sonuçlar

Yapılan analizler sonucunda cinsiyet ile öğrencilerin siber suçları algılamaları, İnternetteki rahatlık seviyeleri ve İnternette aldıkları önlem seviyeleri arasında anlamlı bir farkın olduğu sonucuna varılmıştır. Erkek öğrencilerin bayan öğrencilere nispeten İnternetin kişisel değerlere karşı sakıncalarını algılamalarının daha yüksek olduğu görülmektedir. Yine erkek katılımcıların kadın katılımcılara nispeten İnternetin kişi ve örgütler tarafından kötü niyetle kullanabileceği algısı daha yüksek olduğu görülmektedir. Yani genel olarak erkek öğrencilerin siber suç farkındalıklarının bayan öğrencilere göre daha fazla olduğu söylenebilmektedir.

Öğrencilerin İnternetteki rahatlık seviyelerine bakacak olursak; Bayan öğrencilerin erkek öğrencilere nispeten İnternetteki rahatlık seviyelerinin daha yüksek olduğu görülmektedir.

Yine öğrencilerin İnternette aldıkları önlem seviyelerine bakacak olursak; Erkek katılımcıların kadın katılımcılara nispeten İnternetteki aldıkları önlem seviyelerinin daha yüksek olduğu görülmektedir.

Elde edilen bu sonuçlar doğrultusunda bayan öğrencilerin siber suç farkındalıklarının az olması, İnternette aldıkları önlem seviyelerinin az olması ve İnternette rahatlık seviyelerinin yüksek olması nedeniyle siber suçlara daha fazla maruz kalabilecekleri söylenebilir. Erkek öğrencilerin siber suç konusunda farkındalıklarını yüksek olması, İnternette yeterince önlem almaları ve rahat tavırlar içerisinde olmamaları onların siber suçlar konusunda çok fazla mağdur olmamalarını sağlamaktadır.

4.1.3. Bilişim Bölümü Öğrencilerinin Okudukları Sınıflar ile Siber Suçları Algılama, İnternetteki Rahatlık Seviyesi ve İnternette aldıkları Önlem Seviyelerine İlişkin Sonuçlar

Yapılan analiz sonuçlarına göre sınıf türü ile öğrencilerin siber suçları algılamaları, İnternetteki rahatlık seviyeleri ve İnternette aldıkları önlem seviyeleri arasında anlamlı bir farkın olmadığı anlaşılmıştır. Öğrencilerin bilişim bölümü ile tanışmalarından itibaren lise son sınıfa kadar siber suç farkındalık seviyelerinin, İnternetteki rahatlık seviyelerinin ve İnternette aldıkları önlem seviyelerinin değişmediği görülmektedir. Yani öğrencilerin bilişim bölümünde okudukları süre boyunca siber suçlar ve bunun için alabilecekleri önlemler doğrultusunda bilinçlendirilmedikleri sonucu çıkarılabilir.

4.1.4. Bilişim Bölümü Öğrencilerinin İnterneti Kullanma Yılları ile Siber Suçları Algılama, İnternetteki Rahatlık Seviyesi ve İnternette aldıkları Önlem Seviyelerine İlişkin Sonuçlar

Yapılan analiz sonuçlarına göre öğrencilerin İnterneti kullanma yılları ile öğrencilerin İnternetin kişisel değerlere karşı sakıncalarını algılamaları, İnternetteki rahatlık seviyeleri ve İnternette aldıkları önlem seviyeleri arasında anlamlı bir farkın olmadığı anlaşılmıştır. Bilişim bölümü öğrencilerinin İnterneti kullanma yıllarının artması kişisel değerlere karşı siber suç farkındalık seviyeleri, İnternetteki rahatlık seviyeleri ve İnternette aldıkları önlem seviyelerini etkilememektedir. Öğrencilere çeşitli yollarla bu bilinçlilik verilmediği taktirde İnterneti ne kadar kullanırsa kullansınlar bu bilincin kendiliğinden oluşmayacağı sonucuna varılabilir.

4.1.5. Bilişim Bölümü Öğrencilerinin İnternette Saldırıya Uğrama Durumu İle Siber Suçları Algılama, İnternetteki Rahatlık Seviyesi ve İnternette Aldıkları Önlem Seviyelerine İlişkin Sonuçlar

Yapılan analiz sonuçlarına göre öğrencilerin İnternette saldırıya uğrama durumları ile öğrencilerin siber suçları algılamaları ve İnternette aldıkları önlem seviyeleri arasında anlamlı bir farkın olmadığı anlaşılmıştır. Yani öğrencilerin herhangi siber saldırıya uğraması siber suçlara karşı farkındalıklarını değiştirmemektedir. Aynı

şekilde siber suçlara maruz kalan öğrencilerin İnternette aldıkları önlem seviyelerinde bir değişiklik olmadığı sonucuna varılmıştır. Buna karşın yapılan analiz sonuçlarında öğrencilerin İnternette saldırıya uğrama durumları ile öğrencilerin İnternetteki rahatlık seviyeleri arasında anlamlı bir farkın olduğu tespit edilmiştir. İnternette herhangi bir siber saldırıya maruz kalan öğrencilerin İnternetteki rahat tavırlarında değişiklik olduğu ve artık eskisi kadar rahat davranmadıkları tespit edilmiştir.

4.2. Öneriler

Araştırmanın bulgu ve sonuçlarına dayanılarak aşağıdaki öneriler yapılabilir:

- Bu araştırma Erzurum İlinde üç tane Mesleki ve Teknik Lisesini kapsayacak şekilde yapılmış olup Türkiye'nin değişik bölgelerinde daha fazla Mesleki ve Teknik Lisesine yapılması önerilebilir.
- Bu araştırma, ortaöğretimden bir önceki eğitim-öğretim periyodu olan İlköğretim 6, 7 ve 8'inci sınıflara uygulanıp siber suç olgusunun daha genç yaşlarda araştırılması yapılabilir.
- Ortaöğretim çağındaki öğrencilerin siber suçlara karşı farkındalıklarının artırılması için kamu spotu reklam kuşaklarıyla gençlerin bilinçlendirilmesi yoluna gidilebilir.
- Bilişim bölümü öğretmenlerinin öğrencilerdeki siber suçlara karşı farkındalık seviyelerini artırabilmeleri için siber suç konusunun yasal boyutu hakkında hizmet içi eğitime tabi tutulmaları önerilebilir.
- Bilişim bölümü öğrencilerinin bilgisayar ve İnternet ağırlıklı derslerinde siber suçlar ve yasal boyutlarını kapsayacak şekilde müfredat değişikliği yapılması önerilebilir.
- Geleceğin bilişim öğretmenlerinin yetiştiği Üniversitelerin Teknik Eğitim Fakültesi Bilişim Bölümlerinde siber suç konusunun ders olarak verilmesi önerilebilir.
- Siber suçlarla mücadele konusunda emniyet teşkilatı üyelerinin eğitilmesi ve ortaöğretim öğrencilerinin siber suçlara karşı bilinçlendirilmesi için eğitimli emniyet personelinin liselerde seminerler vermesi önerilebilir.
- Kolluk kuvvetlerinin siber suçlar konusunda önleyici hizmet anlayışına ağırlık vererek toplumda siber suç farkındalığı oluşturmaları önerilebilir.

KAYNAKÇA

- Acar, A. E. (2013). *Medeni Muhakeme Hukukunda Elektronik İmzalı Belgelerin Delil Niteliği*. İstanbul: Levha Yayıncılık.
- Akarslan, H. (2012). *Bilişim Suçları*. Ankara: Seçkin Yayıncılık.
- Akbulut, B. (1999). *Türk Ceza Hukukunda Bilişim Suçları*. Yayınlanmamış Doktora Tezi. Selçuk Üniversitesi Sosyal Bilimler Enstitüsü, Konya.
- Akıncı, H., Alıç, A. E., Er, C. (2004). Türk Ceza Kanunu ve Bilişim Suçları. Yeşim Atamer. (Ed.). *İnternet ve Hukuk*. İstanbul: İstanbul Bilgi Üniversitesi Yayınları.
- Akyazı, E., Dilmen, N. E., Kara, T. (2008). Toplumsal ve Ekonomik Etkileri Bağlamında Bilişim Çağının Yeni Tehdidi: Siberterör. 2. İstanbul Bilişim Kongresinde Sunulmuş Bildiri, İstanbul.
- Alaca, B. (2008). *Ülkemizde Bilişim Suçları ve İnternetin Suça Etkisi (Antropolojik ve Hukuki Boyutları ile)*. Yüksek lisans tezi. Ankara Üniversitesi Sosyal Bilimler Enstitüsü, Ankara.
- Alacakaptan, U. (1975). *Suçun Unsurları*. Ankara: Sevinç Matbaası.
- Altunışık, R., Coşkun, R., Bayraktaroğlu S., Yıldırım E. (2012). *Sosyal Bilimlerde Araştırma Yöntemleri*, Sakarya: Sakarya Kitabevi.
- Atıcı, B., Gümüş, Ç. (2003). Sanal Ortamda Gerçek Tehditler: Siber Terör. *Polis Dergisi*, (37), s.57–66.
- Artuk, M. E., Gökcen, A., Yenidünya, C. (2012). *Ceza Hukuku Özel Hükümler*. (12. Baskı). Ankara: Adalet Yayınevi.
- Aydın, E. D. (1992). *Bilişim Suçları ve Hukukuna Giriş*. Ankara: Doruk Yayınları.
- Becenı, Y., Uçkan, Ö. (2004). Bilişim İletişim Teknolojileri ve Ceza Hukuku, Yeşim Atamer. (Ed.). *İnternet ve Hukuk*. İstanbul: İstanbul Bilgi Üniversitesi Yayınları.
- Berry, A. (2003). *Sonsuzluğun Kıyıları*. Ankara: Tübitak Popüler Bilim Kitapları.
- Bilek, B. T. (2012). *Bilişim Suçları ve Üniversite Lisans Öğrencilerinin Bilişim Suçlarına Yönelik Görüşleri*. Yüksek lisans tezi. Gazi Üniversitesi Bilişim Enstitüsü, Ankara.

- Bostancı, F. (2011). *Suçla Mücadelede Farkındalığın Önemi: Banka ve Kredi Kartlarının Kötüye Kullanılması*. Yüksek lisans tezi. Kara Harp Okulu Savunma Bilimleri Enstitüsü, Ankara.
- Broadhurst, R. (2006). Developments In The Global Law Enforcement Of Cyber-Crime. *International Journal of Police Strategies & Management*, 29(3), p.408-433.
- Burden, K., Palmer, C. (2003). Cyber Crime - A New Breed of Criminal. *Computer Law & Security Review*, 19(3), p.222-227.
- Büyüköztürk, Ş., Çakmak, E. K., Akgün Ö. E., Karadeniz, Ş., Demirel, F. (2012). *Bilimsel Araştırma Yöntemleri*. Ankara: Pegem Yayıncılık.
- Canberk, G., Sağıroğlu, Ş. (2007). Çocuklar ve Gençlerin Bilgisayar ve İnternet Güvenliği. *Politeknik Dergisi*, 10(1), s.33-39.
- Clough, J. (2011). Cybercrime. *Commonwealth Law Bulletin*, 37(4), p.671-680.
- Csonka, P. (2000). Internet Crime. *Computer Law and Security Report*, 16(5), p.329-330.
- Çakmak, H., Demir, C. K. (2009). *Siber Dünyadaki Tehditler ve Kavramlar, Suç Terör ve Savaş Üçgeninde Siber Dünya*. Ankara: Barış Platin Kitabevi.
- Çeken, H. (2002). ABD’de İnternet Yoluyla İşlenen Suçlara İlişkin Düzenlemeler. *Askeri Adalet Dergisi*, (74), s.114.
- Çokluk, Ö., Şekercioğlu, G., Büyüköztürk, Ş. (2010). *Sosyal Bilimler İçin Çok Değişkenli İstatistik*. Ankara: Pegem Yayıncılık.
- Değirmenci, O. (2002). *Bilişim Suçları*. Yüksek lisans tezi. Marmara Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul.
- Demirbaş, T. (2005). *Kriminoloji*. Ankara: Seçkin Yayınları.
- Demircan, T. (2007). *Bilişim Alanında Suçlar*. Yüksek lisans tezi. Selçuk Üniversitesi Sosyal Bilimler Enstitüsü, Konya.
- Dijle, H., Doğan, N. (2011). Türkiye de Bilişim Suçlarına Eğitimli İnsanların Bakışı. *Bilişim Teknolojileri Dergisi*, 4 (2), s.43-54.

- Dönmezer, S. (1981). *Kriminoloji*. İstanbul: İstanbul Üniversitesi Yayını.
- Dönmezer, S. (2001). *Ceza Hukuku Özel Kısım - Kişilere ve Mala Karşı Cürümler*. (16. Baskı). İstanbul: Beta Yayınevi.
- Durmaz, Ş. (2006). *Bilişim Suçlarının Sosyolojik Analizi*. Yayımlanmamış yüksek lisans tezi. Gazi Üniversitesi Sosyal Bilimler Enstitüsü, Ankara.
- Duymaz, S. H. (2013). *Ortaokul Öğrencilerine Yönelik “Bilişim Etiği Öğretim Programı” Uygulaması*. Yüksek lisans tezi. Ege Üniversitesi Fen Bilimleri Enstitüsü, İzmir.
- Dülger, M. V. (2004). *Bilişim Suçları*. Ankara: Seçkin Yayıncılık.
- Dülger, M. V. (2012). *Bilişim Suçları ve İnternet İletişim Hukuku*. (2. Baskı). Ankara: Seçkin Yayıncılık.
- Erbaşı, A. A. (2007). Çocuk Pornografisi. *İstanbul Baro Dergisi*, 81 (4), s.1623 vd.
- Ergün, İ. (2008) *Siber Suçların Cezalandırılması ve Türkiye’de Durum*. (1. Baskı). Ankara: Turhan Kitabevi.
- Gheraouti, S. (2013). *Cyberpower: Crime, Conflict and Security in Cyberspace*. EPFL Press.
- Gözübüyük, A. P. (1988). *Türk Ceza Kanunu Şerhi*. İstanbul: Kazancı Yayınları.
- Grabosky, P., Smith, R. (2001). Telecommunication Fraud in the Digital Age. In D. S. Wall (Ed.), *Crime and the Internet*, p.29-43. London, United Kingdom.
- Griffin, R.C. (2012). Cybercrime. *Journal of International Commercial Law and Technology*, 7(2), p.136-153.
- Hennessy, J. L., Patterson, D. A. (2007). *Computer Architecture: A Quantitative Approach*. Morgan Kaufmann Publishers.
- Horozgil, D. (2012). İfade ve Basın Özgürlüğü Çerçevesinde Soruşturma Evresinde Yayın Yasakları Üzerine Bazı Tespit ve Değerlendirmeler. *Hacettepe Hukuk Fakültesi Dergisi*, 2 (2), s.146-164.

- Hunton, P. (2011). A rigorous approach to formalising the technical investigation stages of cybercrime and criminality within a UK law enforcement environment. *Digital Investigation*, 7(3-4), p.105-113.
- İçel, K. (2001). *Kitle Haberleşme Hukuku*. (5. Baskı). İstanbul: Beta Yayınevi.
- İçişleri Bakanlığı Araştırma ve Etütler Merkezi. (2007). *İnternet ve Çocuklar / Gençler*, Ankara: İçişleri Bakanlığı AREM Yayınları.
- İlbaş, Ç. (2009). *Bilişim Suçlarının Sosyo-Kültürel Seviyelere Göre Algı Analizi*. Yüksek lisans tezi. Başkent Üniversitesi Fen Bilimleri Enstitüsü, Ankara.
- Johnson, T. A. (2005). *Forensic Computer Crime Investigation*. CRC Press.
- Kalaycı, Ş. (2010). *SPSS uygulamalı çok değişkenli istatistik teknikleri*. Ankara: Asil Yayıncılık.
- Kangal, Z. T. (2001). Fransa’da İnternet Yoluyla İşlenen Suçlardan Doğan Ceza Sorumluluğu. *İstanbul Üniversitesi Hukuk Fakültesi Mecmuası*, (1-2), s.227-240.
- Karagülmez, A. (2009). *Bilişim Suçları ve Soruşturma – Kavuşturma Evreleri*. Ankara: Seçkin Yayınevi.
- Karasar, N. (2011). *Bilimsel Araştırma Yöntemi*. (22. Baskı). Ankara: Nobel Kitapevi.
- Kardaş, Ü. (2003). Bilişim Dünyası ve Hukuk. *Karizma Dergisi*, (13), s.16.
- Ketizmen, M. (2008). *Türk Ceza Hukukunda Bilişim Suçları*. (1. Baskı). Ankara: Adalet Yayınevi.
- Koç, S., Kaynak, S. (2009). *Bilişim Suçları Bağlamında Yeni Medya Olarak İnternet ve Kişisel Güvenlik*. 14. Türkiye İnternet Konferansında Sunulmuş Bildiri, İstanbul.
- Kurt, L. (2005). *Açıklamalı İçtihatlı Tüm Yönleriyle Bilişim Suçları ve Türk Ceza Kanununda ki Uygulaması*. (1. Baskı). Ankara: Seçkin Yayınları.
- Lloyd, I. J. (2000). *Information Technology Law*. Butterworths Publishers.
- Mahmutoğlu, F. S. (5 Ekim 2001) *Bankacılık Suçları Bağlamında Çıkar Amaçlı Suç Örgütü*. Avrupa Birliğine Uyum Süreci Bağlamında organize Suçlulukla Mücadele, Panelinde Sunulmuş Bildiri, İstanbul.

- Martin, N., Rice, J. (2011). Cybercrime: Understanding and addressing the concerns of stakeholders. *Computers & Security*, 30(8), p.803-814.
- Meran, N. (2008). *Yeni Türk Ceza Kanunun da Sahtecilik Malvarlığı Bilişim Suçları ile Ekonomi ve Ticaret Alanında Suçlar*. (2. Baskı). Ankara: Seçkin Yayınevi.
- Nacar, F. B. (2010). *Avrupa Birliği Ülkeleri ve Türkiye’de bilişim Suçlarının Ceza Hukukundaki Uygulamaları*. Yüksek lisans tezi. Atılım Üniversitesi Sosyal Bilimler Enstitüsü, Ankara.
- Noyan, E. (2005). *Hırsızlık ve Yağma Suçları*. Ankara: Bilge Yayınevi.
- Nuhoğlu, A. (2002). *Ceza Hukukunda Kredi Kartlarının Kötüye Kullanılması*. İstanbul: Analiz Basım Yayınevi.
- Orta, M. (2005). *Elektronik İmza ve Uygulaması*. Ankara: Seçkin Yayıncılık.
- Özbek, V. Ö. (2002). İnternet Kullanımında Ortaya Çıkabilecek Bazı Ceza Hukuku Sorunları. *DEÜ Hukuk Fakültesi Dergisi*, 4(1), s.102-103.
- Özcan, M. (2004). Yeni Milenyumda Yeni Tehdit: Siber Terör. *Türk Harb-İş Dergisi*, (210), s.36-42.
- Özdamar, K. (2010). *Paket Programlar ile İstatistiksel Veri Analizi Cilt:1*. Eskişehir: Nisan Kitabevi.
- Özdilek, A. O. (2002). *İnternet ve Hukuk*. İstanbul: Papatya Yayıncılık.
- Özpehlivan, A. (2006). *Siber Terörizmle Mücadelede Kolluğun Rolü*. Yayımlanmamış yüksek lisans tezi. Kara Harp Okulu Savunma Bilimleri Enstitüsü, Ankara.
- Pallı, H. (2008). *Türk Hukukunda ve Mukayeseli Hukukta Bilişim Suçları*. Yayımlanmamış yüksek lisans tezi. Erciyes Üniversitesi Sosyal Bilimler Enstitüsü, Kayseri.
- Parlar, A., Hatipoğlu, M. (2008). *Türk Ceza Kanunu Yorumu* (2. Baskı, 4. Cilt). Ankara: Seçkin Yayınevi.
- Peker, B. (2010). *Bilişim Suçları ve Bilişim Güvenliğinin Ulusal ve Uluslararası Boyutu*. Yüksek lisans tezi. Selçuk Üniversitesi Sosyal Bilimler Enstitüsü, Konya.

- Pocor, F. (2004). New Challenges for International Rules Against Cybercrime. *European Journal on Criminal Policy and Research* 10, p.27-37.
- Sağlam, İ. (2007). *Elektronik Sözleşmeler*. İstanbul: Legal Yayınevi.
- Seigfried-Spellar, K.C., Lovely, R. W. ve Rogers, M. K. (2011). Self-Reported internet child pornography consumers: A personality assessment using Bandura's theory of reciprocal determinism. Jaishankar, K. (Ed.) *Cyber criminology exploring Internet crimes and criminal behavior*, p. 65-78, CRC Press.
- Sınar, H. (2001). *İnternet ve Ceza Hukuku*. İstanbul: Beta Yayınevi.
- Silva, K. (2013). Europe's fragmented approach towards cyber security. <http://policyreview.info/articles/analysis/europes-fragmented-approach-towards-cyber-security> adresinden 05.04.2014 tarihinde alınmıştır.
- Soyaslan, D. (2005). *Ceza Hukuku Genel Hükümler*. (Güncelleştirilmiş 3. Baskı). Ankara: Yetkin Yayınevi.
- Şeker, G. (2003). Kamu Alanında Bilginin İnternet ile Sunumu ve Önündeki Tehlikeler: Amerikan Örneği. *Polis Bilimleri Dergisi*, 5 (3-4), s.63-84.
- Şen, B. (2011). Bilişim Suçlarıyla Mücadele. http://www.tbmm.gov.tr/arastirma_komisyonlari/bilisim_internet/docs/sunumlar/egm_bilisim_suclari.pptx adresinden 06.02.2014 tarihinde alınmıştır.
- Taşkın, Ş. C. (2008). *Bilişim Suçları*. Bursa: Beta Yayınevi.
- Topaloğlu, M. (1997). *Bilgisayar Programları Üzerindeki Haklar ve Bu Hakların Korunması*. İstanbul: Bilge Yayıncılık.
- Torun, Ö. (2007). *Resmi Ortaöğretim Kurumlarında Öğrenim Gören Öğrencilerin İnternet Etiğine İlişkin Algılarının İncelenmesi*. Yayımlanmamış yüksek lisans tezi. Marmara Üniversitesi Eğitim Bilimleri Enstitüsü, İstanbul.
- Tulum, İ. (2006). *Bilişim Suçlarıyla Mücadele*. Yüksek lisans tezi. Süleyman Demirel Üniversitesi Sosyal Bilimler Enstitüsü, Isparta.
- Turhan, O. (2006). *Bilgisayar Ağları ile İlgili Suçlar (Siber Suçlar)*. Planlama uzmanlığı tezi. Başbakanlık Devlet Planlama Teşkilatı Müsteşarlığı Hukuk Müşavirliği, Ankara.
- Türkiye Dil Kurumu. (2014). *Büyük Türkçe Sözlük*. Ankara: Türkiye Dil Kurumu.

- Turla, A., Özkanlı, Ç. (2006). Çocuğa Yönelik İstismarda Farklı Bir Boyut: Çocuk Pornografisi. *Polis Bilimleri Dergisi*, 8(1), s.117-133.
- Türkoğlu, A., Özdemir, S., Kalkan, Ö.K., Varol, M. ve Tokdemir, M. (2013). Elazığ'da Üniversite ve Lisede Öğrenim Gören Bilgisayar Bölümü Öğrencilerinin Adli Bilişim Suçlarına Yaklaşımları. *NWSA-Medical Sciences*, 8 (3), s.16-25.
- Uz, B. (2013). Elektronik Haberleşme Sektöründe Açık Hatlar Sorunu ve Düzenleyici Kararların Etkileri. *Gazi Üniversitesi Hukuk Fakültesi Dergisi*, (17), s.295-311.
- Ünver, Y. (2001). Türk Ceza Kanunun ve Ceza Kanunu Tasarısının İnternet Açısından Değerlendirilmesi. *İstanbul Üniversitesi Hukuk Fakültesi Mecmuası*, (1-2), s. 67.
- Wall, D. S. (2008). Cybercrime, media and insecurity: The shaping of public perceptions of cybercrime. *International Review of Law Computers & Technology*, 22(1-2), p.19;45-63.
- Yayla, M. (2013). Hukuki Bir Terim Olarak “Siber Savaş”. *Türkiye Barolar Birliği Dergisi*, (104), s.177-202.
- Yazıcıoğlu, Y. (1997). *Bilgisayar Suçları Kriminolojik Sosyolojik ve Hukuki Boyutları ile*. (1. Baskı). İstanbul: AlfaYayımları.
- Yenidünya, C., Değirmenci, O. (2003). *Mukayeseli Hukukta ve Türk Hukukunda Bilişim Suçları*. İstanbul: Legal Yayınevi.
- Yıldırım, A., Şimşek, H. (2005). *Sosyal Bilimlerde Nitel Araştırma Yöntemleri*. (5. Baskı). Ankara: Seçkin Yayıncılık.
- Zarplı, Ç. (2008). *İfade Özgürlüğü: İçeriği ve Sınırları*. Yayımlanmamış yüksek lisans tezi. Dumlupınar Üniversitesi Sosyal Bilimler Enstitüsü, Kütahya.

EKLER

EK 1. İZİN BELGESİ



T.C.
ERZURUM VALİLİĞİ
İl Millî Eğitim Müdürlüğü

Sayı : 36648235/605.01/1182472

20/03/2014

Konu: Tez Çalışması

VALİLİK MAKAMINA

İlgi: a) Milli Eğitim Bakanlığı'nın Araştırma , Yarışma ve Sosyal Etkinlik İzinleri Konulu 07/03/2012 tarihli ve 3616 (2012/13) sayılı genelgesi.
b) Atatürk Üniversitesi'nin 04/03/2014 tarihli ve 88179374-5159 sayılı yazısı.

Atatürk Üniversitesi Eğitim Bilimleri Enstitüsü yüksek lisans öğrencisi Ömer SİDDİK'in ilgi (b) yazı ile "*Ortaöğretim Kurumlarında Öğrenim Gören Öğrencilerin Siber Suç Algılarının Ölçülmesi (Erzurum Örneği)*" konulu tez çalışmasına esas teşkil edecek çalışmayı 07/04/2014-11/04/2014 tarihleri arasında İlimiz Milli Eğitim Müdürlüğüne bağlı Endüstri ve Anadolu Endüstri Meslek Liselerinde uygulama isteği, ilgi (a) Genelge çerçevesinde Müdürlüğümüzce uygun görülmektedir.

Makamlarınızca da uygun görülmesi halinde olurlarınıza arz ederim.

Mustafa BASTEM
Millî Eğitim Müdür V.

OLUR
20/03/2014

Abdurrahman İÇYER
Vali a.
Vali Yardımcısı

Bu belge, 5070 sayılı Elektronik İmza Kanununun 5 inci maddesi gereğince güvenli elektronik imza ile imzalanmıştır

Yönetim Cad. Valilik Binası Kat:4 Yakutiye ERZURUM
Elektronik Ağ: <http://erzurum.meb.gov.tr>
e-posta: stratejigelistirme25@meb.gov.tr

Ayrıntılı bilgi için: Çiğdem HOPUR Şb.Mdr.
Tel: (0 442) 234 4800
Faks: (0 442) 235 1032

EK 2. ANKET FORMU

Ortaöğretim Kurumlarında Siber Suç Farkındalık Anketi

Değerli öğrenciler,

Bu anket ortaöğretim kurumlarında öğrenim gören öğrencilerinin siber suçları ne düzeyde algıladıklarını ölçmeyi hedefleyen bir ankettir. Vereceğiniz bilgiler sadece bilimsel araştırma amaçlı kullanılacaktır. Bu çalışma sonunda oluşturulacak raporlarda isminiz doğrudan veya dolaylı olarak asla kullanılmayacaktır. İlginiz ve katkılarınız için teşekkür ederiz.

(A1)-Sınıfınız: Lise 1() Lise 2() Lise 3() Lise 4()

(A2)-Cinsiyet: Kız () Erkek ()

(A3)-İnternete nerelerden bağlanıyorsunuz? (Birden fazla seçenek işaretleyebilirsiniz)

- Bağlanmıyorum ()
- Evden ()
- İnternet Kafeden ()
- Cep telefonu ()
- Okulda BT Sınıfından ()
- Diğer ()

(A4)-Kaç yıldan beri İnterneti kullanıyorsunuz?

- Kullanmıyorum ()
- 0-1 yıldır kullanıyorum ()
- 1-2 yıldır kullanıyorum ()
- 2-3 yıldır kullanıyorum ()
- 3 yıldan fazladır kullanıyorum ()

(A5)-İnterneti hangi amaçlarla kullanıyorsunuz? (Birden fazla seçenek işaretleyebilirsiniz)

- Oyun oynamak ()
- Video izlemek ()
- Arkadaşlarımla sohbet etmek ()
- Hayatımda ne olup bittiğini paylaşmak ()
- Ödev yapmak ()
- Araştırma yapmak ()
- Diğer ()

(A6)-Bilgisayarımda antivirüs programı kullanıyorum.

-Evet () -Hayır ()

(A7)-İnternete hangi sıklıkta giriyorsunuz.

- Günde 0-1 saat ()
- Günde 1-2 saat ()
- Günde 2-3 saat ()
- Günde 3-4 saat ()
- Günde 4 saatten fazla ()

(A8)-İnternette ailemin kredi kartı ile alışveriş yaparım.

-Evet () -Hayır ()

(A9)-İnternet ortamında sizi mağdur edecek bir olayla veya saldırıyla karşılaştınız mı?

-Evet () -Hayır ()

Aşağıdaki sorulara verebileceğiniz en uygun ve tek cevabı ilgili kutucuğa (X) yazarak belirtiniz. Boş bırakmayınız.

		Tamamen Katılıyorum	Katılıyorum	Kararsızım	Katılmıyorum	Hiç Katılmıyorum
		1	2	3	4	5
B1	İnterneti yaşamımın her alanında kullanırım.					
B2	İnternet ve bilgisayar alanındaki teknolojik gelişmeleri takip ederim.					
B3	Çevremde kendini hacker olarak tanıtan arkadaşlarım var.					
B4	Bilgisayar ve İnternet her zaman özel ilgi alanıma girmiştir.					
B5	Teknolojik gelişmelerin insanlara yararı olduğu kadar zararı da vardır.					
B6	İnternet üzerinden birçok suçun işlenebileceğine inanıyorum.					
B7	İnternette kötü niyetli insanların çok zararlı çalışmalar yaptığını düşünüyorum.					
B8	İnternette yapılan özel hayatı deşifre edici yayınlar kişileri toplum önünde küçük düşürülebilir.					
B9	Suç ve terör örgütleri çeşitli kurumların web sitelerini ve sistemlerini kendilerine hedef seçip buralara zarar verebilmektedir.					
B10	Bireylerin yeni geliştirilen teknolojileri kullanırken güvende olabilmeleri için daha dikkatli olmaları gerekir.					
B11	Önemsediğim millî ve manevi değerlerimizi karalamak amacıyla yayın yapan web sitelerini kapatmak veya engellemek isterim.					
B12	İnternet aracılığıyla yaptığımız haberleşmenin engellenmesi ve gizliliğinin ihlali söz konusu olabilir.					

B13	İnternette banka ve kredi kartı işlemlerinin yapılması tehlikeli buluyorum					
B14	İnternette gezinirken her an müstehcen yayın içerikli bir site karşımıza çıkabilir.					
B15	Bilgisayar ve İnternet aracılığıyla hırsızlık veya dolandırıcılık olayları daha kolay yapılır hale gelmiştir.					
B16	Günümüzde kumar oynamak ve oynatmak isteyenler sanal ortamı kullanmaktadırlar.					
B17	Her şeye rağmen İnternetin güvenli bir alan olduğunu düşünüyorum.					
B18	Bilgisayarımda lisanssız yazılım kullanmaktan çekinmem.					
B19	Tanımadığım kişilerin İnternetini kullanırım.					
B20	İnternetin özgür bir iletişim platformu olduğunu düşünüyorum.					
B21	Herhangi bir web sayfasına üye olurken kimlik numarası, telefon numarası veya adres bilgilerimi vermekten çekinmem.					
B22	İnternetteki sitelerde oluşturduğum profillerde gerçek kimlik bilgilerimi kullanırım.					
B23	İnternette özgürlüğün sınırsız olması gerektiğini düşünüyorum.					
B24	Bilgisayarımdaki bütün programların orijinal olması gerekmez.					
B25	İnternette gezinirken sitelerin beni yönlendirdiği değişik sitelere girmem.					
B26	İnternet şifrelerimin güvenlik seviyelerini önemserim.					
B27	İnternette güvenli bulmadığım sitelere üye olmam.					
B28	Tanımadığım kişilerden gelen e-postaları açmadan silerim.					
B29	Tanımadığım kişilerin arkadaşlık isteğini kabul etmem.					
B30	İnternetteki yasaklı sitelere girmekten çekinirim.					
B31	İnternetteki şifrelerimi tahmin edilmesi zor biçimde oluştururum.					

ÖZGEÇMİŞ

Kişisel Bilgiler

Adı Soyadı : Ömer Sıddık BUDAK

Doğum Yeri ve Tarihi: Erzurum 06/03/1985

Eğitim Durumu

Lisans : Atatürk Üniversitesi
Matematik Bölümü (2004-2008)

Lisans : Anadolu Üniversitesi
Kamu Yönetimi Bölümü (2008-2012)

Yabancı Dil : İngilizce

İş Deneyimi

2009-2014 : İstanbul İl Emniyet Müdürlüğü (Polis Memuru)

2014-..... : Kafkas Üniversitesi SMYO (Öğretim Görevlisi)

İletişim

Adres : Sarıkamış Meslek Yüksekokulu Sarıkamış/Kars

Elektronik Posta : omersiddikbudak@hotmail.com