T.C.
SELÇUK ÜNİVERSİTESİ
EĞİTİM BİLİMLERİ ENSTİTÜSÜ
BİLGİSAYAR VE ÖĞRETİM TEKNOLOJİLERİ EĞİTİMİ
ANABİLİM DALI

LİSE ÖĞRENCİLERİNİN SİBER SUÇ ALGI DÜZEYLERİNİN FARKLI DEĞİŞKENLER AÇISINDAN İNCELENMESİ (KIRŞEHİR İLİ ÖRNEĞİ)

Erdal LAFVERMEZ

YÜKSEK LİSANS TEZİ

Danışman
Prof.Dr. Ertuğrul USTA

Konya 2018

T.C.
SELÇUK ÜNİVERSİTESİ
EĞİTİM BİLİMLERİ ENSTİTÜSÜ
BİLGİSAYAR VE ÖĞRETİM TEKNOLOJİLERİ EĞİTİMİ
ANABİLİM DALI

LİSE ÖĞRENCİLERİNİN SİBER SUÇ ALGI DÜZEYLERİNİN FARKLI DEĞİŞKENLER AÇISINDAN İNCELENMESİ (KIRŞEHİR İLİ ÖRNEĞİ)

Erdal LAFVERMEZ

YÜKSEK LİSANS TEZİ

Danışman
Prof.Dr. Ertuğrul USTA

Konya 2018

T.C.
SELÇUK ÜNİVERSİTESİ
Eğitim Bilimleri Enstitüsü Müdürlüğü

BİLİMSEL ETİK SAYFASI

Adı Soyadı	**:** Erdal LAFVERMEZ
Numarası	**:**16830501030
Ana Bilim / Bilim Dalı :	Bilgisayar ve Öğretim Teknolojileri Eğitimi Bölümü
Programı	**:**Tezli Yüksek Lisans ● Doktora O
Tezin Adı	**:**Lise Öğrencilerinin Siber Suç Algı Düzeylerinin Farklı Değişkenler Açısından İncelenmesi (Kırşehir İli Örneği)

Bu tezin proje safhasından sonuçlanmasına kadarki bütün süreçlerde bilimsel etiğe ve akademik kurallara özenle riayet edildiğini, tez içindeki bütün bilgilerin etik davranış ve akademik kurallar çerçevesinde elde edilerek sunulduğunu, ayrıca tez yazım kurallarına uygun olarak hazırlanan bu çalışmada başkalarının eserlerinden yararlanılması durumunda bilimsel kurallara uygun olarak atıf yapıldığını bildiririm.

Öğrencinin imzası (İmza)

T.C.
SELÇUK ÜNİVERSİTESİ
Eğitim Bilimleri Enstitüsü Müdürlüğü

YÜKSEK LİSANS TEZİ KABUL FORMU

	Adı Soyadı	Erdal LAFVERMEZ
	Numarası	16830501030
Öğrencinin	Ana Bilim / Bilim Dalı	Bilgisayar ve Öğretim Teknolojileri Eğitimi Bölümü
	Program	Tezli Yüksek Lisans ● Doktora O
	Tez Danışmanı	Prof.Dr. Ertuğrul USTA
	Tezin Adı	Lise Öğrencilerinin Siber Suç Algı Düzeylerinin Farklı Değişkenler Açısından İncelenmesi (Kırşehir İli Örneği)

Yukarıda adı geçen öğrenci tarafından hazırlanan Lise Öğrencilerinin Siber Suç Algı Düzeylerinin Farklı Değişkenler Açısından İncelenmesi (Kırşehir İli Örneği) başlıklı bu çalışma 07/12/2018 tarihinde yapılan savunma sınavı sonucunda oybirliği/oyçokluğu ile başarılı bulunarak, jürimiz tarafından yüksek lisans tezi olarak kabul edilmiştir.

Unvanı, Adı Soyadı	Danışman ve Üyeler	İmza
Prof.Dr. Ertuğrul USTA	Danışman	
Dr.Öğr. Üyesi Ağah Tuğrul KORUCU	Üye	
Dr.Öğr. Üyesi Uğur BAŞARMAK	Üye	

ÖNSÖZ VE TEŞEKKÜR

Teknoloji ve internetin gelişimi her geçen gün biraz daha artmaktadır. Bu gelişim beraberinde insan hayatına birçok yenilik katmakta, hayatı kolaylaştırmakta ve fayda sağlamaktadır. İnsan için birçok kolaylık sağlayan bu gelişim bir takım problemlerin de oluşmasına sebep olmaktadır. Bu problemlerin en başında da siber suçlar gelmektedir. Kişilerin internet ve teknolojiyi bilinçsiz olarak kullanmaları bu suçların ortaya çıkmasına neden olmaktadır. Özellikle genç kuşağın bu durumdan etkilendiği görülmektedir. Bundan dolayı, gençlerin siber suçlarla ilgili bilgi düzeyleri ölçülmeli ve bu suçlara karşı çözümler üretilmelidir. Bu nedenle bu çalışma lise öğrencilerinin farkındalık düzeylerinin belirlenmesi amacıyla gerçekleştirilmiştir. Bu araştırmanın yapılmasında birçok kişinin katkısı olmuştur.

Araştırma süresince görüş ve önerileriyle bana rehberlik eden ve hiçbir zaman yardımını esirgemeyen danışman hocam Prof.Dr. Ertuğrul USTA'ya, jüri üyeliğimi yapan değerli hocalarım Dr. Öğretim Üyesi Ağah Tuğrul KORUCU ve Dr. Öğretim Üyesi Uğur BAŞARMAK' a teşekkürlerimi sunarım.

Çalışmanın ilk gününden itibaren maddi manevi desteklerini benden esirgemeyen ve beni motive eden aileme teşekkürlerimi bir borç bilir şükranlarımı sunarım.

Ayrıca yoğun mesai saatleri arasında bana destek olan değerli çalışma arkadaşlarıma ve anketleri dolduran gençlerimize teşekkür ederim.

Erdal LAFVERMEZ

Konya, 2018

T.C.
SELÇUK ÜNİVERSİTESİ
Eğitim Bilimleri Enstitüsü Müdürlüğü

	Adı Soyadı	Erdal LAFVERMEZ
	Numarası	16830501030
Öğrencinin	Ana Bilim / Bilim Dalı	Bilgisayar ve Öğretim Teknolojileri Eğitimi Bölümü
	Program	Tezli Yüksek Lisans ● Doktora O
	Tez Danışmanı	Prof.Dr. Ertuğrul USTA
	Tezin Adı	Lise Öğrencilerinin Siber Suç Algı Düzeylerinin Farklı Değişkenler Açısından İncelenmesi (Kırşehir İli Örneği)

ÖZET

Günümüzde bilgisayarlar arası iletişim yolu ile işlenen suçlar giderek artmaktadır. Artan bu suçlara karşı ceza yasaları geliştirilmiştir. Toplumun ve gelecek nesilleri siber suç dünyasından korumak için toplumun siber suç algısı ve bilgisi artırılmalıdır. Bu kapsamda yapmış olduğumuz çalışmada lise öğrencilerinin siber suç algılarının demografik etmenlere göre değişimi incelenmiştir. Araştırma Kırşehir ilinde 2016-2017 eğitim-öğretim döneminde eğitim gören 898 lise öğrencisi ile yapılmıştır.

Araştırmada kullanılacak verileri elde etmek için daha önceden İLBAŞ (2009) tarafından hazırlanmış anket ve kişisel bilgileri içeren form kullanılmıştır. Bilişim suçunun suç bakımından değerlendirilmesi için demografik bilgiler içeren anket soruları kullanılmıştır. Ölçeklerden toplanan verilerin analizinde betimsel istatistikler, ikili gruplar arasındaki farklılıkları belirlemek için bağımsız örneklem T-Testi, ikiden fazla olan gruplar arasındaki farklılıkları belirlemek için de tek yönlü ANOVA Testi analizi kullanılmıştır.

Araştırma sonucunda lise öğrencilerinin en çok kişisel bilgilerin çalınması, çocuk pornografisi siteleri yayınlanması ve erişimi, banka hesap bilgilerinin ele

geçirilmesi suçları hakkında bilinçli olduklarını ve bu tür sorulara ağır suç olarak cevap verdikleri görülmüştür.

Anahtar Kelimeler
Siber suçlar, internet suçları, bilişim suçları, algı analizi, bilgisayar suçları

T.C.
SELÇUK ÜNİVERSİTESİ
Eğitim Bilimleri Enstitüsü Müdürlüğü

	Adı Soyadı	Erdal LAFVERMEZ
	Numarası	16830501030
Öğrencinin	Ana Bilim / Bilim Dalı	Bilgisayar ve Öğretim Teknolojileri Eğitimi Bölümü
	Program	Tezli Yüksek Lisans ● Doktora O
	Tez Danışmanı	Prof.Dr. Ertuğrul USTA
	Tezin İngilizce Adı	An Analysis Of High School Students' Perception Levels Of Cyber Crime According To Several Variables (A Sample From Kırşehir Province)

SUMMARY

In today's world, the crimes committed via intercomputeral communication are increasing day by day. In order to protect the society and the future generations from the world of cyber-crimes, the society's perception and awareness of cyber-crimes must be increased. In the study that we conducted in this content, we examined how the perception levels about cyber-crimes of high school students change according to demographic factors. The survey was conducted in Kırşehir province on 898 high school students who are studying in the term of 2016-2017.

In order to get the data to be used in the survey, the questionnaire that was prepared before by İLBAŞ (2009) and a personal information form prepared by the researcher were used. The questions in the questionnaire consist of two sections; demographic information and the evaluation of a group of cyber-crimes as 'crime'.

In the data analysis collected from the scales, descriptive statistics were used, to determine the differences between couple groups, independent sample t-test and in order to determine the differences between groups of more than a couple, one-sided

ANOVA test analysis were used.

It was concluded from the survey that high school students are mostly conscious of the crimes such as; processing of personal data, accessing to and broadcasting of child pornography sites, stolen bank accounts and that they see this kind of crimes as ‘severe crime’.

Keywords

Cyber-crimes, internet crimes, information crimes, perception analysis, computer crimes

KISALTMALAR DİZİNİ

ABD : Amerika Birleşik Devletleri
ARPANET : Advanced Research Projects Agency Network
ATM :Automated Teller Machine
BÖTE :Bilgisayar ve Öğretim Teknolojileri Eğitimi
BT :Bilgisayar Teknolojisi
CMK :Ceza Muhakemesi Kanunu
CD :Compact Disc
DDOS :Distributed Donial Of Service
EGM :Emniyet Genel Müdürlüğü
EİK :Elektronik İmza Kanunu
ENIAC :Electronic Numerical Integrator And Calculator
ETCK :Eski Türk Ceza Kanunu
FSEK :Fikir ve Sanat Eserleri Kanunu
HTTP :Hypertext Transfer Protocol
IP :İnternet Protokol
NATO :Kuzey Atlantik Antlaşması Örgütü
PIN :Personel Identification Number
SPAM :Spiced Park And Ham
SPSS :Sosyal Bilimler İçin İstatistik Programı
SSCB :Sovyet Sosyalist Cumhuriyetler Birliği
TCK :Türk Ceza Kanunu
TDK :Türk Dil Kurumu
TEF :Teknik Eğitim Fakültesi
TF :Teknoloji Fakültesi
UNIVAC :Universal Automic Computer
WWW :World Wide Web
YTCK :Yeni Türk Ceza Kanunu

İÇINDEKILER

BİRİNCİ BÖLÜM

1. GİRİŞ

1.1. Problem Durumu

Bilişim teknolojilerindeki gelişme, internetin yaygın olarak kullanımı ve insanlar üzerindeki etkisi yeni bir yaşam tarzı oluşturmaya başlamıştır. Yeni teknolojilerde olduğu gibi internetin insanlara sağladığı avantajlarının yanı sıra birçok dezavantajlı yanları da vardır. İnterneti kötü amaçları için kullanan kişilerin bulunması ve internet güvenliğinin yetersiz olması, siber suçların ortaya çıkmasına zemin hazırlamıştır. Bilişim teknolojilerindeki gelişme farklı suç ortamları oluşturduğundan günlük hayatta gerçekleştirilen birçok suç artık sanal âlemde gerçekleşmektedir. Böylece bilgisayar kavramı, insan hayatını kolaylaştıran bir araç olmaktan çıkmış, suçla anılan bir durum haline gelmiştir.

İnterneti haberleşme, bilgi toplama ve bilgi paylaşımı gibi iyi amaçlarla kullanan kişilere karşılık, kendini tatmin etmek isteyen, toplumda farklı olup kendine yer edinmek isteyen, macera ve güce sahip olmak gibi benlik oluşturan kişilerde vardır. Bireyleri suça sürüklemek kargaşa yaratmak amacıyla çeşitli sistemlerin açıklarını bulup bu sistemlere girerek kişi veya kurum/kuruluşlara zarar vermeğe çalışan programcılar veya bilgisayar ile uğraşan hackerlerin ortaya çıkması, teknolojiden nemalanarak terör örgütlerinin faaliyetlerini internet ortamına taşıması, hırsızlık ve dolandırıcılık gibi suçların internet ortamından yapılması, internette izinsiz yayınlanan film, müzik ve oyunların çoğalması vb. olayların cereyan etmesi, internetin kötü amaçla kullanılabileceğini ortaya koymuştur. İnsan hayatını kolaylaştırma adına kullanılan bilişim teknolojileri sağladığı yararın yanında güvenlik açısından da kaygılara neden olmuştur. Günümüzde artık fiziksel suçlar yerini sanal ortamlara bırakmıştır. Dolandırıcılık, hırsızlık gibi suçlar internet üzerinden yapılmaya başlanmıştır. Terör örgütleri gelişen teknoloji ile iletişim becerilerini artırmış, yeni faaliyet alanları bulmaya başlamışlardır (Turhan, 2006).

İnternetin dünya genelinde yaygınlaşması, alışveriş ve haberleşme imkânlarını artırması, ayrıca bilgisayar kullanıcıları arasında bağlantıyı sağlaması nedeniyle pek

çok resmi kurum ve kuruluşların bilgisayarı bu ağa bağlanmaktadır. Buna bağlı olarak da her türlü bilgi saklama ve kayıt işlemleri bilişim teknolojileri sayesinde gerçekleşmektedir. Her geçen gün bilgisayarlara olan ilginin artması bilişim teknolojilerinin insanlık için vazgeçilemez olmuş ve toplumun büyük bir kesimini bilgisayarlara bağımlı hâle getirmiştir. Dünya genelinde internet ve bilişimin çok hızlı bir şeklide yayılması insanlara sınırsız özgürlük alanı doğurmuş fakat aynı zaman da interneti suç işleme konusunda önemli bir kaynak haline getirmiştir. Bu sürecin sonucu olarak da hukuki ihlallerde, suçta artış görülmüş ve yeni suç alanlarının doğmasına neden olmuştur (Karagülmez, 2011; Alaca, 2008).

Yaşadığımız dönem bilgi çağı olarak adlandırılsa da bu çağda teknoloji hayatı kolaylaştırmış ancak beraberinde yeni sorunlarla birlikte yeni kavramlar getirmiştir. Bilişim kavramıyla birlikte bilişim suçları, diğer adıyla siber suçlar olarak tanımlanan yeni kavramlar için ülkeler değişik önlemler almış, ülkemizde de nispeten geç de olsa bu konuyla alakalı önlemler alınmıştır. Yeni bir kavram olan siber suçlar, yani bir diğer adıyla bilişim suçları gerek yasal düzenlemeler ve gerekse de uygulayıcılar bazında gerekli eğitim ve teşkilat yapılanmasında uzmanlaşmaya gidilmesi yoluyla sürmektedir.

Hızla gelişen teknoloji beraberinde oldukça üst düzey performans sağlayan bilgisayarları, fiber ağları, mobil telefonları, dijital verileri vb. hayatımıza sokmuş ancak bu durum da beraberinde çeşitli suçları getirmiş, alışık olduğumuz suçlara yeni bir boyut kazandırmıştır. Bu gelişmelere paralel olarak devletler de gerek kendileri ve gerekse de vatandaşlarını korumak adına birtakım yasal düzenlemeleri yapma gereği hissetmişlerdir. Sadece yasal düzenle yapmak yeterli olmayacak, gerekli yönetim sisteminin oluşturulması ve alanın da uzman personelinde yetiştirilmesi gereklidir (Özgan, 2012).

Günlük yaşantımızda iletişim, eğitim, arkadaşlıklar, ödemeler gibi farklı işler için kullanılan bilgisayar/internet ortamı, kullanıcıları mağdur etmekte, özel bilgi, belge kayıplarına yol açmakta ve beraberinde siber suça bulaşma ihtimallerini giderek artırmaktadır. Buna bağlı olarak siber suçlar toplumların önemli bir sorunu haline gelmiştir.

Bilişim ve internet teknolojisinin gelişimi, bilginin bu gelişmeler üzerinden takip edilmesi ve değerinin artması, kısa yoldan kendini kanıtlamak isteyen kişiler bu gelişmeyle suç işlemeye yönelmiştir. Buna bağlı olarak ta bilişim suçları ortaya çıkmıştır. Bilişim suçları artık kişilerin değil devletlerinde ortak bir sorunu haline gelmiştir.

Bu çalışma ile siber ve siber suç kavramı irdelenecek, siber suç kavramının Türk hukuk literatürüne girişi, Türk ceza kanunlarında yer alan siber suçlara değinilerek siber suçlar sınıflandırılacak, Kırşehir örneklemimizde lise öğrencilerine yönelik internet kullanım alışkanlıklarının tespiti, siber (bilişim) suça ilişkin görüşlerinin tespiti ve suç farkındalıkları ortaya konulacaktır.

Problem Cümlesi: Liselerdeki öğrencilerin siber suçlara karşı farkındalık düzeyleri nedir?

1.2. Alt Problemler

1) Lise öğrencilerinin siber suç konularına yönelik ilgileri hangi düzeydedir?
2) Lise öğrencilerinin siber suç konularına yönelik ilgileri;
    - Cinsiyete göre,
    - Sınıf değişkenine göre,
    - İnterneti kullanım yılına göre,
    - Sosyal medya hesabı kullanmaya göre istatistiksel açıdan önemli midir?

1.3. Araştırmanın Amacı

Teknolojide yaşanan hızlı nitelikteki değişim süreci neticesinde bilişim sistemleri de bu değişime ayak uydurmuştur. Sonrasında ise bu uyumdan istifade eden birtakım birey ve gruplar teknolojiyi gerek amaç ve gerekse de hedef olarak kullanmış ve sonuç itibariyle de siber suçlar adı verilen bu suçlar günümüzde modern toplumlarda önem arz eden problemlerden biri haline gelmiştir. Buna bağlı olarak bireylerin bilerek ya da bilmeyerek siber suça olan eğilimleri her geçen gün artmaktadır. Siber suçlar üzerine yapılan çalışmalara bakıldığında genellikle hukuki yaptırımlarına, siber suçlara yönelik devletlerin yaptığı çalışmalara değinilmiştir. Kişilerin bilişim suçlarına karşı farkındalıklarını artırmaya yönelik fazla çalışma olmadığı da görülmektedir. Bu araştırmada lise öğrencilerinin cinsiyet, sınıf, sosyal medya kullanımı ve internet kullanım yılına göre siber suçlar üzerine algıları arasında ilişki olup olmadığı araştırılmaya çalışılmıştır.

1.4. Araştırmanın Önemi

Ülkemizde ve dünyada siber suç olayları hızla artmaktadır. Gelişmiş bilgisayarların, akıllı cihazların hayatımıza girmesiyle önceden bilmediğimiz birçok suç türünü de beraberinde getirmiş olup bildiğimiz suç türleri de bu durumdan etkilenmiştir. Ülke olarak internet kullanımımız ve sanal âleme olan bağımlılığımız artmakta ve siber suçlara bulaşma riskimiz giderek büyümektedir. Buna bağlı olarak Türkiye'de siber suçlara yönelik çalışma faaliyetleri yürütülmeye başlanmıştır. Ancak internetin hızlı gelişimi teknolojiyle kıyaslandığında, bu faaliyetlerin az ve yetersiz kaldığı görülmektedir. Siber suçlarla mücadele noktasında özellikle genç kuşağın bilinçlendirilmesi yönünde adımlar atılmalıdır. İnternet kullanımının özellikle gençler arasında yaygın olması ve gençlerin kendini farklı gösterme çabası onları bilerek ya da bilmeyerek bilişim suçlarına karışmalarına neden olmaktadır. Bu noktadan hareketle gençlerin internet ve sosyal medya bağımlılığı, yapılan bilişim suçlarının neler olduğu, suçların hukuki yaptırımlarının ne gibi sonuçlar doğuracağı vb. konularda bilgilendirme çalışmalarının yapılması son derece önemlidir.

1.5. Sınırlılıklar

Araştırma lise öğrencilerinin siber suç algısı ve derecelendirmesi olarak sınırlandırılmıştır. Bu çalışma 2016-2017 eğitim-öğretim yılı Kırşehir ili merkezinde bulunan liselerde yapılmıştır. Kişisel bilgi formu olarak hazırlanan anket sorularından elde edilen cevaplar bu çalışmanın verilerini oluşturmaktadır.

1.6. Varsayımlar

Araştırma kapsamına göre öğrenciler, anket sorularını okuyup anlayarak cevaplamışlardır.

Bu suçlar hususunda öğrencilerin yeterli farkındalıklarının bulunduğu varsayılmıştır.

1.7. Tanımlar

Siber Suç: Bilgisayar ve ağları aracılığıyla hukuk dışı yöntemlerle siber uzayda yapılan eylemlerdir (Yazıcıoğlu, 1997).

Siber Suç Farkındalığı: Bu suç tipi hakkında insanların bilgi düzeyidir.

Siber Ortam: Bilgisayarlar ve bilişim sistemleri üzerinde bulunan, sonsuz ve kontrolü zor olan sanal âlemdir (Özpehlivan, 2006).

İKİNCİ BÖLÜM

2. KURAMSAL ÇERÇEVE

Tarih boyunca insana faydalı olmuş teknolojik yenilikler karşılaşılan sorunlara çözüm ve yaşam kolaylığı sağlamıştır. Sağladığı bu kolaylığın yanında farklı birçok yeni soruna da yol açmıştır. 20. yüzyılın ortalarında bilgisayar teknolojisi ve bilgisayarlar arası ağ ile iletişim artmıştır. Dünya çapında internet yayılımı ile insanlar arası iletişim çok gelişmiş ve günümüzde gündelik hayatımızın bir parçası haline gelmiştir. Bilgisayar teknolojisi ile veri girişi, veri saklama ve veri paylaşma işlemleri başlamıştır.

İlk zamanlarda yerel ve bölgesel bilgi paylaşımı ağ bağlantısı sağlanabilmiştir. Daha sonraları daha büyük bir ağ oluşturarak dünyadaki tüm bilgisayarları birbirine bağlayan bir yapı oluşturulmuştur.

İletişimin yanında eğitim, alışveriş, bankacılık işlemleri gibi birçok alanda var olan ihtiyaçlara cevap verilmiştir. İnternet kullanımının sağladığı yararlar olduğu gibi kötüye kullanımında vermiş olduğu zararlarda mevcuttur.

İnternet ve bilgisayar alanındaki bulunan tüm gelişmeler gibi bu alandaki suçlar da ilk defa Amerika'da meydana gelmiştir. Amerika'dan dünyaya yayılan bir suç dünyası da oluşmuştur. 1960'lara kadar uzanan siber suç tarihi 1980'lerde bilgisayarları kontrol edip bilgileri tamamen çalmaya yönelik illegal bir şekilde kullanılmıştır.

Günümüze kadar internet ağları vasıtası ile kötü niyetli kişiler veri çalma, sabote etme gibi birçok şekilde siber suç işlemiştir ve günümüzde de işlemeye devam edilmektedir. Ülkeler bu suçlar konusunda daha fazla önlem ve savunma yöntemleri oluşturması gerekmektedir.

2.1.SİBER SUÇ İLE İLGİLİ TANIMLAR

2.1.1. Bilişim Kavramı

Fransızca "informatique" diye bilinen bilişim « değişken bilgi « anlamına gelmektedir (Yenidünya ve Değirmenci, 2003). Fransa'da otomatik ve bilgi kelimelerinin birleşik halde kullanılmasıyla meydana gelen "informatique" otomatik bilgi diye tanımlanabilir. Türkçe 'ye zaman içerisinde enformasyon şeklinde geçmiştir. Türk Dil Kurum' unun tanımına göre ise; insanların bilimsel veya iletişim için ihtiyacı olan bilgilerin elektronik araçlar aracılığıyla makul bir şekilde işlenmesidir (Nacar, 2010).

Bilişim alanı, verilerin belli bir yerde depolanması, istenildiği esnada erişilebilmesi ve dağıtımının yapılabilmesi fonksiyonlarını gerçekleştiren alandır. Bu alanı sadece bir bilgisayar şeklinde de düşünebileceğimiz gibi bilgisayarların tümüyle toplu bir şekilde bağlı oldukları bir ağ biçiminde de düşünebiliriz (Akıncı, Alıç ve Er, 2004).

2.1.2. Bilgisayar

İçerisine yüklenen programları kullanarak aritmetiksel ve mantıksal işlemler yapmaya yarayan cihazlara bilgisayar ismi verilmiştir. Bilgisayarın üretilme tarihi 1940'lara kadar dayanmaktadır. 1940'lı yıllarda ilk üretilen bilgisayarın boyutu bina büyüklüğü diye tabir edilebilir. Daha sonra 1946'da Amerika'da ordu tarafından üretilen bilgisayar ise ENIAC'tır (Hennessy ve Patterson, 2007). İlk defa ticari amaçlı bilgisayar ise 1951 yılında üretilmiştir. Ticari amaçlı bu bilgisayara UNIVAC ismi verilmiştir (Yazıcıoğlu, 1997). İşlevleri hakkında genel bilgi vermek gerekirse verileri depolamak, verileri sınıflandırmak, yüklenen programlara göre verilen emirleri yerine getirmek denilebilir.

İki ana eleman kategorisinden meydana gelen bilgisayarlar somut olarak görülebilen donanım ve soyut olarak kodlar yardımı ile oluşturulmuş yazılımlar sayesinde işlevlerini yerine getirmektedirler (Topaloğlu, 1997).

2.1.3. İnternet

Dünyada bulunan bilgisayarların birbirleri ile bağlantı kurması ve bu bağlantı sayesinde dünyadaki insanların iletişimini gerçekleştirmesi internet sayesinde olmuştur. Yine Amerikan ordusu tarafından bulunan Arpanet ilk bilgisayarlar arası bağlantıdır. Arpanet ağı 1950'lerden 1990'lara kadar kullanılmıştır. 1990'larda WWW teknolojisi ile Arpanet kullanılmaya son verilmiştir. İnternete bağlanabilmek ve iletişim için HTTP diye bilinen uluslararası bir sistem vardır. Aynı şekilde internette bulunan her sitenin çalıştığı bilgisayarların ip adresi bulunmaktadır. Herhangi bir siteye girmemiz için oluşturulan sağlayıcılar vardır. Bunlar; içerik, erişim ve servis sağlayıcılarıdır.

2.1.4. Bilişim Suçu

Avrupa'da genel olarak Ciber Crime diye bilinen suçlar Türkiye'de internet suçu, sosyal medya suçu, bilgisayar suçu, teknoloji suçu gibi farklı farklı isimlendirilmektedir. Az kullanılmakla birlikte bilişim suçu da denilmektedir. Avrupa Ekonomik Topluğu Uzmanlar Komisyonunu tarafından bilişim suçları tanımı; bilgilerin otomatik olarak işlendiği ya da verilerin transferini sağlayan bir sistemde kanuna ve ahlaki değerlere aykırı ya da yetkisiz olarak yapılan bütün davranışlardır (Durmaz, 2006). Bilişim suçları ikiye ayrılır: Birincisi bilişim alanındaki teknolojileri kullanarak işlenen suçlar. İkincisi ise bilişim alanını sabote ederek bilgi çalma veya bilgi yok etme, tehdit, müstehcenlik, cinsel istismar, intihara yönlendirme gibi suçların hepsi bilişim suçudur.

2.1.5. Siber Kavramı

Siber İngilizce "Cyber" kelimesinden Türkçeye geçmiştir. Türkçede genel olarak siber ve bilişim sözcükleri eş anlamlı gibi kullanılır. Bu kelimeler eş anlamlı olarak kullanılsa da arada fark bulunmaktadır (Çakmak ve Demir, 2009). Peker'e göre; "Siber, bilgisayar ve buna bağlı elektronik sistemlerin bulunduğu ortam; bilişim ise bu ortamdan etkin olarak faydalanma ve bu ortam aracılığıyla bilgi üretilmesidir."

2.1.6. Siber Suç

İnternet suçu, sanal suç, bilgisayar suçu, diye isimlendirilebilir. Siber suç terimi bu suç tiplerinin tümünü kapsayan bir niteliktedir (Yazıcıoğlu, 2002). Uluslararası literatürde "ciber crime" bildiğimiz adıyla "siber suç" terimi kullanılır. Bu çalışmada bilişim suçları ile aynı manayı taşıyan siber suçlar, bilgisayar suçları, bilişim sitemlerini hedef olarak alan suçlar, bilişim sistemleri vasıtasıyla işlenen suçlar, İnternet suçları ve bilgisayara bağlı elektronik sistemlerde gerçekleşen suçlardan oluşmaktadır. Ülkemizde siber suçlar aşağıdaki gibi nitelendirilmiştir;

- Elektronik ortamda verilen sertifikalarda yapılan sahtekârlık[1]
- Haberleşmenin engellenmesi[2]
- Bilgisayar koruma programlarını etkisizleştirmeye yönelik eylemler[3]
- İntihara yönlendirme[4]
- Hakaret[5]
- Çocukları cinsel istismarı[6]
- Cinsel taciz [7]
- Şantaj[8]
- Fuhuş[9]
- Haberleşmenin gizliliğini ihlali[10]

---

[1] EİK Madde 17
[2] TCK madde 124
[3] FSEK madde 72
[4] TCK madde 84
[5] TCK madde 125
[6] TCK madde 103
[7] TCK madde 105
[8] TCK madde 107
[9] TCK madde 227
[10] TCK madde 132

- İmza oluşturma verilerine habersiz ulaşım[11]
- Kişisel verileri kaydedilmesi[12]
- Hukuki olmayan yollardan verileri elde etme[13]
- Tehdit[14]
- Özel hayatın gizliliğini ihlal[15]
- Nitelikli dolandırıcılık[16]
- Kişiler arasındaki konuşmaların dinlenmesi ve kayda alınması[17]
- Nitelikli hırsızlık[18]
- Müstehcenlik[19]
- Kumar oynanması için yer ve imkân sağlama[20]
- Maddi-manevi haklara tecavüz[21]

Öncelikle siber suç kavramının ne olduğunu açıklamadan, bu suça neden internet suçu değil de siber suç denildiğini açıklamada fayda vardır. Uzay ve internet kavramlarıyla anlamdaş olarak yaygın bir şekilde kullanılan siber kavramı, aslında aynı anlamı ifade etmezler. Siber uzay kavramı, yalnızca İnternet'i değil, intranet sayesinde bütün ağları kapsamaktadır. Yani şöyle açıklamakta fayda vardır; suç intranet ortamında işlense bile siber uzayda işlendiği kabul edilir fakat suç internet suçu olarak kabul edilmez. Bu sebepten ötürü siber suç, internet suçunu da içine alan

[11] EİK madde 16
[12] TCK madde 135
[13] TCK madde 136
[14] TCK madde 106
[15] TCK madde 134
[16] TCK madde 158
[17] TCK madde 133
[18] TCK madde 142
[19] TCK madde 226
[20] TCK madde 228
[21] FSEK madde 71

geniş bir kavramdır. Özetlemek gerekirse; İnternet'te işlenmiş her suç bir siber suç olmakla birlikte, her siber suç bir İnternet suçu değildir (Sınar, 2001:69). Ancak çoğu siber suç, internet aracılığıyla işlenmektedir. İnternetin diğer suç argümanlarından insanlar tarafından daha fazla kullanılması bu durumun nedenini oluşturmaktadır.

2.2.SİBER SUÇLARIN TARİHÇESİ

İlk bilgisayar ve internetin Amerika'da bulunması ve kullanılması sebebi ile ilk siber suç yine Amerika'da işlenmiştir. Bir bilgisayar uzmanı banka hesaplarında kayıtlara geçmiştir (Aydın, 1992). İlk suçun işlendiği Amerika'da giderek siber suçlar artmış ve bu noktada güvenlik önlemleri almak ve suçları durdurmak için 1995 yılı itibari ile siber savaş komutanı diye adlandırılan devlet görevlileri yetiştirilmiştir. Daha sonraları suçların paralel olarak artması ile bu görevliler bir komutanlık altında toplanmış ve siber savaş komutanlığı isimli birim oluşturulmuştur (Yayla, 2013). Dünyaya yayılan siber suç çeteleri tüm dünya ülkelerini önlem almak için aynı paydada buluşturmuş ve uluslararası sözleşmeler imzalanmıştır. Bu sözleşmelere örnek 2001 yılında Avrupa Konseyi'nin hazırladığı "Avrupa Siber Suç Sözleşmesi" dir. 2007 yılında ise "NATO Siber Savunma Politikası" ile siber suçların gündemde kalması amaçlanmıştır (Yayla, 2013). Ülkemizde ise önlemler TCK'da eklenen ve değişen maddeler ile alınmaya başlanmıştır. 1991, 1995, 2004, 2007 ve 2008 yıllarında çıkan ve eklenen kanun maddeleri siber suçlar ile mücadele için atılan adımlardır.

2.3.SİBER SUÇLARIN SINIFLANDIRILMASI

Bu suç türünün insan yaşamına girmesi ve kişileri olumsuz etkilemesi nedeniyle, bu suçları farklı şekilde sınıflandırma ihtiyacı gerekmiştir. Kanun koyucuların Ceza Hukukunda yer alan "kanunsuz suç ve ceza olmaz" ilkesini dikkate alarak bilişim suçları için gerekli düzenlemeleri yapmaları zorunluluğu ifade edilmiştir.

Fakat teknolojik gelişmelere paralel olarak internet dünyasının da hızlı bir şekilde gelişim göstermesi ve daha çok insanın kullanması yeni ihlalleri de

beraberinde getirmektedir. Bundan dolayı siber suçları sınıflandırma çalışmaları farklılaşmaktadır.

Görüldüğü şekliyle siber suç ile alakalı tanımlarda herkesçe benimsenen ortak bir tanım yoktur. Bu konuyla ilgilenen uzman kişilerin birtakımı bu suçları gruplara ayırarak sınıflandırmaya tabi tutmayı gerekli görmemekte, bazı uzmanlar ise bu suçları ana başlıklar halinde ele almaktadır.

Bu hususta McConnel International isimli ABD küresel teknoloji ve politika yönetimi danışmanlık firmasının yaptığı sınıflandırma öne çıkmaktadır. Bu firmanın yapmış olduğu sınıflandırmaya göre siber suçlar dört başlık altında toplanmaktadır. Yapılan bu çalışma ise, bu dört başlığa diğer suçlar başlığı da eklenerek toplam beş başlıkta altında yapılmıştır.

2.3.1. Veri Suçları

Bu suç türü toplam üç başlıkta incelenecektir.

2.3.1.1.Verilerle Mücadele Edilmesi

Bu suç türü, siber uzayda veriler transfer edilirken üçüncü şahısların transferi engellemesi, yolunu değiştirmesi veya ele geçirmesi şeklinde karşımıza çıkmaktadır.

2.3.1.2.Verilerin Değiştirilmesi

Verilerin muhafaza edildiği ortamda ya da iletildiği anda değiştirilmesi, kısmen ya da bütünüyle ortadan kaldırılması bu suçu meydana getirmektedir. Buradan çıkan bir sonuçta şudur; verilerin transfer sırasında değiştirilebilir, bozulabilir ya da silinebilir olmasıdır. Bu durum iki değişik suçu meydana getirmektedir ve bu suçlar birleştirilip tek bir kusur bulunur.

2.3.1.3.Veri Hırsızlığı

Verilerin çalınması suretiyle veri sahibi olan kişinin aleyhine kullanılması ya da çalınan bu verileri çalan kişinin kendi menfaatine veya başka bir kişinin menfaatine kullanarak haksız nitelikte bir kazanç sağladığı bir durum olarak karşımıza gelir.

2.3.2. Ağ Suçları

Bilgilerin bir ortamdan başka bir ortana aktarımına olanak tanıyan sistem ağ sistemi olup bu alanda ki suçlar iki şekilde karşımıza çıkmaktadır.

2.3.2.1.Ağ Engellenmesi

Ağın tamamının ya da bir kısmının erişiminin kapatılmasıdır. Bu suç türünde en fazla karşılaşılan durum web siteleri ve İSS üzerinden engelleyici verilerin gönderilmesi suretiyle erişimin engellenmesidir. Bu durumDistributed Denial Of Service (DDOS) saldırıları olarak adlandırılır. DDOS' lar, hacklenen bilgisayarların yönlendirildiği sistemlere erişiminin engellenmesidir.

2.3.2.2.Ağ Sabotajı

Ağın ya da ilgili sistemlerin mekaniksel ve elektromanyetik olarak kullanılamaz hale getirilmesidir.

2.3.3. Yetkisiz Erişim Suçları

Yetkisi olmayan kişilerin bir bilgisayarın sistem ya da ağına girmesidir. İletişimin nasıl olduğu mühim değildir. Yetkisiz erişim yakın ya da uzak mesafelerden olabilmektedir.

2.3.3.1. Yetkisiz Dinleme

Yetkisi olmayan şahısların ilgili sistemleri kullanarak sistem içinde yaptıkları teknik dinlemelerdir. Her türlü bilgisayar iletişimi suçun temel hedefidir. Topluma açık veya da özel iletişim sistemlerinde yapılan veri hareketlerinin dinlenmesi ve takip edilmesi işlemleridir.

Bu işlemin suç unsuru oluşturması için yapılan dinleme ve takiplerin yetkisiz ve kasten olması gerekmektedir.

2.3.3.2. Virüs Yayılması

Bilgisayarlara ağ sistemini kullanarak veya disketler ve CD kullanımı ile zarar verme amaçlı yapılan eylemlerdir.

2.3.4. Bilgisayarlarla İlgili Suçlar

2.3.4.1. Bilgisayarlarla İlgili Sahtekârlıklar

Kanuna aykırı bir şekilde, kendine ya da başka birisine maddi fayda sağlamak ve kişinin zarara uğramasına sebep olmak için, bilgisayar üzerinden sahte belge (banka kartı, banknot, çek vs.) meydana getirmek ya da elektronik ortamda bulunan dokümanlarda değişiklikler yapmaktır. Dijital ortamlardaki belgeleri değiştirmek bir çeşit sahtekârlık olup, değiştirilen bu belgeler insanlarda yanlış kanaatler oluşturulabilmektedir.

2.3.4.2. Hesap İhlali

Kişinin başka bir kişiye ait hesabını bilgisayar sistemlerinden erişerek herhangi bir ödeme yapmaktan kaçınıp hesabını kanunlara aykırı bir biçimde kullanması durumudur. Ayrıca, bir şahsın başkasına ait internet, telefon ya da benzer bir sistemdeki hesabını haberi olmadan rızası dışında kullanması olarak ta açıklanabilir.

2.3.4.3. Bilgisayar Sabotajı

2.3.4.3.1. Mantıksal Bilgisayar Sabotajı

Bir iletişim yahut bilgisayar sisteminin fonksiyonlarını engellemek için bilgisayar programları ya da verilerinin sisteme girilmesi, değiştirilmesi veya silinmesidir. Programların ya da verilerin “zaman bombası”, “truva atları”, “virüsler”, “solucanlar” adı verilen ve günümüzde sıkça kullanılan yazılımlar vasıtasıyla değiştirilmesi, silinmesi veya çalışmaz vaziyete getirilmesidir.

2.3.4.3.2. Fiziksel Bilgisayar Sabotajı

Bir iletişim sistemine veya bilgisayarı oluşturan unsurlara, işlevlerini yapamamasına sebep olacak şekilde fiziksel olarak zarar verilmesidir.

2.3.4.4. Banka Kartı Dolandırıcılığı

Ödemelerin kartlı sistemler kullanılarak yapıldığı hırsızlık ve dolandırıcılık suçlarıdır.

Bu dolandırıcılık suçları, bankamatik kartları, kredi kartları gibi kartlar

üzerinden yapılmaktadır. Kartlı ödeme sistemleri (ATM-Automated Teller Machine) bankalar tarafından kullanılmakta olup kart sahiplerinin erişim sağlaması için kişi tanımlama numarası (PIN-Personel Identification Number) gerektirmektedir. Dolandırıcılar bu kartları çalarak, kopyalayarak ya da kart sahiplerinin iletişim hatlarını engelleyip dinleyerek bilgileri çalma yoluyla suç işlemektedirler.

2.3.4.5. Girdi/Çıktı/Program Hileleri

İlgili sistemlere kasıtlı olarak doğru olmayan verileri yüklemek, sistemden doğru olmayan çıktıları almak veya sistem üzerindeki programları değiştirerek suç işlemektir.

Özellikle bilgisayarı veri tabanlarına doğru olmayan verileri yüklemek çok kullanılan bir dolandırıcılık türüdür. Bu nedenle bu tür davalar incelenirken sistemdeki yazılım programların tümünü kapsayacak bir teknik tanımlama gerekmektedir.

2.3.4.6. İletişim Servislerini Yetkisiz ve Haksız Olarak Kullanma

Şahısların kendileri için ya da bir başkası için fayda sağlamak amacıyla iletişim sistemlerindeki açıklardan yararlanarak iletişim servislerini ya da diğer bilgisayar destekli sistemleri hukuksuz olarak kullanmalarıdır.

2.3.4.6.1. Lisans Sözleşmesine Aykırı Kullanma

Yazılımlar genelde bir bilgisayarda lisanslı kullanmak için tasarlanmaktadır. Tek bir bilgisayarda kullanmak amacıyla alınan lisanslı bir yazılımın daha fazla bilgisayarda kullanılma ve kopyalanması yasaktır. Bu kapsamda buna aykırı bir eylem yapılması suçtur.

2.3.4.6.2. Lisans Haklarına Ters Çoğaltma

Lisans anlaşması ile korunan bir yazılımın bir ortamdan başka bir ortama kanunsuz olarak kopyalanmasıdır. Daha net bir ifadeyle ödeme yapmaktan kaçınmak için önceden satın alınana ya da kopyalanan bir yazılımın başka bir dijital ortama taşınmasıdır.

Bu işlemi yapan ve kopyalanmasına müsaade edende lisans sözleşmesini ihlal etmiş olur. Günümüzde farklı ortamlarda satılan film, program ve oyun CD'lerinin bu şekilde çoğaltıldığı ve bandrol bulundurmadığı görülmektedir.

2.3.4.6.3. Lisans Haklarına Aykırı Kiralama

Lisans haklarına aykırı olarak oyun, film ve yazılımların kiralanmasıdır. Söz konusu suçta daha çok oyun CD'si ve filmlerin kiralandığı görülmektedir.

2.3.5. Diğer Suçlar

2.3.5.1. Kişisel Verilerin Suiistimali

Devlet kurumları, banka, hastane gibi kişisel bilgilerin bulunduğu kurumlarda kişilerin rızası olmaksızın menfaat sağlamak veya başkasının zararına bu verilerin kullanılmasıdır.

2.3.5.2. Kişilik Taklidi ve Sahte Kişilik Oluşturma

Çıkar amacıyla gerçek şahısların taklidinin yapılması veya olmayan kişiler oluşturulması eylemidir

Burada gerçek kişinin bilgileri kullanılarak faaliyetler yapılmakta ve aksi bir durumda suçun gerçek şahsın üzerine kalması söz konusudur. Diğer taraftan çeşitli programlar kullanılarak elde edilen gerçek bilgiler yoluyla hayali şahıslar oluşturarak çıkar sağlanmaya çalışılmaktadır.

2.3.5.3. Yasadışı Yayınlar

Bilgisayar sistem ve ağlarının yasadışı unsurların yayınlanması ve dağıtılması da kullanılmasıdır.

Kanunun yasakladığı tüm materyal, elektronik postalar, web siteleri, haber portalları gibi verileri saklayacak şekilde kayıt yapan argümanlar kullanılması suretiyle saklanması, dağıtılması ve yayınlamasıdır.

2.3.5.4. Terörist Faaliyetler

İletişim, propaganda ve suç işleme amaçlı kötü niyetli terör örgütleri bilişim ağlarını kullanmaktadır (Atıcı ve Gümüş, 2003). Terör örgütleri internet ağını kullanırken yakalanmamak için genellikle internet kafeleri tercih etmektedir (Zarplı, 2008).

2.3.5.5. Çocuk Pornografisi

15 yaşından küçük çocukların pornografik resimlerinin internet yolu ile dağıtılması yayınlanması paylaşılması siber suçlarda çocuk pornografisi diye bilinir (Bilek, 2012). Bu tür suçları işleyen insanların ve örgütlerin yakalanıp yargı önüne çıkarılması çocuklarımızı korumak adına çok önemlidir.

2.3.5.6. Satılması Yasak Ürünlerin Ticareti

Normal ticarette satışı yasak olan şeylerin internet üzerinden bir şekilde satılmaya çalışılması suçtur. Buna örnek vermek gerekirse; kadın ticareti, uyuşturucu ticareti, silah ticareti sayılabilir.

2.3.5.6.1. Kadın Ticareti

Videolu görüşmelerinde gerçekleştirilebildiği çağımızda fuhuş yaptırılan kadınların internet yolu ile pazarlandığı görülmektedir. İnternet üzerindeki bu fuhuş ticareti yaygın bir siber suç tur.

2.3.5.6.2. Çocuk Ticareti

Çocukların ve ailelerinin kandırılarak kaçırılması daha sonra dilendirilme, organlarının satılması gibi suçlar çocuğa ve ailesine bilişim ağları yolu ile ulaşarak meydana gelmektedir. Bu tip suçlar 3. Sınıf ülkelerde daha çok görülmektedir.

2.3.5.6.3. Organ Ticareti

Fakir insanların zor durumunu kullanarak, organ nakli bekleyen insanlara aracılık edip internet üzerinden organ ticareti yapılmaktadır. Bazı siteler ve internet sayfalarında bu tip pazarlıklar ilanlar bulunmaktadır.

2.3.5.6.4. Uyuşturucu Ticareti

Toplumun ve geleceğin en büyük düşmanı olan uyuşturucu maddelerin tanıtımı ve dağıtımının sanal ortamda yapılmasıdır. Uyuşturucu satıcıları ve kullanıcılarının birbirlerine ulaşmak için internet üzerinden iletişime geçtikleri bilinmektedir.

2.3.5.6.5. Silah Ticareti

Normal var olan yollarla silah alındığında gerekli evraklar ve kayıtlar oluşturulmaktadır. Fakat sanal ortamda silah satışı yapıldığında devletin herhangi bir kayıt veya belge tutma imkânı olmamaktadır. Bu şekilde kayıtsız bir durum yani suç teşkil etmektedir.

2.4. SİBER SUÇLARIN İŞLENİŞ ŞEKİLLERİ

Bilişim konusunda yeteneklerini ve bilgilerini geliştiren insanlar kötü niyetlerini bilişim ağları üzerinde birçok işlem yaparak gerçekleştirmeye çalışmaktadır. Suçları işleyiş şekilleri farklı farklı olmaktadır.

2.4.1. Bilişim Korsanlığı

Yetkisi olmayan bir bilişim ağına ulaşarak ağda bulunan verilerin silinmesi, çalınması, değiştirilmesi gibi işlemlerin yapılmasına bilişim korsanlığı denilmektedir. Bu tür suçları işleyen kişilere hacker denilir. Hackerler genel olarak bilişim sektöründe çalışan insanlardan meydana gelmektedir. Son zamanlarda gençler bunu zevk amaçlı yapabilmektedir. Okulunun verilerini değiştiren öğrenciler olmuştur. Zıt görüşlü kişiler ve topluluklarda sürekli olarak bu tür suçlar işlemektedir. Hacker yetkisi olmayan bilişim ağına bir şekilde bağlanarak veri değişimi, veri yok edilmesi, vs. işlemlerini yaptıktan sonra çıkarken ardında iz bırakmayacak şekilde hareket etmektedir. Çoğu hacker bulunamamaktadır.

2.4.2. Gizli Kapılar

Bilişim ağının sistemini kuran veya yazılımını yazan kişiler sistemin bir noktasında açık kapı bırakmaktadır. Gerektiği takdirde bu açık kapıdan sisteme girip işlem yapabilmek amaçlı yaptıkları bu açık kapı hackerler tarafından bulunduğunda kötü niyetli olarak kullanılmaktadır.

2.4.3. Ağ Solucanları

Ağlara bir şekilde girdikten sonra ağın her yerine yayılabilen ve iz bırakmayan virüs benzeri bir yapıdır. Sisteme girer ve kendi kendine iz bırakmadan hareket ederek sistemin hepsini ele geçirebilir. Genel olarak mail yolu ile yapılır.

2.4.4. Truva Atı

Sistem kullanıcısı tarafından fark edilmeyecek şekilde oluşturulmuş yararlı sanılan fakat asıl yazılımcı tarafından bilgisayara müdahale edilmesini kolaylaştırır. Kullanıcı tarafından internetten indirilen herhangi bir programın içine gizlenen dosya şeklinde olabilir. Yazılımcısı tarafından verileri değiştirme, silme, şifreleri kopyalama işlemleri yapılabilir. Bilgisayarda çoğalmadığı için solucanlardan farklıdır.

2.4.5. Salam Tekniği

Banka sistemlerindeki artan veyahut hissedilmeyecek çok küçük miktarları başka hesapta toplayan Truva atı kullanılan tekniktir (Alaca, 2008).

2.4.6. İstem Dışı Elektronik Postalar (Spam)

Farklı yollarla bulunan mail adreslerine sürekli olarak ve yoğun şekilde mail gönderen bir işlemdir. Mail içeriği rahatsız edici yasadışı olduğu veya çok fazla gelip sistemi duracak aşamaya getirirse buna işlem yapılmaktadır (Kurt, 2005).

2.4.7. Çöpe Dalma

Çöp kutusundan geri dönüşüm sağlayan üst düzey sistemlerdir. Kalan artık verileri toplayarak veri çalma işlemi yapmaktır (Yazıcıoğlu, 1997).

2.4.8. Tarama

Aranan bilgisayarın bulunması için yapılan ip tarama işlemidir (Kurt, 2005).

2.4.9. Oltaya Gelme

İnternet sitelerinin kopyalarını yaparak siteye üye olanların giriş yapması ile bilgilerini çalmak ya da sahte mail yolu ile şifre benzeri bilgileri çalmak denilebilir.

Kişi sahte olana girdiği için oltaya gelme denilir (Akarslan, 2012).

2.5. SİBER SUÇLARIN TÜRK CEZA KANUNUNDA YERİ

2.5.1. Siber Suçların Türk Hukuk Sisteminde Yer Alması ve Düzenlenen Suç Fiillerinin Bölümlere Ayrılması

Kişisel bilgisayarların kullanımı 80'li yıllarla başlaması ve Dünya'da hızlı bir şekilde artması, 90'lı yıllarda da bilgisayarların birbirine bağlanması suretiyle veri aktarımının sağlanmasına başlanılmasıyla ülkemizde bilgisayar kullanımı önemli ölçüde yaygınlaşmıştır.

Dünya genelinde bilgisayar ve bilgisayar ağlarının kullanımının artması beraberinde birtakım hukuki problemleri de beraberinde getirmiştir ve bu durum sonucunda da gelişmiş ülkeler bu konuda işlenen suçları cezasız bırakmamak amacıyla bir dizi mevzuat çalışmaları başlatmıştır. Dünya'da ki bu gelişmelere paralel olarak ülkemizde de kanun koyucular siber suçlara karşı harekete geçmişler ve birtakım düzenlemelerin yapılması ihtiyacı doğmuştur.

6.6.1991 tarihinde yayımlanan 3756 sayılı Kanunun 20'nci maddesiyle TCK'nın 765 sayılı ikinci kitabına "Bilişim Alanında Suçlar" ismiyle 525/a, 525/b, 525/c ve 525/d maddelerinden meydana gelen bir babın eklenmesi Türk hukukunda siber suçlara dair ilk düzenlemedir. Bu düzenlemedeki suçlar, hemen hemen hiç bir değişikliğe uğramadan 1989 tarihli Türk Ceza Kanunu Tasarısından alınmıştır.

Kanun koyucu TCK'da ihtiyaca binaen değişiklikler yapılmış kapsam genişletilmiştir. Bu kapsamda "Herhangi bir şekilde dil ve yazı ile ifade olunan eserler ve her biçim altında ifade edilen bilgisayar programları ve bir sonraki aşamada program sonucu[22] doğurması koşuluyla bunların hazırlık tasarımları" da eser olarak kabul edilmiş ve bu kanun kapsamında bilgisayar programları açısından bu tip faaliyetler suç sayılmıştır[23].

Elektronik İmza 15.01.2004 tarih ve 5070 sayılı Elektronik İmza Kanunu ile

[22] Tasarının bazı kısımları hazırlanırken Fransız Ceza Kanunu Tasarısından yararlanılmıştır (1.3.1993 tarihinde).

[23] 3.3.2004 tarih ve 5101 sayılı Kanunla, 5846 sayılı Kanun'da siber suçlarla ilgili değişiklikler olmuştur.

yasalaşmış ve bu kanunla sahte elektronik sertifika uyarlanması ve kullanılması suç olarak belirtilmiştir.

2.5.1.1 Siber Suçlarla İlgili Düzenlemenin 5237 Sayılı Yeni Türk Ceza Kanununda Sınıflandırılması

Siber suçlara dair yapılan düzenlemeler 5237 sayılı Yeni Türk Ceza Kanun'unda, genel manada 765 sayılı Türk Ceza Kanun' unda mevcut düzenlemelere benzer bir biçimde, ama daha geniş çerçevede "özel hayatın gizli alanına karşı suçlar" ve "bilişim sistemlerine karşı suçlar" kısımlarında toplanmıştır. Bunlarla beraber 5237 sayılı Yeni Türk Ceza Kanun'unun bazı bölümlerinde bilişim sistemleriyle işlenmesi mümkün olan suçlar da mevcut bulunmaktadır. Buna göre 5237 sayılı Yeni Türk Ceza Kanun'unda siber suç olarak sınıflandırılacak suç türlerinin yanında bilgisayarlar üzerinden işlenen fakat yalnızca siber suç kapsamında olmayan suç çeşitleri de mevcut bulunmaktadır (Dülger, 2004:114).

Bilişim alanındaki suçlar bölümünde, "bilişim sistemine hukuka aykırı olarak girme ve sistemde kalma suçu"[24] (m.243), "sistemi engelleme, bozma, verileri yok etme veya değiştirme" (m.244), " banka veya kredi kartlarının kötüye kullanılması" (m.245) ve "tüzel kişiler hakkında güvenlik tedbiri uygulanması" hususları (m.246) düzenlenmiştir.

(m. 135) "Kişisel verilerin kaydedilmesi"; (m.136) "kişisel verileri hukuka aykırı olarak verme veya ele geçirme" ve (m.138) "bilgilerin ortadan kaybedilmesi" suçları, özel yaşamın gizliliği ile ilgili suçlar kısmında yer verilen suçlardır.

Son olarak, 5237 sayılı Türk Ceza Kanunu'nun bazı kısımlarında siber suçları içeren suç tipleri de bulunmaktadır. Bu suçlar; (m. 132) "haberleşmenin gizliliğini ihlal suçu", (m. 124) "haberleşmenin engellenmesi suçu", (m. 125) "hakaret suçu", (m. 142 fkr.2 b. "e") "bilişim sisteminin kullanılması yoluyla işlenen hırsızlık suçu", (m. 158 fkr.1 b. "f") "bilişim sisteminin kullanılması yoluyla işlenen dolandırıcılık suçu" ve (m.226) "müstehcenlik suçu" dur.

---

[24] 243'üncü madde, eski TCK da yer almayan bir suç hali saymaktadır.

765 sayılı Türk Ceza Kanun'unda yer alan siber suçlarla Yeni Türk Ceza Kanun'unda düzenlenen siber suçlar yukarıda sade bir şekilde anlatılmıştır. Yeni Türk Ceza Kanun'unun 243'üncü maddesinde bulunan "bilişim sistemine hukuka aykırı olarak girme ve sistemde kalma suçu" 765 sayılı Türk Ceza Kanun'unda mevcut olmayan yeni bir suçtur. Ayrıca Yeni Türk Ceza Kanun'unda bulunan (m.135) "kişisel verilerin kaydedilmesi"; (m.136) "kişisel verileri hukuka aykırı olarak verme veya ele geçirme"; (m.245) "banka veya kredi kartlarının kötüye kullanılması"; (m. 142 fkr.2 b. "e") "bilişim sisteminin kullanılması yoluyla işlenen hırsızlık" ve (m.158 fkr.1 b. "f") "bilişim sisteminin kullanılması yoluyla işlenen dolandırıcılık " suçları, 765 sayılı Türk Ceza Kanun'undan farklı olarak düzenlenmişlerdir.

765 sayılı Türk Ceza Kanun'unun 525 a/2 bendinde yer alan suç fiiline dair yapılan tenkitler göz önünde bulundurularak Yeni Türk Ceza Kanun'unda bu mevcut değildir. Verilerin ele geçirilmesinin suç unsuru olarak sayılması, YTCK ile getirilen başka bir yeniliktir. Bu yeni düzenlemeye göre hukuka aykırı bir şekilde bilişim sistemine girilmesi durumu, suçun meydana gelebilmesi için yeterli bir faktör olarak sayılmıştır.

2.5.1.2. YTCK'nın 243'üncü Maddesince Bilişim Sistemine Girmek ve Orada Kalmaya Devam Etmek Suçu

Başlıkta ifade edilen suç türü yeni bir düzenleme ile kanun koyucu tarafından bir suç olarak kabul edilmiştir. Bu suçun kanun koyucu tarafından düzenlenmesinin sebeplerinden biri de, Avrupa Konseyinin kabul ettiği Siber Suçlar Sözleşmesinin 2'nci maddesinde mevcut olan fakat 765 sayılı Türk Ceza Kanun'unda bunu kapsayan bir ifadenin olmaması, yasadışı erişim olarak kabul edilmesiyle bir koşutluk sağlanması[25] olsa dahi, bu suç durumunun meydana gelebilmesi için gerekli "orada kalmaya devam etme" faktöründen dolayı sözü geçen anlaşmanın 2'nci maddesinde yer alan "kanuna aykırı erişim" suç olmaktan kaldırılmıştır.

Toplum düzeninin korunması, bu suçla ilgili düzenlemenin yapılmasını zorunlu

[25] TBMM Genel Kurulunda yapılan değişiklikle, 243'üncü maddenin 1'inci fıkrasının ilk hali "giren veya kalmaya devam eden" şeklinde düzenlenirken "veya" ibaresi "ve" olarak değiştirilmiştir.

kılmıştır ve öncelikli amacı oluşturmaktadır. Diğer bir amaç ise bilişim sistemleri açısından güvenliğin sağlanmasıdır. Bilişim sistemlerine yasalara aykırılık teşkil eden bir erişimin önlenmesi sayesinde, bu sistemleri kullananların farklı türdeki menfaatleri korunmuş olmaktadır. Kullanıcıların özel hayatın gizliliğinin korunması, özel yaşamın dokunulmazlığı, kurumların ihtiyacını hissettiği güvenlik duygusu gibi farklı tipteki hukuki yararlar, bu menfaatleri meydana getirmektedir (Karagülmez, 2005:166; Dülger, 2004:214). Buna ilaveten bahsi geçen bilişim sistemleri vasıtası ile kişilerin haberleşme taleplerini karşılayan ve bununla birlikte kişilerin özgürce haberleşmelerinin sağlanması hedeflenmektedir (Doğan, 2005:294).

İlgili maddede "orada kalmaya devam etme" fiili suç faktörü olarak değerlendirilmişse de kalma süresi noktasında bir açıklık ortaya konulmamıştır. Fakat "orada kalmaya devam eden" ifadesi, "kalan" kelimesine kıyasla daha kapsamlı bir anlam ifade etmektedir. Bu sebepten ötürü yasada ifade edilen sürekliliğin olabilmesi için, "mütemadi bir suç" şeklinde olması ve bir süre devam etmesi gerekmektedir. Failin sistemi hemen terk etmeyip, ilgili bilgileri öğrenmesi halinde "kalmaya devam etme" fiilin gerçekleşmiş olacağı ise farklı bir görüştür.

Ancak sistemde kalmayı sürdürmeyi, failin sistemdeki bilgileri öğrenmiş olmasını düşünmek, bu suçun teşkil ettiği alanı daraltacağı gibi, ilgili maddede bilgilerin öğrenilmesi suç olarak düzenlenmemiş ve gerekçe olarak (Karagülmez, 2005:170.)[26] haksız ve bilerek sisteme girilmesi suçun oluşması için yeterli görülmüştür.

Kanunun hükmünü yerine getirme, bir hakkın icrası, meşru müdafaa durumu, görevin ifası veya mağdur olan kişinin rızası biçiminde kanuna uygun bulunmasıyla, bilgisayar sistemlerine girilip ve orda kalma sürdürülse yani suçun unsurları kanıtlansa dahi suç oluşmuş sayılmayacaktır. Örnek vermek gerekirse bilişim sisteminin sahiplerinin rızası ile sistemin test edilmesi ya da muhafazasına ilişkin erişimler bu suç için bir unsur teşkil etmeyecektir (İçel, 2001:8).

CMK m.134'de geçen m. 135'de "bilgisayarlarda, bilgisayar programlarında

[26] Suçu işleyenin hareketlenmesiyle sona ermeyip uygulanması uzun süren suç.

ve kütüklerinde arama, kopyalama ve el koyma" maddesiyle ifade edilen "iletişimin tespiti, dinlenmesi ve kayda alınması" ve m.l40'da belirtilen "Teknik Araçlarla İzleme" muhafaza önlemlerinin icra edilmesi durumunda, kanun hükmünün uygulanması hukuka uygunluktan dolayı bir suç oluşturmayacaktır (Doğan, 2005:297.).

Kast unsuru, bilgisayara ulaşma ve orada durmada ısrar etme suçunun manevi öğesini oluşturmaktadır. Buna ilaveten maddede düzenlenen bu suç için özel kast[27] durumu aranmamaktadır. Fail açısından genel suç işleme kastının bulunması yeterli olmaktadır. Buna göre fail iradi olarak girmeli ve kalmalıdır.

Tüm bu suçlarda kasten işlenişin dikkate alınarak ilgili düzenlemelerin yapılması Avrupa Konseyinin Siber Suç Sözleşmesi'ne de uygundur.

Her iki Türk Ceza Kanun'unda, bir suçun kusurlu işlenebilmesi ayrıcalıklı bir durumu teşkil etmektedir ve ceza alabilme çerçevesinden değerlendirildiği zaman kanuni açıklık gerektirmektedir[28]. Bu madde metninde hukuka aykırı bir şekilde bir bilişim sistemine girmenin suç şeklinde onaylanabileceğine ilişkin bir hüküm bulunmamasından dolayı, failin dikkatsizliği neticesinde hukuka aykırı olarak bir bilişim sistemine girmesi suç teşkil etmemektedir. Ancak ilgili maddenin 3'üncü fıkrasında bahsi geçen suçta verilerin yok edilmesi ya da değişmesinde taksir hususu tartışmalıdır (Karagülmez, 2005:173).

Kanuna aykırı usullerle bir bilişim sistemine girme ve orada kalma fiilinden dolayı sistemde bulunan verilerin yok olması veya değişmesi durumunda, kanuna göre daha ağır bir ceza verilmelidir (YTCK m.243/3).Eğer fail ulaştığı bilgileri yok etmiş veya değiştirmiş ise Yeni Türk Ceza Kanun'unun m.244. maddesince cezalandırılmalıdır.

Bir yıla kadar hapis yahut para cezası bu suç için yapılacak olan yaptırımdır.

---

27 Failin belirli bir amaç doğrultusunda hareketlenmesi özel kast olarak adlandırılır. Örneğin; failin başka bir kişinin malını alması hırsızlık suçunun olması için yeterli değildir. Suçun oluşabilmesi için aldığı maldan fayda sağlaması gerekir.

28 YTCK'nın 22. Maddesi "Taksirle işlenen fiiller, kanunun açıkça belirttiği durumlarda cezalandırılır."

Hâkim burada eldeki deliller ışığında suçluya hapis veya para cezası[29] uygulayacaktır. Yani burada hâkimin takdir yetkisi bulunmaktadır.

2.5.1.3. Sistemi Engelleme, Verileri Yok Etme, Bozma veya Değiştirme Suçları (YTCK M.244)

Yeni Türk Ceza Kanun'unun 244'üncü maddesinin 1'nci fıkrasında, "Bir bilişim sisteminin işleyişini engelleyen veya bozan kişi, bir yıldan beş yıla kadar hapis cezası ile cezalandırılır."; ardından ise "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." ifadeleri mevcuttur.

Türk Ceza Kanun'unun 765 sayısının 525/b-2 ile 525/b-1 maddelerinde mevcut suç unsurlarının, bir takım değişikliklerle beraber Yeni Türk Ceza Kanun'unun 244'üncü maddesinde düzenlendiği görülmektedir.

Bu düzenlemeler ile Avrupa Konseyi Siber Suç Sözleşmesi'nin ilgili maddelerine uyum amaçlanmıştır. Bu düzenleme aracılığıyla kanun koyucu tarafından bilişim mekanizmasının bozulması ve engellenmesi cezalandırılmak istemiştir. Bu maddeyle bilişim sistemine ilişkin zarar verme fiillerinin ayrı bir suç haline getirildiği maddenin sebebinde de belirtilmektedir (Karagülmez, 2005:186). Buna ilaveten bahsi geçen düzenlemede, 765 sayılı Türk Ceza Kanun'unda mevcut düzenlemeden farklı şekilde "zarar verme" fiili bulunmayarak, bilişim sistemlerinin donanım alanına hasar vermek için yapılan faaliyetler bunun dışında bırakılmaya çalışılmıştır (Dülger, 2004:230). Bu madde ile bilgisayarın mekanik kısmı ve sistemin faaliyetlerini oluşturan diğer tüm unsurların korunması istenmektedir.

Kanunda öngörülen maddede failin hangi niteliklere sahip olduğuna dair bir açıklama bulunmadığından dolayı herkesin bu suçun bir faili olabilmesi muhtemeldir. Suçlunun bulunabilmesi için suç olan eylemin kime ve neye karşı işlendiği ve zararı kimin oluşturduğunun tespit edilmesi gereklidir.

---

[29] YTCK'nın 52.Maddesi "Adli Para Cezası".

Mağdur olan kişi açısından da değerlendirildiğinde bu suç belirgin bir nitelik taşımadığı için, herkes bu suçun mağduru olabilmektedir. Aynı şekilde bu suçun mağduru olmak için zarara uğrayan verilerin veya bilişim sisteminin maliki ya da zilyedi olunması gerekmemektedir. Bilgisayar içerisindeki bilgi ve belgelere başkalarının erişiminden zarar gören herkes işlenen suçun mağduru olmaktadır.

Kanuni olarak birden çok fiil gerektiren suçlar seçimli hareketli suçları oluşturmakta olup, bunlardan birinin bile yapılması suçun oluşmasını sağlamaktadır. Yeni Türk Ceza Kanun'unun 244'üncü maddesinde bu tür suçlar bulunmaktadır. Bundan dolayı aşağıda bahsi geçen fiillerden birinin bile işlenmesi suçun oluşması yeterli görülmektedir.

Söz geçen maddenin 1'inci fıkrasında "bilişim sisteminin işleyişini engelleme" ya da "bozma", 2'nci fıkrasında ise "sisteme hukuka aykırı biçimde veri sokma" ya da "var olanları başka bir yere gönderme", "sistemdeki verileri yok etme" ya da "bozma", "değiştirme" ya da "erişilmez kılma" fiilleri suç olarak belirtilmektedir.

İlk fıkra, bilişim sistemlerinin kendisine dönük işlenen engelleme ya da bozma biçiminde zarar verme eylemlerini özel nitelikte bir suç olarak saymaktadır. Bozmak, sistemin programlandığı şekliyle çalışmamasına neden olmak, engellemek ise sistemin düzgün bir şekilde işlemesine engel teşkil etmektir. Engellemek ya da bozmak fiili çeşitli birtakım müdahaleler aracılığıyla sağlanmaktadır. Mesela bilişim mekanizmasının işleyişini sağlayan bilgisayara virüs bulaştırmak veya kasıtlı olarak alıcının iletişimini bloke edecek ya da yavaşlatacak şekilde fazla e-posta göndermek bu tür suçun oluşmasını sağlayabilir.

İkinci fıkrada ise sisteme bilgi girilmesi, bilgilerin ortadan kaldırılması, ulaşılmaz hale getirilmesi ya da düzenlenmesi suçtur. Bu suçun meydana gelmesini sağlayan eylemler aşağıdaki gibidir;

"Verilerin bozulması", veriler var olmakta fakat görevlerini yapmasının olanaksız hale getirildiği durumlardır.

"Verilerin yok edilmesi", yani silinmesi olup burada amaç eldeki verileri

değiştirmek suretiyle yerlerine farklı verilerin yerleştirilmesi ve asıl verileri işlevsiz kılmaktır.

"Verileri erişilmez kılmak", bilişim sistemini kullan kişinin verilere arzu ettiği anda ulaşmasının engellenmesi manasına gelmektedir.

"Sisteme veri yerleştirmek", failin bilişim sisteminin sahibinin ya da kullanıcısının rızası ve haberi olmadan sistemine dışarıdan girmektir.

Sistemdeki bilgileri başka bir ortama aktarmak, sistem içerisindeki mevcut verilerin taşıma aracına aktarılması, yerlerinin değiştirilmesi ya da verilerin kaydedilmesi yahut kopyalanması anlamına gelmektedir

244'üncü maddenin 4'üncü fıkrasına göre, yukarıdaki fıkralarda tanımları yapılan eylemlerin gerçekleştirilmesiyle şahsın kendisi ya da başka birinin yararına kanunsuz bir çıkar elde etmesinin başka bir suçu ortaya çıkarmasıyla, iki yıl ile altı yıl arasında hapis ve beş bine kadar adli para cezası verilir.

Bu maddeyi bir örnek vererek açıklayalım; suç teşkil eden fiili işleyen kişi bilgisayarda hasara neden olacak bir virüsü bilişim sistemine yolladığında sistemdeki veriler bundan zarar görürse, ikinci fıkrada belirtilen suçu işlemiş olur. Eğer aynı virüs sistemin tüm mekanizmasını bozar ya da engel koyarsa birinci fıkrada bulunan suç ortaya çıkacaktır. Bu suçu işleyen şahıs bu faaliyeti ile anti-virüs geliştiren bir firmanın çıkarını hedeflediğinde ve buna ulaştığında dördüncü fıkra hükmünden cezalandırılır. Ayrıca 244'üncü maddenin 4'üncü fıkrasının hayata geçirilebilmesi için meydana gelen fiilin "başka bir suç oluşturmaması" gerekmektedir. Bu durumu bir misalle açıklayacak olursak; dolandırıcılık kastıyla sanık (S) oluşturduğu biz web sitesini bir bankanın web sitesiymiş gibi lanse ederek banka müşterisine kişisel bilgiler ve hesap bilgilerinin güncellenmesi gerektiğini belirten bir e-posta göndermiştir. Bu gönderilen e-posta bilişim sistemini yıpratıcı faktörlere de sahiptir. Mağdur (M) bu işlem sonucunda yanlış bilgilerle kandırılmış ve (S) bu durumdan haksız çıkar sağlamıştır.

(S) eylemi ile (M)'yi dolandırmıştır. Bu eylemi yaparken (M) ye ait bilişim

sistemini çalışmasını bozmuş ya da bloke etmiş ise 244/1'e göre; bozmamış ya da bloke etmemiş ise 244/2'ye gereğince suç oluşmuş olacaktır. 2'nci fıkradaki olduğunu varsayarsak ve (S)'nin amacı haksız fayda elde etmek olacağından, 244'üncü maddenin 4'üncü fıkrası dikkate alınacaktır. Ama bu fıkranın hayata geçirilebilmesi için eylemin 244'üncü madde haricinde bir suç içermemesi gereklidir (Doğan, 2005:304). Bu olayda (S)'nin eylemi, Yeni Türk Ceza Kanun'unun 158'inci maddesinin 1'nci fıkrasının (f) bendindeki bilişim sistemlerinin araç olarak kullanılması amacıyla sahtekârlık kapsamına da girdiği için 244/4 göre hüküm verilemeyecektir. Bu olayda hüküm; Yeni Türk Ceza Kanun'unun "Fikri İçtima" kenar başlıklı 44'üncü maddesindeki "İşlediği bir fiil ile birden fazla farklı suçun oluşmasına sebebiyet veren kişi, bunlardan en ağır cezayı gerektiren suçtan dolayı cezalandırılır." İfadesinden hareketle daha ağır ceza içeren 158/1-f'ye göre verilir.

2.5.1.4. Banka ve Kredi Kartlarının Kötüye Kullanılması Suçları (YTCKm.245)

Gelişen teknolojiyle birlikte insanlar alış verişlerde nakit ödeme yapmaktan ziyade banka ve kredi kartlarını kullanmaya başlamaları, bu kartlara olan ilginin artmasına ve toplumda gitgide çoğalmasına neden olmuştur.

Toplumda internet kullanımının hızla yaygınlaşmasıyla birlikte gerek kredi kartı ve gerekse de banka kartıyla ilgili suçlar büyük miktarda artış göstermiştir. 2002 yılı verilerine göre kredi kartı dolandırıcılığı, Avrupa' da 4 milyar dolara kadar ulaşmıştır. FBI raporlarına göre, bir milyondan fazla kredi kartı numarası e-ticaret siteleri üzerinden bilgisayar korsanları tarafından ele geçirilmiştir. Bu gelişmeler neticesinde ise internet kullanıcılarının birçoğu, internet üzerinden yapılan alışverişi güvenli görmemektedir. Avrupa'da yapılan bir araştırmaya göre; İnternet kullanıcılarının yaklaşık olarak yarısı internette alışveriş için kredi kartı bilgilerini vermeyi güvenli bulmamaktadır.

Yukarıda bahsi geçen güvensizlik durumu ve kart bilgilerinin çalınmasından dolayı kanun koyucular tarafından e-ticaret'in güvenliğini arttırmak amacıyla düzenlemeler yapılmıştır.

Bu konudaki düzenleme Türkiye'de ilk defa ETCK'nın 525/b-2 (Philippsohn and Thomas'tan, 2003:7-9.)[303132] maddesinde yer almaktadır. İlgili madde de bu kartların kötüye kullanımı ile ilgili bir düzenleme bulunmasa da, ülkemizde bu tür olaylarla alakalı mahkemelerde birçok dava bulunmuş ve YTCK bu konuya açıklık getirmek için 245. Madde de aldığı kararlar doğrultusunda ilgili kartların kötüye kullanılması ile ilgili yapılan işlemler bu madde kapsamında değerlendirmeye alınmıştır. Bu madde ile suçun önlenmesi için gerekli cezai müeyyide belirlenmiştir.

245'inci maddenin gerekçesinde, bu suçun aslında hırsızlık, dolandırıcılık, sahtecilik ve güveni kötüye kullanma suçlarını teşkil etiği ve bu suçlardan ilgili değerlerin korunması gerektiği anlaşılmakta olup, bunun faydalarında biride bankaların sunmuş olduğu hizmetler yoluyla devam eden ticaretin bankacılık sektöründeki güvenirliliğin sürmesiyle devam edeceği de anlaşılmaktadır. [3334]

---

30 Madde 525/b-2 "Bilgileri otomatik işleme tabi tutmuş bir sistemi kullanarak veya başkası lehine hukuka aykırı yarar sağlayan kimseye bir yıldan beş yıla kadar hapis ve iki milyondan yirmi milyon liraya kadar ağır para cezası verilir."

31 Emniyet Genel Müdürlüğü Kaçakçılık ve Organize Suçlarla Mücadele Daire Başkanlığının yaptığı araştırmaya göre, kredi ve banka kartlarıyla ilişkili kanuna aykırı eylemler dokuz grupta toplanabilir (Değirmenci, 2003:509). Bunlar;

1) Kayıp veya çalıntı kart kullanılması,
2) Talep üzerine sistem kuruluşu tarafından çıkarılan banka veya kredi kartının kart sahibinin eline geçmeden, ele geçirilmesi ve kötü amaçlı kullanılması,
3) Sahte bir kimlikle banka veya kredi kartlı sistem kuruluşuna başvuru yapılıp kredi kartı alınması ve kötüye kullanılması,
4) İşyerleriyle birlikte yapılan etkinlik sonunda, boş plastik üzerine kabartma olarak basılan gerçek kredi kart numaralarıyla alış veriş yapılmış izlenimi bırakılmakta ve bu miktarın sonradan bankadan alınması,
5) Kredi kartlarının üzerinde bulunan kabartma numaralarının kesilip değiştirilmesi ya da ütü yapılarak yenisinin basılması,
6) Farklı yollarla üretilen kartın arka yüzünde bulunan manyetik şerit "encoder" adı verilen bir cihaz yardımı ile kodlanıp içine elektronik yollardan kart bilgilerinin yazılarak kullanılması,
7) Başka kartlara ait bilgilerin gerçek kartın manyetik şeridinde bulunan bilgilerle değiştirilmesi,
8) Önceden ayarlanmış bir adrese kredi kartı numarası kullanılarak posta veya telefonla mal siparişlerinde bulunulması,
9) Kart sahibi ATM cihazlarında işlem yaparken kredi kartı ve şifre bilgilerinin ele geçirilmesi kötüye kullanılması,

32 YCGK, K.t. 10.04.2001, E:2001/7630, K:2001/757, YKD, Haziran 2001, sf. 913-915.

33 Madde 245 "Banka veya kredi kartlarının kötüye kullanılması",

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

(2) "Başkalarına ait banka hesaplarıyla ilişkilendirilerek sahte banka veya kredi kartı üreten, satan, devreden, satın alan veya kabul eden kişi üç yıldan yedi yıla kadar hapis ve on bin güne kadar adli

Bu suç açısından herkes fail olabilir. Ancak gerçek manada bir kişinin suçu işleyen sayılabilmesi için farklı bir kişinin kredi kartı ya da banka kartını, herhangi bir nedenden eline geçiren yahut elinde bulunduran birisi olmalıdır (Dülger, 2004:251; Kurt, 2005:178.). Bundan dolayı ki, şahsına ait banka ya da kredi kartını haksız yere kullanmak suretiyle yarar sağlayan kişi bu suçun faili olarak sayılmaz, bu kişi sadece güveni suistimal etme veya dolandırıcılık yapılan kişi olabilir. Buna ilaveten Kredi Kartları ve Banka Kartları Kanununda "Sözleşme ve Eki Belgelerde Sahtecilik Suçu" (m.37), "Gerçeğe Aykırı Beyan" yer almaktadır. Bu kanuna göre, banka kartı ya da kredi kartını kaybettiği yahut çaldırdığı yolunda gerçeği yansıtmayan beyanda bulunarak kartı bizzat kullanan veya başkasına kullandıran kart hamilleri ile bunları bilerek kullananlar"

Düzenlenen bu madde ile aşağıdaki üç tip suç belirlenmiştir;

a) (YTCK m.245/1) Gerçek kredi ya da banka kartının kötü amaçlı kullanımı

Bahsi geçen maddenin ilk fıkrasına göre, kanuni yollar aracılığıyla hazırlanmış bir kredi ya da banka kartının kötü niyetle kullanılması durumunda ceza verilir.

Fail tarafından başka bir şahsa ait kredi kartının ya da banka kartının ele geçirilmesi ya da elinde bulundurulması bu suçun meydana gelmesi için ilk şarttır. Bu kart fail tarafından bulunmuş, çalınmış ya da yanlışlıkla ona ulaştırılmış şeklinde de olabilmektedir. Sonrasında ise failin bu kartı sahibinin rızası dışında kullanması ya da kullandırması ve bunun sonucunda da failin kendisi ya da başkası lehine haksız kazanç sağlaması suçun oluşması için gereklidir. Netice itibariyle suçun meydana gelebilmesi için failin kartı ele geçirip kullanması tek başına yeterli olmamakta ve bu

---

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 adli para cezası ile cezalandırılır."

(4) 1.fıkrada bulunan suçun;

a) Haklarında ayrılık hükmü bulunmayan eşlerden birisinin,

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

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

[34] 245'inci maddenin gerekçesinden.

karttan haksız bir şekilde fayda sağlaması gerekmektedir.

b) (YTCK m.245/2) Sahte kredi kartı veya banka kartı üretmek, satmak, satın almak, devretmek veya kabul etmek

Yeni Türk Ceza Kanun' nun m.245/2'de düzenlenen "sahte banka veya kredi kartı üretmek", "satmak", "devretmek", "satın almak" veya "kabul etmek" suçlarında, suçun olabilmesi için herhangi bir çıkar elde edilmesi şartı aranmamaktadır. Bu eylemlerin yapılması suçun meydana gelmesi çerçevesinden değerlendirildiğinde tek başlarına yeterli olmaktadır (Bayraktar, 2000:201; Ekinci, 2002:101).

c) Üzerinde sahtecilik yapılan ya da sahte oluşturulan kredi veya banka kartlarının kötü amaçlı kullanımı (YTCK m.245/3)

Yeni Türk Ceza Kanun'unun 245/3 maddesinde düzenlemesi yapılan suçun suç unsurunun mevzuu, kart üzerinde düzmecilik yapmak ya da kartın farklı bir şekle uyarlanmasıdır.

Bu suçun meydana gelmesi birden çok hareketin varlığına bağlı olmaktadır. Diğer bir ifadeyle, bu suçun tam olarak oluşması için üzerinde sahtecilik yapılan veya sahte olarak düzenlenen bir kartı ele geçirmek ve bu kartı kullanarak haksız yarar sağlamak gerekli olmaktadır. Ayrıca sahtecilik fiilini işleyen kişi ile bu kartları kullanmak suretiyle haksız yarar sağlayan kişinin aynı kişiler olma zorunluluğu söz konusu değildir.

2.5.1.5. Tüzel Kişiler Hakkında Güvenlik Tedbiri Uygulaması (YTCK m.246)

Yeni Türk Ceza Kanun'unun 20/2 maddesiyle "Tüzel kişiler hakkında ceza yaptırımı uygulanamaz. Fakat suçtan ötürü kanunda öngörülen güvenlik tedbiri niteliğindeki yaptırımlar saklıdır." biçiminde bir düzenleme de mevcuttur. Yeni Türk Ceza Kanun'unun 60'ıncı maddesinde ise tüzel kişiler hakkında uygulanacak güvenlik tedbirleri mevcuttur. Bu maddeye göre;

1- "Bir kamu kurumunun verdiği izne dayalı olarak faaliyette bulunan özel

hukuk tüzel kişisinin organ veya temsilcilerinin iştirakiyle ve bu iznin verdiği yetkinin kötüye kullanılması suretiyle tüzel kişi yararına işlenen kasıtlı suçlardan mahkûmiyet halinde, iznin iptaline karar verilir."

2- "Müsadere hükümleri, yararına işlenen suçlarda özel hukuk tüzel kişileri hakkında da uygulanır."
3- "Yukarıdaki fıkra hükümlerinin uygulanmasının işlenen fiile nazaran daha ağır sonuçlar ortaya çıkarabileceği durumlarda, hâkim bu tedbirlere hükmetmeyebilir."
4- "Bu madde hükümleri kanunun ayrıca belirttiği hallerde uygulanır."

Bu düzenlemeyle birlikte Yeni Türk Ceza Kanunu tüzel kişilerin cezai sorumluluğu kabul edilmiştir. Kanunda yalnızca özellikle belirtilen yerlerde haklarında bazı güvenlik önlemlerinin alınacağı hükmüne varılmıştır. 246'ncı madde de bu maddelerden birisini oluşturmaktadır. Bu madde kapsamında haksız çıkar elde eden tüzel kişiler hakkında güvenlik tedbirlerine hükmolunacaktır.[35] Bu kapsamda karşılaştırmalı hukukta;

a) Cezai sorumluluğu reddedip idari yaptırımları tahmin edenler,
b) Güvenlik tedbirini tahmin edenler,
c) Tüzel şahısların cezai yükümlülüğünü kabul edenler olmak üzere üç farklı sistem bulunmaktadır.

2.5.1.6. YTCK'da Düzenlenen Diğer Siber Suç Tipleri

Yukarıda bahsedilen YTCK'nın "Bilişim Alanındaki Suçlar Bölümü" bulunan suçlar haricinde, yine bu kanunun farklı bölümlerinde siber suçlarla ilgili düzenlemeler bulunmaktadır. Bu düzenlemeler aşağıda "Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar Bölümünde Düzenlenen Suç Tipleri" ve "Bilişim Sistemleri Aracılığıyla İşlenebilecek Diğer Suç Tipleri" olmak üzere iki ana başlık altında ele alınacaktır.

---

35 Madde 246: "Tüzel kişiler hakkında güvenlik tedbiri uygulanması",
"Bu bölümde yer alan suçların işlenmesi suretiyle yararına haksız menfaat sağlanan tüzel kişiler hakkında bunlara özgü güvenlik tedbirlerine hükmolunur."

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

2.5.1.6.1.1.Kişisel Verilerin Kaydedilmesi Suçu (m.135)

Yeni Türk Ceza Kanun'unun 135'inci maddesinin birinci fıkrasıyla, kanuna aykırı bir şekilde kişisel verilerin kayıt altına alınması eylemi; ikinci fıkrasıyla da kişilerin felsefi, siyasi ya da dini görüşlerinin, sendikal bağlantılarının, ırki kökenlerinin, cinsel yaşamlarının ve sağlık durumlarının kişisel veri olarak kayıt altına alınması eylemleri suç olarak hüküm altına alınmıştır[36] (Özel, 2001:865; Değirmenci, 2002:156-157)[37].

Bahsi geçen maddedeki suçlar, çoğunlukla bilgisayarlar vasıtasıyla işlenmektedirler. İlgili maddenin gerekçesinde "günümüzde birçok kurumun şahıslar ile ilgili bilgileri bilgisayarlarda arşivleyerek muhafaza ettiğini belirtmektedir. Bu bilgiler amaç dışı kullanılırsa hakkında bilgi toplanan kişilere büyük zararlar verilebilecektir. Bu çerçeveden bakıldığında, kişilerle ilgili bilgilerin hukuka aykırılık teşkil edecek biçimde kaydedilmesi suç olarak tanımlanmıştır." denilmektedir.

135'inci madde, Yeni Türk Ceza Kanun'unun "özel hükümler" başlıklı ikinci kitabının "kişilere karşı suçlar" başlıklı ikinci kısmının "özel hayata ve hayatın gizli alanına karşı suçlar" başlıklı dokuzuncu bölümünde düzenlenmiştir. Buradan 1982 Anayasasının "Özel Hayatın Gizliliği ve Korunması" başlıklı 20'nci maddesindeki, "Herkes, özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahiptir. Özel hayatın ve aile hayatının gizliliğine dokunulamaz..." ifadesiyle hükmolunmuştur.

135'inci maddede suçun işlenme biçimi ile alanına herhangi bir sınırlandırma

---

36 Madde 135 "Kişisel verilerin kaydedilmesi";
1- "Hukuka aykırı olarak kişisel verileri kaydeden kimseye altı aydan üç yıla kadar hapis cezası verilir."
2- "Kişilerin siyasi, felsefi veya dini görüşlerine, ırki kökenlerine; hukuka aykırı olarak ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin bilgileri kişisel veri olarak kaydeden kimse, yukarıdaki fıkra hükmüne göre cezalandırılır."

37 Türkiye'nin de paydaşı olduğu bu sözleşmeye göre, sözleşmenin onaylanabilmesi için paydaş devletlerin sözleşmede değinilen ilkelere uygun bir kanun (uygulama kanunu) kabul etmesi gerekir.

getirilmemiştir. Bu suç ile şahsi bilgilerin kanuna ters biçimde kayıt altına alınması eyleminde ceza almış olur. Buna ilaveten suç en çok bilişim sistemlerinde işlense de yalnızca burada işlenebileceğini söylemek doğru bir ifade olmayacaktır.

Yeni Türk Ceza Kanun'unun 137'nci[38] maddesinde "özel hayata ve hayatın gizli alanına karşı suçlar" kısmında düzenlenen suçlar için failin sıfatından ötürü ağırlaştırıcı sebepler ortaya koyulmuştur. Buna göre, söz konusu maddenin "a" bendinde "kişisel verilerin kaydedilmesi" suçunun bir kamu görevlisi tarafından ve görevinin verdiği yetkinin kötüye kullanılması halinde failin cezası arttırılarak uygulanacaktır. Söz konusu maddenin "b" bendinde ise belirli bir meslek ve sanatın sağladığı kolaylıktan yararlanmak hasebiyle bu suç gerçekleştirilirse failin cezası yine arttırılarak uygulanacaktır.

Hukukta şahsi bilgilerin kayıt altına alınması suçunda, suç işleyenler için yaptırım olarak altı aydan üç yıla kadar hapis istemi yer almaktadır.

2.5.1.6.1.2.Kişisel Verileri Hukuka Aykırı Olarak Verme ya da Ele Geçirme Suçu

Yeni Türk Ceza Kanun'unun 136'ncı maddesinde "Kişisel verileri, hukuka aykırı olarak bir başkasına veren, yayan veya ele geçiren kişi, bir yıldan dört yıla kadar hapis cezası ile cezalandırılır." hükmü düzenlenmiştir. Bu suçun, yaygın olarak İnternet'te işlendiği görülmektedir. Kimlik hırsızlığı olarak da bilinen İnternet'teki kişisel verilerin ele geçirilmesi eylemleri, genel olarak müşterilerin adı, doğum tarihi, kredi kartı bilgileri, sosyal güvenlik numaraları kendi bilgisi olmadan ele geçirilmektedir. Daha sonra elde edilen bu verilerle, haksız kazanç elde etmek üzere, İnternet dolandırıcılığının da içinde bulunduğu pek çok suç işlenmektedir. Kredi kartı bilgileri ele geçirilerek genellikle müşteri hesaplarından nakit para transferleri yapma veya kartın kopyalanarak sahtesinin yapıldığı görülmektedir.

Bu suçun faili, şahsi bilgilere ulaşılması suçunda, suç işleyen yönünden bir

---

38 Madde 137 "Nitelikli haller";
"Yukarıdaki maddelerde tanımlanan suçların; Kamu görevlisi tarafından ve görevinin verdiği yetki kötüye kullanılmak suretiyle; belli bir meslek ve sanatın sağladığı kolaylıktan yararlanmak suretiyle işlenmesi halinde, verilecek ceza yarı oranında artırılır."

nitelik araştırılmadığından herkes olabilir. Bu sebeple ele geçirilen verilerle alakalı olan herkes mağdur olabilir (Karagülmez, 2005:233; Fedorek'ten, 2004:5).

Bu suçla hukuka uygun olarak kayıt altına alınan veya kayıt altına alınmayan kişisel verileri hukuka aykırı olarak başkasına vermenin, yaymanın ya da ele geçirmenin bağımsız bir suç olarak düzenlendiği görülmektedir[39] (Dülger, 2004:271).

Maddenin gerekçesinde de açıklandığı üzere suçun oluşmasında; başka bir kişiye ulaştırılan, elde edilen verilerin kayıt altına alınışının hukuki boyutuna bakılmaz. Veriler nasıl kaydedildiğine bakılmaksızın yukarıdaki eylemlerden birini yapan suç işlemiş olmaktadır. Bu suç da bilerek ve isteyerek işlenebilen bir suçtur. İlgili maddede eylemin hukuk dışı gerçekleştiği ifade edilmekte ve failin kast eyleminde, eylemin kanuna ters olduğunu da kapsam içine alması gereklidir (İçel ve Ark, 2000:8).

YTCK'nın 137'nci maddesinde "özel hayata ve hayatın gizli alanına karşı suçlar" bölümünde düzenlenen eylemler için failin sıfatından dolayı ağırlaştırıcı sebepler sezilmiştir. Maddede yer alan hallerin oluşmasıyla, istenilen ceza yarısı kadar arttırılıp işleme konulacaktır.

2.5.1.6.1.3.Verilerin Yok Edilmemesi Suçu (M.138)

Bu maddeyle, kişisel bilgilerin hukuka aykırı olmadan kayıt altına alınması kanunlarca belirlenen sürelerin geçmiş olmasına karşın ortadan kaldırılmaması suçu bağımsız olarak değerlendirilmiştir.

Yani kanunlar tarafından belirlenen süreler içinde kamu ve özel sektör kuruluşlar ellerinde mevcut olan kişisel verileri yok etmek durumundadırlar.

Bu kapsamda verileri yok etmekle (geri getirilemeyecek şekilde silme) yükümlü olan kişi bunu yapmamış ise suç işlemiş olur. Sorumlu olan kişi verilerin bir kısmını silmiş fakat bir kısmı duruyor ve bu kısım veri özelliği taşıyorsa ilgili madde kapsamınca suçlu demektir.

---

[39] Madde gerekçesinden.

2.5.1.6.1.4. Haberleşmenin Gizliliğini İhlal Suçu (M.132)

YTCK'nın "haberleşmenin gizliliğini ihlal" kenar başlıklı 132'nci maddesinde,

(1) " Kişiler arasındaki haberleşmenin gizliliğini ihlal eden kimse, altı aydan iki yıla kadar hapis veya adli para cezası ile cezalandırılır. Bu gizlilik ihlali haberleşme içeriklerinin kaydı suretiyle gerçekleşirse, bir yıldan üç yıla kadar hapis cezasına hükmolunur."

(2) "Kişiler arasındaki haberleşme içeriklerini hukuka aykırı olarak ifşa eden kimse, bir yıldan üç yıla kadar hapis cezası ile cezalandırılır."

(3) "Kendisiyle yapılan haberleşmelerin içeriğini diğer tarafın rızası olmaksızın alenen ifşa eden kişi, altı aydan iki yıla kadar hapis veya adli para cezası ile cezalandırılır."

(4) "Kişiler arasındaki haberleşmelerin içeriğinin basın ve yayın yolu ile yayınlanması halinde, ceza yarı oranında artırılır" ifadesine yer verilmiştir."

Günümüzde teknolojinin hızlı bir şekilde gelişme göstermesi insanların iletişimlerini de başta internet olmak üzere çeşitli yollar ile sağlamasına olanak tanımıştır. Bu haberleşme yöntemleri ise YTCK'nın ilgili maddelerince koruma altına alınmış ve aksi durumların cezalandırılması gerektiği ifade edilmiştir. Bu sayede bu konudaki tartışmalara da son verilmiştir.

2.5.1.6.1.5. Haberleşmenin Engellenmesi Suçu (m.124)

YTCK'nın "haberleşmenin engellenmesi" kenar başlıklı 124'üncümaddesinde;

(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 cezalandırılır." hükümleri yer

almaktadır.

YTCK'nın 124'üncü maddesinde de ifade edildiği gibi haberleşme hangi cihazla yapılırsa yapılsın engellenmesi suç teşkil etmektedir.

2.5.1.6.1.6.Hakaret (Aşağılama) Suçu (m.125)

Bu tür suç YTCK'nın 125'inci maddesinde düzenlenmiş olup, ilgili maddenin 2. fıkrasında; mağdur açısından hakaret oluşturan eylemin (yazı, ses ya da görüntü yoluyla) bilgisayar vasıtasıyla işlenmesinde suç olduğu belirtilmektedir.

2.5.1.6.1.7.Bilişim Sistemlerinin Kullanılması Yoluyla İşlenen Hırsızlık Suçu (m.142)

YTCK'nın "malvarlığına karşı suçlar" başlıklı onuncu bölümünün 142'nci maddesinin ikinci fıkrasının "e" bendinde bilişim sisteminin kullanılması aracılığı ile işlenen hırsızlık suçu yer almaktadır.

Ama bu konu ile ilgili yapılan düzenlemelerde hangi tip hırsızlık fiilinin suç unsuru olduğu net olarak ifade edilmemiştir. Yani bilişim sistemi yoluyla somut nesnelerin alınması mı yoksa verilerin çalınması mı suç unsurudur. Buradan anladığımız ilgili şahsın rızası olmadan, failin kendisine ya da başkasına fayda sağlamak niyetiyle bilişim sistemini kullanarak eşya üzerinden sahibinin hükmünü kaldırması suçu oluşturmaktadır.

Belirtmek gerekir ki uygulamada oluşabilecek hataların önüne geçmek için bu suç türünün bağımsız olarak ele alınması ve ilgili düzenlemelerin daha açık bir şekilde yapılması zaruridir (Dülger, 2004:290). Bu şekliyle olası hataları düzeltmek Yargıtay'a kalmaktadır.

2.5.1.6.1.8.Bilişim Sisteminin Kullanılmasıyla Gerçekleşen Dolandırıcılık Suçu (m.158)

Bu suç türünün sebepleri ve işleniş şekilleri üstte ifade edilen suç türü ile aynıdır. Bu madde ile çokça karşılaşılan suç türlerinden olan bu suç türü düzenlenmekte ve ilgili cezai müeyyideler ifade edilmektedir.

2.5.1.6.1.9.Müstehcenlik (Edebe Aykırılık) Suçu (M.226)

Edebe aykırılık (müstehcenlik) suçu YTCK'nın 226'ncı maddesinde yer almaktadır. Bu maddede edebe aykırı yayınlar ve çocukların/gençlerin bunlara karşı nasıl korunması gerektiğine yönelik düzenlemeler bulunmaktadır. Maddede belirtilen yayınlar bilgisayar ağları aracılığı ile gerçekleştirilmektedir. Bu düzenlemelerde uygulamada karışıklığa neden olacak eksiklikler bulunmakta olup bunlardan biride Avrupa Konseyi Siber Suç Sözleşmesi göz ardı edilerek çocuk pornografisinin ayrı bir suç olarak uygulamaya konulmasıdır.

2.6.POLİS İSTATİSTİKLERİNE GÖRE SİBER SUÇLAR (2003-2012)

Polisin sorumlu olduğu alanlarda meydana gelen siber suçların istatistiksel verileri, Emniyet Genel Müdürlüğü'nün faaliyet raporları ile bazı kaynaklarda mevcuttur. Bu raporlarda genel olarak; "Banka Dolandırıcılığı", "Kredi Kartı Sahteciliği ve Dolandırıcılığı" , "İnternet Aracılığıyla Dolandırıcılık", "Bilişim Suçları ve Dolandırıcılığı" ve "Diğer" biçiminde sınıflandırılmıştır. İlk yıllarda özellikle finans sektörüyle alakalı bilişim suçlarında oldukça fazla bir yoğunluğun söz konusu olduğu görülmektedir.

2007 yılı itibariyle sınıflandırmaya "Diğer" (telif hakkı suçları, cinsel istismar, hakaret, özel hayatın gizliliği gibi) başlığı eklenmiştir. Sınıflandırma genel olarak maddi kayıplara göre hazırlanmış olup 2003- 2012 yılları arasında tespit edilen durum aşağıda tablada verilmiştir.

Tablo 1: 2003-2012 Yılları Arası Siber Suç Sayılan Eylemler

Suçun Nevi Ve Yıllara Göre Olay Sayıları	Kredi Kartı Sahteciliği ve Dolandırıcılığı	Banka Dolandırıcılığı	Bilişim Suçları ve Dolandırıcılığı	İnternet Aracılığıyla	Diğer	Toplam
Olay Sayısı 2003	**80**	**15**	**X**	**X**	**X**	**95**
Olay Sayısı 2004	**146**	**22**	**16**	**X**	**X**	**184**
Olay Sayısı 2005	**195**	**9**	**91**	**X**	**X**	**295**
Olay Sayısı 2006	**122**	**98**	**4**	**X**	**X**	**224**
Olay Sayısı 2007	**594**	**642**	**416**	**X**	**91**	**1.743**
Olay Sayısı 2008	**830**	**1.177**	**560**	**X**	**157**	**2.742**
Olay Sayısı 2009	**1.511**	**550**	**353**	**412**	**45**	**2.871**
Olay Sayısı 2010	**1.131**	**151**	**972**	**71**	**28**	**2.353**
Olay Sayısı 2011	**1.772**	**141**	**1.738**	**111**	**31**	**3.793**
Olay Sayısı 2012	**1.724**	**264**	**3.669**	**278**	**783**	**6.718**

Söz konusu istatistiklerin birçoğu EGM' nin kaynaklarından alınmış olup, polis tarafından yapılan çalışmalar neticesinde meydana getirilmiştir. Maalesef ülkemizde polis istatistiklerinde çeşitli nedenlerden dolayı birçok eksiklik bulunmakta olup bu kurumun istatistikleri ile Adalet Bakanlığı'nın istatistikleri

arasında uyum bulunmamaktadır. Tüm bu konularda gerekli çalışmaların olmaması da eleştirileri beraberinde getirmektedir (Polat, 2008: 4). Türkiye' de ilk bilişim suçu 1990 yılında işlenmiş olup, bu yıldan 2011 yılının Temmuz ayına kadar geçen sürede mahkemelere toplamda 40 farklı suç maddesi ile 73.185 tane suç dosyası ve bu suçlara ait 98.391 adet maznun olduğu saptanmıştır (Köksal ve İlbaş, 2015). Tablo-1 ile Tablo-2 ilişkilendirildiğinde, adliyede süren fakat polis istatistiklerinde olmayan birçok olayın olduğu gözükmektedir.

Ülkemizde ilk olarak siber suç 1990 yılında işlenen banka kartı dolandırıcılığıdır. 1990 ila 2003 yılları arasında adliyeye ulaşan siber suç dava sayısı, 389 adettir. Bu sayının ağırlıklı kısmını banka ve kart dolandırıcılığı oluşturmaktadır. Diğer suçları ise telif hakkı ile bilişim sistemlerine giriş suçları oluşturmaktadır. Bakıldığında bu yıllarda bilişim suçlarının çok da fazla olmadığı görülmektedir. Bunun sebebi ise; 5237 sayılı Türk Ceza Kanun'unun 2004 tarihinde kabul edilmesi ve önceki yıllarda siber suçlarla alakalı olarak özel kolluk kuvvetlerinin bulunmaması, bu yıllar arasında bilgisayar kullanımının yaygınlığı ile bilişim okuryazarlığının oranının düşük olması, suça maruz kalan kişilerin yasal nitelikteki haklardan yararlanma olanağının olmayışıdır. EGM kayıtlarına göre 2003-2012 yılları arasında toplamda 21.018 siber suç olmuştur. Ayrıca 2007 yılından itibaren siber suçların önemli derecede arttığı görülmektedir.

Tablo 2: 2003-2012 Yılları Arası İşlenen Siber Suçlarda Yakalanan Şüpheliler

Suçun Nevi ve Yıllara Göre Şüpheli	Kredi Kartı Sahteciliği ve Dolandırıcılığı	Banka Dolandırıcılığı	Bilişim Suçları ve Dolandırıcılığı	İnternet Aracılığıyla	Diğer	Toplam
2003	**268**	**49**	**X**	**X**	**X**	**317**
2004	**422**	**72**	**31**	**X**	**X**	**525**
2005	**543**	**33**	**179**	**X**	**X**	**755**
2006	**241**	**172**	**9**	**X**	**X**	**422**
2007	**907**	**1.187**	**764**	**X**	**134**	**2.992**
2008	**991**	**2.114**	**842**	**X**	**416**	**4.363**
2009	**2.176**	**1.113**	**534**	**731**	**116**	**4.670**
2010	**1.005**	**300**	**1.346**	**115**	**134**	**2.900**
2011	**1.429**	**327**	**1.842**	**283**	**123**	**4.004**
2012	**630**	**120**	**1.085**	**56**	**289**	**2.180**

2014 yılı verilerine göre banka ve kredi kartı dolandırıcılığı başta olmak üzere internet üzerinden online kumar faaliyetleri, yetki dışı erişim ve sistem engelleme şeklindeki suçlara ilişkin olarak yapılan operasyonlar kapsamında 2.788 şüpheli şahıs yakalanıp adli organlara götürülmüştür (EGM, 2015: 28). 2003-2012 yılları arasında toplamda 23.098 şüpheli şahıs siber suç işlemekten dolayı tutuklanmıştır. Görülmektedir ki 2007 yılından bu yana siber suçlarla alakalı şüpheli sayısında önemli miktarda artış olmuştur. Ayrıca 2012 yılında işlenen siber suçlarda artış gözlenmekte iken aksine şüpheli sayısında bir azalış söz konusudur.

Tablo-1 ve Tablo-2 değerlendirildiğinde gerek siber suçlar olsun ve gerekse de bu suçları işleyen şüphelilerin sayısı olsun önemli derecede bir artış göze çarpmaktadır. Bu durumun aslında iki nedeni vardır. Bunlar; İstanbul merkezli Bilişim Suçları ve Sistemleri Şube Müdürlüğünün kurulması ve buna bağlı olarak da siber suçlara karşı mücadele eden uzman kolluk birimleri ile personel sayısının artışı

ve 5651 sayılı Kanunun yürürlüğe girmesidir. Bu durum, siber suçlarla mücadele eden hukuki mevzuatların yürürlüğe girmesi ve özel polis birimlerinin kurulması ile suçla mücadelenin etkin hale gelmesi şeklinde de açıklanabilir[40].

2.6.1. Dünyada Siber Suçlar

Bilgisayar teknolojisinin ilk olarak girdiği ülkelerin başında ABD gelmektedir. Buradan hareketle ilk siber suçların da ABD' de ortaya çıktığı gözlemlenmektedir. Çok sayıda siber suçlar ABD' de meydana gelmektedir. Netice itibariyle de ABD bu suçlara hala yürürlükte olan çeşitli kanun maddeleri ile önlem almıştır.

Almanya'da Kıta Avrupası Hukuk Sistemi' ne dayalı olarak siber suçların önlenmesi için birtakım kurallar koymuştur çeşitli kurallar koymuştur (Kurt, 2005).

- Bilgisayar sistemlerine izinsiz bir biçimde girilmesi suretiyle verilerin ele geçirilmesi

- Bilgisayar sistemleri kullanılması ile yapılan sahtekârlık ve dolandırıcılıklar (Değirmenci, 2002).

- Verilerin tamamıyla silinmesi, değiştirilmesi ve bilgisayarların sabotaj edilmesi ile veri aktarım sürecinin engellenmesi

İsviçre ise Federal Ceza Yasası ve Haksız Rekabet yasaları ile siber suçları önleme adına gelişmeler sağlamıştır.

Fransa'da oluşturulan yeni ceza kanunu ile aşağıdaki maddeler suç kavramına dâhil edilmiştir.

- Sisteme yetki dışı erişim ile verilerin tahrip edilmesi, silinmesi, çalınması (Pallı, 2008)

---

[40] (TBD, 2015: 16).

- Banka ve kredi kartlarının kötüye kullanılması (Karagülmez, 2009).

- Çocukların kullanılması suretiyle ya da çocukların görmesini sağlayacak biçimde cinsel içerikli yayınların ya da mesajların yayınlanması (Ünver, 2001).

- Şahsın görüntü ve ses kayıtlarına montaj yapılması suretiyle, kişinin rızası dışında yayınlanması (Kangal, 2001). Bilişim sistemlerini kullanılması suretiyle dolandırıcılık, hırsızlık vb. suçların işlenmesi ve bu suçların örgütlü bir şekilde işlenmesi (Dülger, 2004).

İngiltere siber suçlar için özel kanunlar yapmıştır. Computer Misuse Act Kanunu, Müstehcen Yayınlar Kanunu ve Telekomünikasyon Kanunları içerisine siber suçları dâhil etmiştir (Dülger, 2004).

İtalya, çocukların korunması ve veri güvenliği adına adımlar atmak için aşağıdaki ceza konular hakkında ceza yasaları oluşturmuştur.

- İletişimin engellenmesi ya da yetki dışı olacak bir biçimde dinlenmesi,

- Bilişim sistemleri vasıtasıyla hırsızlık, dolandırıcılık ve kumar oynanmasına olanak verme,

- Sisteme erişimi virüs kullanılarak engelleme,

- Bilişim sistemleri kullanılarak devlet sırlarını açığa vurma.

- Japonya teknolojinin hızla ilerlemesi ile siber suçları yasalarının içine almış fakat veriler değiştirilmediği sürece erişim hakkı vardır.

Rusya G-8 ülkeleri ile yapmış olduğu toplantılarda siber suçlar adına ortak güvenlik ağı oluşturulmasına imza atmıştır. Aşağıdaki yasal düzenlemeler yapılmıştır.

- Bilişim sistemleri kullanılarak pornografik unsurlar barındıran yayınların hukuk dışı yollar kullanılarak çoğaltılması ve yayınlaması.

- Verileri almak amacıyla hukuk dışı sisteme erişim

- İnsan ve çocuk ticaretinin yapılması konularında

İsrail, "bilgisayar kanunu" ile siber suçlarla mücadele etmektedir. Farklı ülkeler ile siber suçlar konusunda ortak çalışmalar yapmaktadır.

Kanada siber suçları genel yasaların içine almıştır. Kanada'da siber suçlar özellikle üzerinde durulan önem taşıyan bir konudur.

2.7. İLGİLİ LİTERATÜR ÇALIŞMASI

Dünyada oluşturulan Haziran 2014 verileri dünya nüfusunu 7,2 milyar olarak düşündüğümüzde bu nüfusun ortalama % 42,3'ü yani 3.035.755.340 kişi interneti günlük yaşamı ve iş hayatında kullanıyor. Türkiye'de ise internet kullanıcı sayısı giderek artmakta ülke nüfusunun % 56'5'i 46.292.850 kişi interneti kullanmaktadır (internetworldstats. com. 2017)

Geçtiğimiz çeyrek asırda büyüme hızı en yüksek olan sektör bilişim sektörüdür. Sınırları bilinmeyen, kaideleri oluşturulamayan, hem demokratik hem de anarşik bir platform olan internet, insanlara kendini ve düşüncesini özgürce, kimliği belli olmadan ifade etmesini sağlamaktadır (Yetim, 2014: 179). İnternet ortamında görüntülü ve sesli iletişim, özel paylaşımlar, çevrimiçi alışveriş vs. gibi birçok şekilde yeni gelişmelere öncülük etmiş, sonuçları bazen olumlu bazen olumsuz yeni alışkanlıklar kazanılmasını sağlamıştır. Siber psikoloji denilen teknolojinin insan davranışını inceleyen bilim dalının doğmasına neden olmuştur (EUROPOL, 2014: 62).

Dünyada her gün 294,3 milyar e-mail yolu ile iletişim, Google'da ise 6,3 milyar arama yapılmakta, Facebook'ta 3,6 milyar mesajlaşma ve Twitter'da 40,9 milyar Tweet paylaşımı yapılmaktadır. Bu yoğunluk içerisinde birçok suç işlenmekte ve bu suçların kontrollü giderek zorlaşmaktadır.

Ülkemizde 2000-2014 yılları arasında çok hızlı bir büyüme yaşayarak %2550 oranında artmıştır. Bu duruma beraberinde ilgili alandaki suç oranının artmasına neden olmuştur. Örneğin 2000, 2001 ile 2002 yıllarında bu alanda kayıtlı suç sayısı

çok düşük iken 2003 sonrası ciddi artışlar görülmüştür. Buradan anladığımız İnternetin yaygınlaşması ile bilinçsiz ve amacı dışında kullanımında yaygınlaşmasına yol açmıştır. Kötü niyetli insanlar internetin sağlamış olduğu tüm kolaylıkları illegal işlerde kullanmaya başlamıştır. 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).

Normal suç zanlılarının izini kaybettirmesi ne kadar zor ise siber suç zanlılarının izini kaybettirmesi bir o kadar kolaydır. Bilişim suçu işleyen zanlılara karşı emniyet güçlerinin etkin bir şekilde mücadele edebilmesi için en az onlar kadar altyapılarının olması gereklidir. Günümüzde siber suçların sayısı hızla artmaktadır. Ancak bu artışa karşılık güvenlik birimlerinde kendini yetiştirmiş eleman sayısı oldukça azdır. Bu sebepten ötürü ki siber suçlarla alakalı kovuşturma sayısı, siber suç sayısından nispeten çok görülmektedir. Bundan dolayı bilişim suçu zanlıları açısından; güvenlik görevlilerinin, suç işlendikten sonra değil de suç işlenmeden önce önlem almaları önem arz etmektedir. Siber suç açısından farkındalık yaratmak bu hususta önemlidir. İnsanların siber suçlar hususunda bilinçli olma düzeyleri, siber suç farkındalığıdır. Yapmış oldukları işin sanal ortamda olmasından dolayı şüpheliler, sonuçları tahmin etmede yetersiz kalmaktadırlar. Bu duruma örnek vermek gerekirse; sosyal paylaşım mecralarında duyarsız bir şekilde paylaşılan mesajların belki de milyonlarca kişi tarafından okunacağı ve ne şekilde anlaşılacağı paylaşan kişi tarafından tahmin edilememektedir. Bu örnekte olduğu gibi sanal ortamda yapılan bir eylemin ne gibi sonuçlar doğuracağı, eylemin muhataplarına karşı ne gibi zararı olacağı şeklindeki hususlar paylaşan kişilerce düşünülmemektedir. İnsanların sanal ortamlarda da bir sorumlulukları vardır ve bu genelde unutulmaktadır. Dijle ve Doğan (2011) tarafından kişilerin siber suçlar açısından farkındalığını ölçmek amacıyla, üniversite öğrencileri ile öğretim görevlileri üzerinde bir araştırma yapmıştır. Bu araştırma neticesinde katılımcıların % 35,6'sının siber suç kavramına yabancı oldukları yani daha önce hiç duymadıkları saptanmıştır. Yine bu araştırmaya göre, katılımcıların %29,6' sı İnternetten film ve

müzik indirmenin suç unsuru teşkil ettiğini bilmediğini ve %42.2' sinin ise yeterli bilgi birikimine sahip olduklarında hackerlik yapabilecekleri neticesine ulaşılmıştır. Bilişim suçlarını işleyenlere baktığımız zaman genel itibariyle 16 - 35 yaş arası kitle göze çarpmaktadır. Daha çok kendini ispat amacı taşıyan ve yasal olup olmadığı hakkında bilgi sahibi olmayan gençler, bu işe daha çok meyillidir. Martin ve Rice (2011)' ın yapmış olduğu bir araştırma neticesinde özellikle de okul çağında genç kişiler sırf kabadayılık egoları için bilgisayarı kötü amaçlar için kullanmaktadır. Bu durum ise toplumda endişelere sebebiyet vermektedir. Bilek (2012) tarafından Türkiye'nin farklı üniversitelerinden BÖTE bölümü öğrencileri üzerinde bilişim teknolojilerini kullanma durumları ile bilişim suçları hususunda bilgi seviyeleri ile tutumlarını ölçmek için bir araştırma yapılmıştır. Araştırma neticesinde katılımcıların % 25' i yakalanmayacağını düşündükleri için bilgisi olsa hackerlik yapacağını beyan etmiştir. Yine aynı araştırmaya göre %34 oranında öğrencinin bilgisayarlarında lisansı olmayan işletim sistemi kullandığı saptanmıştır. Öte yandan bu araştırma açısından en dikkat çekici nokta ise %95 oranında öğrencinin bilişim suçları hususunda bilgilendirilmek istemeleri olmuştur. 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 ulaşılıp yapılan hırsızlık" en ağır bilişim suçları olarak gösterilmiştir. Aynı araştırmada öğretim elemanı, öğrenci gruplarında ki en belirgin algı farklılığı akademik aşırmacılık fiilinde tespit edilmiştir. Akademik aşırmacılık öğretim elemanları için ağır bir bilişim suçu olarak kabul edilmesine rağmen aynı suçun öğrenciler için o kadarda önemsenen 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.

ÜÇÜNCÜ BÖLÜM

3. YÖNTEM

3.1. Araştırma Modeli

"Lise Öğrencilerinin Siber Suç Algı Düzeylerinin Farklı Değişkenler Açısından İncelenmesi (Kırşehir İli Örneği)" isimli bu araştırma, Kırşehir ilinde bulunan liselerde öğrenimlerine devam eden öğrencilerin siber suçlar üzerine farkındalıklarını ortaya koymayı amaçlamaktadır. Ayrıca araştırmada, öğrencilerin siber suçlar ile ilgili görüşlerinin cinsiyet, sınıf, sosyal medya kullanımı ve internet kullanım yılına göre farklılaşıp farklılaşmadığı belirlenmeye çalışılmıştır. Araştırma, nicel bir çalışma olup, genel tarama modeline göre yürütülmüştür.

Betimsel çalışmalarda genellikle tarama yöntemi (survey) kullanılır. Özellikle anket ve mülakat yöntemlerinin araştırmalarda önemli bir yeri vardır (Aslantürk 1999; Karasar 2004). Ankette dayalı araştırmalar niceleyici varsayımlar içerdiği için çoğunlukla istatistiksel olarak değerlendirilir ve elde edilen veriler sayısallaştırılır veya formülize edilirler (Çepni 2001).

3.2. Çalışma Grubu

Bu çalışmanın örneklemini, Kırşehir ili merkezde bulunan 16 lisede öğrenim gören öğrenciler oluşturmaktadır.

3.3. Veri Toplama Araçları

Çalışmada veriler, İLBAŞ (2009)'ın "Bilişim Suçlarının Sosyo-Kültürel Seviyelere Göre Algı Analizi" adlı yüksek lisans tezinde kullanmış olduğu anket ve araştırmacı tarafından geliştirilen "kişisel bilgi formu" ile toplanmıştır. Kullanılacak olan anket formu için gerekli izinler alınmıştır. Anket sorularının herhangi birine cevaplama oranı 0.5 olarak kabul edilmiş ve homojen olmadığı kabul edilerek varyans $\sigma 2 = 0.25$ alınmıştır. Anketin içeriğinde demografik sorular olduğu gibi likert ölçekli sorularda bulunmaktadır. Bu sayede öğrencilerin görüşlerine ulaşmak amaçlanmıştır. Ankette beşli dereceleme ölçeği "en hafif (1)", "hafif (2)", "orta (3)", "ağır (4)", "en ağır (5)" ölçütleri kullanılmıştır. Herhangi bir seçeneği öğrencinin işaretlemesi istenmiştir. Seçenekler 1, 2, 3, 4 ve 5 puanlaması ile derecelendirilmiştir.

DÖRDÜNCÜ BÖLÜM

4. BULGULAR VE YORUM

Bu bölümde araştırmanın başında tespit edilen problemlerin cevaplarına ulaşmak için; lise öğrencilerinden alınan bilgiler istatistiksel olarak değerlendirilmiş ve aşağıdaki bulgular elde edilmiştir.

Tablo 3. Araştırmaya Katılan Öğrencilerin Demografik Özelliklerinin Frekans ve Yüzde Dağılımları

Cinsiyet	**%**
Kadın	54.8
Erkek	45.2
Sınıf	
Lise 1	33.4
Lise 2	34.9
Lise 3	16.5
Lise 4	15.2

Tablo 4. Araştırmaya Katılan Öğrencilerin Teknoloji ve İnternet'e Olan İlgisinin Dağılımı

İnterneti Kullanım Yılları	**%**
1-2 yıl	12
3-4 yıl	24.6
5 yıl üstü	63.4
İnterneti Kullanım Saati	
0-1 saat	25.6
1-2 saat	35.4
3-4 saat	20.4
4 saat üstü	18.6
Sosyal medya kullanımı	
Evet	83
Hayır	17

Araştırmaya katılan öğrencilerin çoğunluğunu kızlar (%54.8) oluşturmaktadır.

Katılımcıların %12'si interneti 1-2 yıl arasında kullandığını, % 24.6'sı 3-4 yıl arasında kullandığını, %63.4'ü ise interneti 5 yıl ve daha uzun süre kullandığını belirtmiştir. Öğrencilerin çoğunluğunun 5 yıl ve üzeri internet kullandıkları söylenebilir.

Çalışmaya katılan 898 öğrenciden %25.6'sının internet kullanımı günde 0-1 saat olur iken, %35.4'ünün 1-2 saat arasında, %20.4'ünün 3-4 saat arasında, % 18.6'sının ise İnternet kullanımı dört saatten fazla olduğu belirlenmiştir. Katılımcıların yarısından fazlasının günde bir saatten fazla internet kullandığı söylenebilir.

Araştırmaya katılan öğrencilere yöneltilen sosyal medya kullanımı hakkındaki soruya katılımcıların %83 'ü evet, % 17'si hayır cevabı vermiştir. Lise öğrencilerinin büyük çoğunluğunun sosyal medya kullandığı söylenebilir.

Yaptığımız bu ankette değişik ülkeler açısından hukuk sistemleri incelendiğinde bilişim suçu kapsamındaki fiillerin kişisel algı seviyesinde suç şiddeti çerçevesinden değerlendirilmesi gayesiyle sorulan soruda 14 madde mevcuttur. Bahsi geçen bu sorular sık rastlanılan bilişim suçu çeşitlerine göre aşağıdaki biçimde gruplanmıştır.

- İnternet üzerinden yapılan yayınlar
- Siber ihlal
- Siber dolandırıcılık, siber hırsızlık
- Kimlik hırsızlığı
- Kişisel bilgilerin korunması
- Korsancılık, plagiarism
- Çocuk pornografisi

Tablo 5. Araştırmaya Katılan Öğrencilerin Siber Suç Algılarına Göre Dağılımı

	En Hafif		Hafif		Orta		Ağır		En ağır	
Madde	**Sayı**	**%**	**Sayı**	**%**	**Sayı**	**%**	**Sayı**	**%**	**Sayı**	**%**
1	126	**14.03**	92	**10.2**	217	**24.1**	113	**12.6**	350	**39.06**
2	277	**30.8**	106	**11.8**	187	**20.8**	154	**17.1**	174	**19.3**
3	76	**8.4**	13	**1.4**	69	**7.6**	136	**15.5**	604	**66.8**
4	14	**1.5**	10	**1.1**	41	**4.5**	262	**29.1**	571	**63.5**
5	15	**1.6**	30	**3.4**	114	**12.7**	152	**16.9**	587	**65.3**
6	19	**2.1**	13	**1.4**	122	**13.5**	244	**27.1**	500	**55.6**
7	66	**7.3**	34	**3.7**	230	**25.6**	255	**28.3**	313	**34.8**
8	125	**13.9**	110	**12.2**	262	**29.1**	199	**22.1**	202	**22.4**
9	20	**2.2**	48	**5.3**	194	**21.6**	291	**32.4**	345	**38.4**
10	11	**1.2**	94	**10.4**	101	**11.3**	96	**10.6**	596	**66.3**
11	17	**1.8**	69	**7.6**	62	**6.9**	52	**5.7**	698	**77.8**
12	14	**1.5**	12	**1.3**	26	**2.8**	129	**14.3**	717	**79.9**
13	19	**2.1**	98	**10.9**	201	**22.3**	278	**30.9**	302	**33.7**
14	176	**19.5**	151	**16.8**	165	**18.3**	143	**15.9**	263	**29.2**

Çocuk pornografisi ile alakalı fotoğraf ve video içeriği bulunan internet sitesi yayınlarının yapılması eylemi, ülkemizde yürürlükte bulunan Türk Ceza Kanunu çerçevesinde siber suçlar açısından en ağır suçu 10 numaralı maddede (Bkz. Ek1) teşkil etmektedir. Soruları yanıtlayan katılımcıların %66,3 gibi büyük bir kısmı bahsi geçen eylemi en ağır suç olarak işaretlemiştir. Çocuk pornografisi suçunun diğer suçlardan ayrışmasının ve daha ağır nitelikte olmasının temel nedenlerinden birisi de son yıllarda basın ve yayın organları vasıtasıyla bu suçun sürekli gündeme gelmesi ve bu suçun uluslararası anlaşmalar çerçevesinde kovuşturmaya tabi tutulmasıdır.

Aynı şekilde sürekli gündeme gelen suçlardan bir diğeri de internet aracılığıyla banka hesap bilgilerinin ele geçirilip hırsızlık suçudur. Sözü edilen bu suçu katılımcıların %66.8'i 3 numaralı maddede (Bkz. Ek1) en ağır suç olarak seçmişler ve çocuk pornografisi suçu kapsamında banka dolandırıcılığından daha ağır niteliği bulunan 11 numaralı "Çocuk pornografisini temsil eden çizim ve animasyonlara yönelik içeriği bulunan İnternet sitesi yayınlarının yapılması" ve 12 numaralı "Çocuk pornografisi konulu içeriği bulunan İnternet sitesi yayınlarına erişilmesi" suçlarından daha hafif bir suç olarak belirlemişlerdir.

Katılımcıların en hafif suç olarak belirlediği "Bir ülke veya devlet aleyhinde yayın yapan bir web sitesinin, bir kişi ya da grup tarafından kapatılması, erişiminin engellenmesi" suçu katılımcılar tarafından en hafif suç olarak 2 numaralı madde (Bkz. Ek1) belirlenmiştir. Bu suç, genel düşüncenin aksine siber ihlal türünde bir suç niteliği taşımaktadır. Bu suç diğer ülkelerin hukuk sisteminde de bir ceza unsuru oluşturan bir suç niteliği olmakla beraber, TCK'nın 243. ve 244. Maddeleri gereğince bir bilişim sistemine yetkisiz olarak girme, bilişim sistemindeki verileri bozma ve bilişim sistemine genel erişimi engelleme suçu çerçevesinde değerlendirilmektedir.

Katılımcıların %19.5 ' i, en hafif suç olarak 14. maddede yer alan (Bkz. Ek1) bilişim sistemindeki verilere yetkisi olmadan girip, haksız erişim sağlayan ancak herhangi bir zarar vermeden sitemden çıkılması eylemi olup, bu suç fiili de siber ihlal kapsamında bir suç olarak tanımlanmaktadır. Ayrıca bu suç, tüm ülkelerin hukuk sistemleri ile ceza kanunlarında genellikle ilk olarak düzenlenen bilişim suçu olma özelliğini taşımaktadır.

Yine %14,03 ile en hafif suç olarak 1.maddede (Bkz. Ek1), bir ülke veya devlet aleyhinde web sitesi yayını yapılması eylemi gösterilmektedir. Bu suç en hafif suçlar arasında üçüncü sırada görülmektedir.

Dikkati çeken bir başka sonuç, akademik aşırmacılık (plagiarism) fiilinin sorulduğu 8. madde (Bkz. Ek1) ye verilen yanıtlardır. Bu soruya katılımcıların %13.9'u akademik aşırmacılık eyleminin en hafif suç olduğuna ilişkin yanıt

vermişlerdir. En hafif suçlar arasında yer alan aşırmacılık eylemi dördüncü sıradadır.

Araştırmaya iştirak eden öğrencilerin %51.66'sı devlet aleyhine web sitesi yayını yapılması sorununa ağır ve çok ağır suç yanıtını vermişlerdir. Bu soruya verilen hafif ve çok hafif cevabı ise %24.2 oranındadır.

Bir kişi ya da grubun, bir devlet yahut ülke adına yayın yapan bir web sitesini kapatması ya da erişimini engellemesi sorusuna %42.6' oranında hafif ve çok hafif yanıtı verilmiştir. Bu yanıt esas olarak bir önceki soruya verilmiş cevabı destekleyici bir niteliğe sahiptir.

Katılımcı öğrencilerin %82.3'si bir kişinin banka hesap bilgilerinin ele geçirilmesi suretiyle yetki dışı para aktarımı sorusuna bu suçun ağır ve çok ağır suç olduğu yönünde karar bildirmişlerdir. Bu orana göre değerlendirme yapıldığında katılımcılar hesap bilgilerinin çalınmasının çok ağır bir suç teşkil edeceğine kanaat getirmişlerdir.

Öğrencilerin %92.62' lik bir bölümü sahte loto, şirket ortaklığı şeklindeki vaatlerle dolandırıcılık yapılması sorusuna bunların ağır nitelikte bir suç teşkil ettiği yanıtını vermişlerdir.

%82,3 oranla öğrenciler kimlik numarası, telefon numarası ve adres bilgileri gibi şahsi bilgilerin web siteleri vasıtasıyla toplanıp üçüncü kişilere servis edilmesi yahut satılması fiiline ağır suç olduğu yönünde yanıt vermişlerdir.

%82.7' lik bir oranla şahsi bir bilgisayara erişip şahsi bilgilerin, dosyaların, dokümanların ve belgelerin çalınması ise öğrenciler tarafından yine ağır bir suç şeklinde değerlendirilmiştir.

Öte yandan bilgisayarda donanımsal olarak fiziksel nitelikteki bir zarara ise öğrencilerin %53.2'si ağır suç, % 36.6'sı ise orta ve hafif suç yanıtını vermişlerdir.

Yazılım üzerinde değişiklik yapılması suretiyle hak iddia edilmesi konusunda öğrencilerin vermiş oldukları cevaplar ise %70.9 ile ağır ve çok ağır suç, %29.1 oranı ile de orta ve hafif suç şeklindedir.

İnternetten alınan bir makale yahut raporun kaynak gösterilmeden kullanılması hususuna ise katılımcıların vermiş oldukları cevaplara göre bu suç, orta ağırlıkta bir suç teşkil etmektedir. Öğrenciler ise bu soruya %44.5 oranında ağır ve çok ağır cevabı verirken, %55.2'si ise hafif ve orta suç cevabını vermiştir.

Çocuk pornografisiyle alakalı fotoğraf ya da video gibi içerikleri barındıran web sitesi yayınlarının yapılması sorusuna ise öğrencilerin %76.9' u ağır ve çok ağır cevabını vermiş, %22.9'u ise bu suçu orta ya da hafif şeklinde yanıtlamıştır.

Ayrıca öğrencilerin %94.2'lik bir kısmı çocuk pornografisi içeriklerini barındıran web sitesi yayınlarına erişilmesi hususuna verdikleri yanıt ise bu suçun ağır ve çok ağır nitelikte bir suç kapsamına girdiği yönündedir. Bu suç öğrencilerin en yüksek ağırlıkta suç gördüğü hususdur.

Diğer yandan bilgisayar sistemi için zararlı kodlar hazırlanarak gönderilmesi sorusuna ise öğrencilerin %64.6'ü ağır ve çok ağır yanıtını vermişlerdir. %35.4'ü ise hafif ve orta yanıtını verenlerden oluşmaktadır.

Öğrenciler, bir bilişim sistemine girilip herhangi bir şekilde zarar vermeden çıkılması sorusuna ise zarar teşkil etmediği için hafif ve orta nitelikte bir suç olduğu yanıtını vermişlerdir.

Şahısların kimlik, telefon ve adres bilgileri gibi verilerin internet siteleri vasıtasıyla toplanıp üçüncü şahıslara servis edilmesi ya da satılması sorusuna kadın katılımcıların %70.3' ü en ağır suç yanıtını vermişler, erkek katılımcıların ise %59.3'ü bu soruya tıpkı kadın katılımcılar gibi en ağır suç olduğunu belirtmişlerdir.

Öğrencilerin Sınıflarına Göre Suç Algısı Farklılaşması

1. Bir ülke veya devlet aleyhinde web sitesi yayını yapılması

Eğitim Durumu	N	Ortalama	Std.Sapma	f-değeri	p-değeri
1.Sınıf	245	7.9224490	1.35126918		
2.Sınıf	168	8.0297619	1.23047917		
3".Sınıf	297	7.9831650	1.36673292	.223	.880
4.Sınıf	188	7.9734043	1.36194855		

2. Bir ülke veya devlet aleyhinde yayın yapan bir web sitesinin, bir kişi ya da grup tarafından kapatılması, erişiminin engellenmesi

Eğitim Durumu	N	Ortalama	Std.Sapma	f-değeri	p-değeri
1.Sınıf	245	8.0571429	1.25645872		
2.Sınıf	168	7.6845238	1.45651492		
3.Sınıf	297	8.1885522	1.17611517	.792	.664
4.Sınıf	188	8.2074468	1.23433408		

3. Bir banka müşterilerinin hesap bilgileri elde edilerek yetkisiz para transferi yapılması

Eğitim Durumu	N	Ortalama	Std. Sapma	f-değeri	p-değeri
1.Sınıf	245	8.1265306	1.35058814		
2.Sınıf	168	7.6666667	1.50315702		
3.Sınıf	297	8.0976431	1.15689524	.982	.072
4.Sınıf	188	7.9468085	1.33137395		

4. Sahte Loto, şirket ortaklığı gibi tuzaklarla dolandırıcılık Yapılması

Eğitim Durumu	N	Ortalama	Std. Sapma	f-değeri	p-değeri
1.Sınıf	245	8.1346939	1.17095152		
2.Sınıf	168	7.9345238	1.30011460		
3.Sınıf	297	7.8552189	1.33656277	2.431	.064
4.Sınıf	188	7.8670213	1.40601369		

5. Kimlik numarası, telefon numarası ve adres gibi kişisel bilgilerin web siteleri aracılığıyla toplanıp üçüncü şahıslara sunulması veya satılması

Eğitim Durumu	N	Ortalama	Std. sapma	f-değeri	p-değeri
1.Sınıf	245	8.0244898	1.26402470		
2.Sınıf	168	7.9464286	1.39828350		
3.Sınıf	297	8.1447811	1.26647843	.886	.448
4.Sınıf	188	8.0531915	1.38260408		

6. Bir kişisel bilgisayara uzaktan müdahale ederek kişisel dosya, belge ve dokümanların elde edilmesi

Eğitim Durumu	N	Ortalama	Std.Sapma	f-değeri	p-değeri
1.Sınıf	245	7.9877551	1.40689646		
2.Sınıf	168	7.8750000	1.37203682		
3.Sınıf	297	8.1919192	1.21374533	2.473	.060
4.Sınıf	188	8.0053191	1.15854113		

7. Bilgisayar donanımlarına kişisel zarar verilmesi

Eğitim Durumu	N	Ortalama	Std.Sapma	f-değeri	p-değeri
1.Sınıf	245	7.7102041	1.43496229		
2.Sınıf	168	7.9940476	1.27385982		
3.Sınıf	297	8.0841751	1.29564711	3.805	.091
4.Sınıf	188	8.0212766	1.37182281		

8. İnternette bulunan bir makale veya raporun referans gösterilmeden kullanılması

Eğitim Durumu	N	Ortalama	Std.Sapma	f-değeri	p-değeri
1.Sınıf	245	8.1346939	1.26191875		
2.Sınıf	168	7.7202381	1.46383793		
3.Sınıf	297	7.9898990	1.35188769	.958	.078
4.Sınıf	188	8.0531915	1.38260408		

9. Bir başkası tarafından hazırlanan bilgisayar yazılımlarında değişiklik yaparak yazılım üzerinde hak iddia edilmesi

Eğitim Durumu	N	Ortalama	Std. Sapma	f-değeri	p-değeri
1.Sınıf	245	7.8448980	1.33996899		
2.Sınıf	168	7.8809524	1.38343287		
3.Sınıf	297	8.1346801	1.18921504	2.560	.054
4.Sınıf	188	7.9680851	1.39097263		

10. Çocuk pornografisi konulu fotoğraf ve video içeriği bulunan İnternet sitesi yayınlarının yapılması

Eğitim Durumu	N	Ortalama	Std. Sapma	f-değeri	p-değeri
1.Sınıf	245	7.9265306	1.41229605		
2.Sınıf	168	7.9583333	1.30569534		
3.Sınıf	297	8.2323232	1.14338535	.751	.879
4.Sınıf	188	7.8617021	1.35710500		

11. Çocuk pornografisini temsil eden çizim ve animasyonlara yönelik içeriği bulunan İnternet sitesi yayınlarının yapılması

Eğitim Durumu	N	Ortalama	Std. Sapma	f-değeri	p-değeri
1.Sınıf	245	8.0734694	1.21917325		
2.Sınıf	168	7.8214286	1.39855113		
3.Sınıf	297	7.9865320	1.34308304	1.784	.149
4.Sınıf	188	8.1117021	1.24241927		

12. Çocuk pornografisi konulu içeriği bulunan İnternet sitesi yayınlarına erişilmesi

Eğitim Durumu	N	Ortalama	Std.Sapma	f-değeri	p-değeri
1.Sınıf	245	8.0734694	1.21917325		
2.Sınıf	168	7.8214286	1.39855113		
3.Sınıf	297	7.9865320	1.34308304	1.894	.156
4.Sınıf	188	8.1117021	1.24241927		

13. Bilgisayar sistemine zarar veren kodlar yazılması ve yayınlanması

Eğitim Durumu	N	Ortalama	Std.Sapma	f-değeri	p-değeri
1.Sınıf	245	7.8408163	1.34406991		
2.Sınıf	168	7.9821429	1.31537756		
3.Sınıf	297	8.1616162	1.19718479	.754	.031
4.Sınıf	188	8.0372340	1.26816083		

14. Bir bilişim sistemindeki verilere yetkisiz olarak erişilip her hangi bir zarar verilmeden sistemden çıkılması

Eğitim Durumu	N	Ortalama	Std. Sapma	f-değeri	p-değeri
1.Sınıf	245	7.8000000	1.43606932		
2.Sınıf	168	8.0476190	1.35721414		
3.Sınıf	297	7.8989899	1.38886705	1.077	.058
4.Sınıf	188	7.9521277	1.49967759		

Anova Testi analizi sonucunda katılımcıların sorudaki siber suç algılarının sınıflara göre istatistiksel olarak anlamlı bir şekilde farklılaştığı 13. anket sorusunda ortaya çıkmaktadır. Yapılan analiz sonucunda 13. Soru'da p=0.031 bulunmuş bu sonuç neticesinde (p<.050) sınıf farklılığının öğrencilerin 13. soruda siber suç algı durumlarına etki ettiği anlaşılmıştır. Diğer anket sorularında herhangi bir anlamlı farklılık olmadığı anlaşılmaktadır.

Öğrencilerin Cinsiyetlerine Göre Suç Algısı Farklılaşması

1. Bir ülke veya devlet aleyhinde web sitesi yayını yapılması

Cinsiyet	N	Ortalama	Std.Sapma	f-değeri	p-değeri
Kadın	492	8.1524390	1.20890035	.998	.114
Erkek	406	7.8916256	1.36375618		

2. Bir ülke veya devlet aleyhinde yayın yapan bir web sitesinin, bir kişi ya da grup tarafından kapatılması, erişiminin engellenmesi

Cinsiyet	N	Ortalama	Std. Sapma	f-değeri	p-değeri
Kadın	492	7.9857724	1.30086952	3.368	.067
Erkek	406	7.8768473	1.39119130		

3. Bir banka müşterilerinin hesap bilgileri elde edilerek yetkisiz para transferi yapılması

Cinsiyet	N	Ortalama	Std.Sapma	f-değeri	p-değeri
Kadın	492	7.9024390	1.32600273	1.446	.229
Erkek	406	7.7980296	1.34571879		

4. Sahte Loto, şirket ortaklığı gibi tuzaklarla dolandırıcılık Yapılması

Cinsiyet	N	Ortalama	Std. Sapma	f-değeri	p-değeri
Kadın	492	7.9857724	1.30086952	3.368	.067
Erkek	406	7.8768473	1.39119130		

5. Kimlik numarası, telefon numarası ve adres gibi kişisel bilgilerin web siteleri aracılığıyla toplanıp üçüncü şahıslara sunulması veya satılması

Cinsiyet	N	Ortalama	Std.Sapma	f-değeri	p-değeri
Kadın	492	7.8414634	1.37894714	5.615	.791
Erkek	406	7.8177340	1.28285206		

6. Bir kişisel bilgisayara uzaktan müdahale ederek kişisel dosya, belge ve dokümanların elde edilmesi

Cinsiyet	N	Ortalama	Std. Sapma	f-değeri	p-değeri
Kadın	492	7.9857724	1.33791674	3.354	.555
Erkek	406	8.0369458	1.23772572		

7. Bilgisayar donanımlarına kişisel zarar verilmesi

Cinsiyet	N	Ortalama	Std. Sapma	f-değeri	p-değeri
Kadın	492	7.7784553	1.38279479	1.364	.106
Erkek	406	7.6231527	1.48684965		

8. İnternette bulunan bir makale veya raporun referans gösterilmeden kullanılması

Cinsiyet	N	Ortalama	Std.Sapma	f-değeri	p-değeri
Kadın	492	7.7642276	1.37674193	2.760	.097
Erkek	406	7.7906404	1.47171222		

9. Bir başkası tarafından hazırlanan bilgisayar yazılımlarında değişiklik yaparak yazılım üzerinde hak iddia edilmesi

Cinsiyet	N	Ortalama	Std.Sapma	f-değeri	p-değeri
Kadın	492	7.7296748	1.30723098	2.805	.284
Erkek	406	7.7315271	1.44507375		

10. Çocuk pornografisi konulu fotoğraf ve video içeriği bulunan İnternet sitesi yayınlarının yapılması

Cinsiyet	N	Ortalama	Std.Sapma	f-değeri	p-değeri
Kadın	492	7.6768293	1.41249577	3.250	.047
Erkek	406	7.7561576	1.48145708		

11. Çocuk pornografisini temsil eden çizim ve animasyonlara yönelik içeriği bulunan İnternet sitesi yayınlarının yapılması

Cinsiyet	N	Ortalama	Std.Sapma	f-değeri	p-değeri
Kadın	492	7.9857724	1.30086952	3.368	.041
Erkek	406	7.8768473	1.39119130		

12. Çocuk pornografisi konulu içeriği bulunan İnternet sitesi yayınlarına erişilmesi

Cinsiyet	N	Ortalama	Std.Sapma	f-değeri	p-değeri
Kadın	492	7.9857724	1.33791674	2.354	.241
Erkek	406	8.0369458	1.23772572		

13. Bilgisayar sistemine zarar veren kodlar yazılması ve yayınlanması

Cinsiyet	N	Ortalama	Std.Sapma	f-değeri	p-değeri
Kadın	492	7.4491870	1.58257420	2.042	.245
Erkek	406	8.2125000	1.04678939		

14. Bir bilişim sistemindeki verilere yetkisiz olarak erişilip her hangi bir zarar verilmeden sistemden çıkılması

Cinsiyet	N	Ortalama	Std. Sapma	f-değeri	p-değeri
Kadın	492	7.3882114	1.50684225	.887	.074
Erkek	406	8.4437500	.81711224		

Yapılan analiz sonucunda 10. ve 11. sorular dışında cinsiyet farklılığının verilen cevaplara anlamlı bir farklılık oluşturmadığı görülmüştür. (p>.050) 10. ve 11. sorularda ise p<0.050 olduğundan bu sorularda cinsiyetin önemli bir yer teşkil ettiği anlaşılmaktadır. Çocuk pornografisi ile site yayınları yapılması ve bu yayınlara ulaşılması hakkındaki sorulara verilen cevaplar arasında kadın ve erkek katılımcılar arasında anlamlı bir farklılık vardır.

Kişilerin bilgisayarına uzaktan müdahale edilmek suretiyle kişisel dosya, belge ve dokümanların ele geçirilmesine yönelik olarak kadın katılımcıların %46.1'i bu durumun en ağır suç olarak nitelenmesi gerektiğini belirtirken, erkek katılımcıların %67.2'ü bu davranışı ağır suç şeklinde tanımlamıştır.

Çocuk pornografisi hususunda kadın katılımcıların %68.6'sı, bunun en ağır suç olduğu yönünde belirlenmesi gerektiği yönünde görüş bildirmiş, erkek katılımcıların ise %52.4'ü bunun en ağır suç olduğunu belirtmişlerdir. Aynı eylem erkek katılımcıların %20.2' lik kısmı tarafından orta, hafif ve en hafif suç olarak algılanmış olup bu oran kadın katılımcılarda ise %29.9' dur.

Çocuk pornografisini barındıran internet sitesi yayınlarına erişilmesi eylemini %83.1'lik oranla kadın katılımcılar en ağır suç şeklinde işaretlemiş olup; bu oran erkek katılımcılarda ise %75.8' dir. Öte yandan çocuk pornografisini barındıran internet yayını yapma eylemini ağır ve en ağır suç şeklinde belirleyen kadın katılımcıların oranı %94.4 iken bu oran erkek katılımcılarda ise %93.7' dir.

Öğrenciler, bilgisayar sistemlerine zarar veren yıkıcı suçlar (virüs, trojan) konusunda tespit edilmiştir. Virüs, trojan vs. aracılığıyla bilgisayar sistemine zarar veren kodlar yazmak ve yayınlamak ile alakalı soruya en ağır suç olarak bakan kadın katılımcıların oranı % 40.0 iken; erkek katılımcılarda söz konusu oran %25.8' dir.

İnternet Kullanım Yılına Göre Suç Algısı Farklılaşması

1. Bir ülke veya devlet aleyhinde web sitesi yayını yapılması

İnternet kullanım yılı	N	Ortalama	Std. Sapma	f-değeri	p-değeri
1-2	143	7.9370629	1.40028560	.745	.447
3-4	304	7.6414474	1.46906243		
5-6	150	7.9666667	1.24467546		
7-8	105	8.8000000	.57845949		
9-10	100	8.4400000	.78263993		
10+	96	7.6979167	1.47341202		

2. Bir ülke veya devlet aleyhinde yayın yapan bir web sitesinin, bir kişi ya da grup tarafından kapatılması, erişiminin engellenmesi

İnternet kullanım yılı	N	Ortalama	Std. Sapma	f-değeri	p-değeri
1-2	143	8.1118881	1.29519641	.541	.212
3-4	304	7.8750000	1.29386723		
5-6	150	7.6866667	1.46152750		
7-8	105	8.8952381	.51746069		
9-10	100	8.3800000	.89645768		
10+	96	7.9270833	1.37070701		

3. Bir banka müşterilerinin hesap bilgileri elde edilerek yetkisiz para transferi yapılması

İnternet kullanım yılı	N	Ortalama	Std Sapma	f-değeri	p-değeri
1-2	143	8.1328671	1.35956581	.614	.318
3-4	304	7.7368421	1.33120379		
5-6	150	7.6333333	1.51243910		
7-8	105	8.7619048	.59684764		
9-10	100	8.5000000	.95874497		
10+	96	7.7916667	1.35271008		

4. Sahte Loto, şirket ortaklığı gibi tuzaklarla dolandırıcılık yapılması

İnternet kullanım yılı	N	Ortalama	Std. Sapma	f-değeri	p-değeri
1-2	143	8.1398601	1.27047401	1.210	.159
3-4	304	7.5756579	1.37428033		
5-6	150	7.8266667	1.32475991		
7-8	105	8.7904762	.47424511		
9-10	100	8.4900000	.79766072		
10+	96	7.5520833	1.48586173		

5. Kimlik numarası, telefon numarası ve adres gibi kişisel bilgilerin web siteleri aracılığıyla toplanıp üçüncü şahıslara sunulması veya satılması

İnternet kullanım yılı	N	Ortalama	Std. Sapma	f-değeri	p-değeri
1-2	143	8.1048951	1.24308389	.865	.175
3-4	304	7.7664474	1.44699274		
5-6	150	7.9200000	1.41193380		
7-8	105	8.8476190	.55089006		
9-10	100	8.4300000	.79461572		
10+	96	7.8541667	1.43621701		

6. Bir kişisel bilgisayara uzaktan müdahale ederek kişisel dosya, belge ve dokümanların elde edilmesi

İnternet kullanım yılı	N	Ortalama	Std. Sapma	f-değeri	p-değeri
1-2	143	8.0559441	1.40309629	.615	.125
3-4	304	7.8519737	1.35014828		
5-6	150	7.7933333	1.39171405		
7-8	105	8.7047619	.61899126		
9-10	100	8.4800000	.79747075		
10+	96	7.7916667	1.38348657		

7. Bilgisayar donanımlarına kişisel zarar verilmesi

İnternet kullanım yılı	N	Ortalama	Std. Sapma	f-değeri	p-değeri
1-2	143	7.7272727	1.45438539	.417	.088
3-4	304	7.6776316	1.45380790		
5-6	150	7.9266667	1.29063049		
7-8	105	8.8380952	.59036836		
9-10	100	8.3700000	.86052603		
10+	96	7.7916667	1.49325971		

8. İnternette bulunan bir makale veya raporun referans gösterilmeden kullanılması

İnternet kullanım yılı	N	Ortalama	Std. Sapma	f-değeri	p-değeri
1-2	143	8.1468531	1.30523346	.457	.089
3-4	304	7.7105263	1.40311572		
5-6	150	7.7200000	1.47060687		
7-8	105	8.7619048	.59684764		
9-10	100	8.4900000	.89324061		
10+	96	7.7083333	1.46479146		

9. Bir başkası tarafından hazırlanan bilgisayar yazılımlarında değişiklik yaparak yazılım üzerinde hak iddia edilmesi

İnternet kullanım yılı	N	Ortalama	Std. Sapma	f-değeri	p-değeri
1-2	143	7.8391608	1.36686312	.587	.047
3-4	304	7.7500000	1.38711658		
5-6	150	7.7866667	1.39792112		
7-8	105	8.8285714	.56256868		
9-10	100	8.4100000	.84201538		
10+	96	7.7812500	1.40077516		

10. Çocuk pornografisi konulu fotoğraf ve video içeriği bulunan İnternet sitesi yayınlarının yapılması

İnternet kullanım yılı	N	Ortalama	Std. Sapma	f-değeri	p-değeri
1-2	143	8.0000000	1.41918445	2.782	.039
3-4	304	7.7927632	1.41181259		
5-6	150	7.8666667	1.32941258		
7-8	105	8.6952381	.66684979		
9-10	100	8.4600000	.78392950		
10+	96	7.8125000	1.34800047		

11. Çocuk pornografisini temsil eden çizim ve animasyonlara yönelik içeriği bulunan İnternet sitesi yayınlarının yapılması

İnternet kullanım yılı	N	Ortalama	Std. Sapma	f-değeri	p-değeri
1-2	143	7.8811189	1.41166923	2.965	.037
3-4	304	7.7500000	1.47922913		
5-6	150	7.7466667	1.46175709		
7-8	105	8.6952381	1.02959859		
9-10	100	8.2600000	.92790630		
10+	96	7.8541667	1.43621701		

12. Çocuk pornografisi konulu içeriği bulunan İnternet sitesi yayınlarına erişilmesi

İnternet kullanım yılı	N	Ortalama	Std. Sapma	f-değeri	p-değeri
1-2	143	8.1188811	1.27538732	3.457	.046
3-4	304	7.7467105	1.32940433		
5-6	150	7.8000000	1.40469013		
7-8	105	8.8285714	.56256868		
9-10	100	8.4000000	.89893315		

10+	96	7.6666667	1.52637628		

13. Bir bilişim sistemindeki verilere yetkisiz olarak erişilip her hangi bir zarar verilmeden sistemden çıkılması

İnternet kullanım yılı	**N**	**Ortalama**	**Std. Sapma**	**f-değeri**	**p-değeri**
1-2	143	7.8251748	1.36513264	.814	.136
3-4	304	7.7828947	1.35421485		
5-6	150	7.9466667	1.32496254		
7-8	105	8.7809524	.58803703		
9-10	100	8.4300000	.79461572		
10+	96	7.8645833	1.39638474		

14. Bilgisayar sistemine zarar veren kodlar yazılması ve yayınlanması

İnternet kullanım yılı	**N**	**Ortalama**	**Std. Sapma**	**f-değeri**	**p-değeri**
1-2	143	7.8881119	1.40474495	1.025	.042
3-4	304	7.5328947	1.53686391		
5-6	150	7.9866667	1.38538230		
7-8	105	8.8476190	.71764777		
9-10	100	8.3700000	.88369061		
10+	96	7.5208333	1.53540097		

İnternet kullanım yılına ait Anova Testi sonuçlarına göre 9. 10. 11. 12. ve 14. sorular dışında kalan diğer sorular arasında verilen cevapların anlamlı bir farklılık taşımadığı görülmektedir. Fakat bahsi geçen bu beş soru için sonuçlara bakıldığında internet kullanım yılları ve anket sorularına verdikleri cevaplar arasında anlamlı bir farklılık olduğu görülmektedir. ($p<0.050$).

Sosyal Medya Kullanımına Göre Suç Algısı Farklılaşması

1. Bir ülke veya devlet aleyhinde web sitesi yayını yapılması

Sosyal medya kullanımı	N	Ortalama	Std. Sapma	f-değeri	p-değeri
Evet	740	8.0662162	1.33939750	.954	.066
Hayır	158	7.8860759	.99664842		

2. Bir ülke veya devlet aleyhinde yayın yapan bir web sitesinin, bir kişi ya da grup tarafından kapatılması, erişiminin engellenmesi

Sosyal medya kullanımı	N	Ortalama	Std. Sapma	f-değeri	p-değeri
Evet	740	7.9378378	1.36014235	1.057	.089
Hayır	158	7.6962025	1.21931828		

3. Bir banka müşterilerinin hesap bilgileri elde edilerek yetkisiz para transferi yapılması

Sosyal medya kullanımı	N	Ortalama	Std. Sapma	f-değeri	p-değeri
Evet	740	7.9081081	1.37331585	.992	.093
Hayır	158	7.6075949	1.11066310		

4. Sahte Loto, şirket ortaklığı gibi tuzaklarla dolandırıcılık yapılması

Sosyal medya kullanımı	N	Ortalama	Std. Sapma	f-değeri	p-değeri
Evet	740	7.9918919	1.37341438	1.209	.260
Hayır	158	7.6772152	1.15801822		

5. Kimlik numarası, telefon numarası ve adres gibi kişisel bilgilerin web siteleri aracılığıyla toplanıp üçüncü şahıslara sunulması veya satılması

Sosyal medya kullanımı	N	Ortalama	Std. Sapma	f-değeri	p-değeri
Evet	740	7.8972973	1.35967171	2.928	.087
Hayır	158	7.5189873	1.17143017		

6. Bir kişisel bilgisayara uzaktan müdahale ederek kişisel dosya, belge ve dokümanların elde edilmesi

Sosyal medya kullanımı	N	Ortalama	Std. Sapma	f-değeri	p-değeri
Evet	740	8.0513514	1.32226108	2.532	.114
Hayır	158	7.8101266	1.12952218		

7. Bilgisayar donanımlarına kişisel zarar verilmesi

Sosyal medya kullanımı	N	Ortalama	Std. Sapma	f-değeri	p-değeri
Evet	740	7.7770270	1.47243939	2.471	.235
Hayır	158	7.3860759	1.17687205		

8. İnternette bulunan bir makale veya raporun referans gösterilmeden kullanılması

Sosyal medya kullanımı	N	Ortalama	Std. Sapma	f-değeri	p-değeri
Evet	740	7.8229730	1.43878682	.578	.447
Hayır	158	7.5569620	1.30892902		

9. Bir başkası tarafından hazırlanan bilgisayar yazılımlarında değişiklik yaparak yazılım üzerinde hak iddia edilmesi

Sosyal medya kullanımı	N	Ortalama	Std. Sapma	f-değeri	p-değeri
Evet	740	7.7864865	1.38826751	1.114	.291
Hayır	158	7.4683544	1.25515947		

10. Çocuk pornografisi konulu fotoğraf ve video içeriği bulunan İnternet sitesi yayınlarının yapılması

Sosyal medya kullanımı	N	Ortalama	Std. Sapma	f-değeri	p-değeri
Evet	740	7.7662162	1.46615189	2.736	.098
Hayır	158	7.4620253	1.30962180		

11. Çocuk pornografisini temsil eden çizim ve animasyonlara yönelik içeriği bulunan İnternet sitesi yayınlarının yapılması

Sosyal medya kullanımı	N	Ortalama	Std. Sapma	f-değeri	p-değeri
Evet	740	7.9918919	1.37341438	1.269	.260
Hayır	158	7.6772152	1.15801822		

12. Çocuk pornografisi konulu içeriği bulunan İnternet sitesi yayınlarına erişilmesi

Sosyal medya kullanımı	N	Ortalama	Std. Sapma	f-değeri	p-değeri
Evet	740	8.0513514	1.32226108	2.535	.112
Hayır	158	7.8101266	1.12952218		

13. Bir bilişim sistemindeki verilere yetkisiz olarak erişilip her hangi bir zarar verilmeden sistemden çıkılması

Sosyal medya kullanımı	N	Ortalama	Std. Sapma	f-değeri	p-değeri
Evet	740	7.8418919	1.46889322	1.874	.077
Hayır	158	8.0000000	1.17294338		

14. Bilgisayar sistemine zarar veren kodlar yazılması ve yayınlanması

Sosyal medya kullanımı	N	Ortalama	Std. Sapma	f-değeri	p-değeri
Evet	740	7.9013514	1.39969001	1.982	.102
Hayır	158	8.0000000	1.14547017		

Sosyal medya kullanımı etkeni için yapılan t testinde sosyal medya kullanımına evet veya hayır diye cevap veren katılımcıların vermiş oldukları cevaplar arasında herhangi bir anlamlı farkındalığa rastlanmamıştır.

BEŞİNCİ BÖLÜM

5. SONUÇ VE TARTIŞMA

Araştırmaya katılan öğrencilerin cinsiyet farklılıklarının siber suç algı düzeylerine etkisi yapılan t testi ile incelenmiştir. Analiz sonucunda kız öğrencilerin kişisel bilgiler ve müstehcenlik konusunda erkek öğrencilere göre suç algı düzeyinin yüksek olduğu görülmektedir. Buradan hareketle kadınların erkeklere göre kişisel bilgilerin saklanması noktasında daha duyarlı oldukları ortaya çıkmaktadır. Ayrıca müstehcen içerik barındıran web sitelerinin varlığı ve bunlara erişim yapılmasını da daha ağır suç olarak gören kadınların farkındalıkları erkeklere oranla daha yüksektir. Bu durum cinsiyet değişikliğinin siber suçlar üzerinde önemli bir etkisinin olduğunu göstermektedir.

Öğrencilerin devam etmekte oldukları sınıflarına göre yapılan Anova Testine göre sınıflar arasında sadece 13.soruda anlamlı bir farklılık olduğu, diğer sorularda ise siber suç algı düzeylerinde anlamlı bir farklılık bulunmadığı tespit edilmiştir. Katılımcıların okudukları sınıflara göre siber suçlara olan bilgi düzeylerinde farklılık olduğu yapılan anket değerlendirmelerinde görülmektedir.

Öğrencilerin internet kullanım yılları ve siber suç algıları arasında bir bağ olup olmadığını analiz etmek amaçlı uygulanan Anova Testinde öğrencilerin belirli sorularda internet kullanım yıllarının vermiş oldukları cevaplara etki ettiğini söyleyebiliriz. 1-2 yıl internet kullanan öğrencilerin siber suç algısı 3-4 ve daha fazla yıl internet kullanan öğrencilere göre düşük düzeydedir. Bu iki grup arasında anlamlı bir farklılık bulunmaktadır. Katılımcıların internet kullanım yılları arttıkça siber suçlara bulaşma riskleri de artmaktadır. Bu durum anket sorularına verilen cevaplar karşılaştırıldığında görülmektedir. Öğrencilerin internet kullanım yıllarına bakıldığında erken yaşta internet kullananların çok fazla olduğu görülmektedir. Bu duruma bakıldığında öğrencilerin çocuk yaşta farkında olmadan suça bulaşabileceği de ortaya çıkmaktadır.

Sosyal medya kullanan öğrenciler ile kullanmayan öğrencilerin vermiş oldukları cevapları t testi analizi ile karşılaştırdığımızda anlamlı bir farklılık ortaya

çıkmamaktadır. Bu durum bize sosyal medya kullanımının siber suç algısı üzerinde bir etken olmadığını göstermektedir.

Anket değerlendirilmesi çalışmamızın sonucunda lise öğrencilerinin en çok kişisel bilgilerin çalınması, çocuk pornografisi siteleri yayınlanması ve erişimi, banka hesap bilgilerinin ele geçirilmesi suçları hakkında bilinçli oldukları ve bu tür sorulara ağır suç olarak cevap verdikleri, akademik aşırmacılık fiilini suç olarak görmedikleri ortaya çıkmıştır. Çıkan bu sonuç İlbaş (2009) tarafından yapılan araştırma sonuçlarıyla benzerlik göstermektedir. Bu çalışmada katılımcılar sırayla "çocuk pornografisi" ve "bilgisayar aracılığıyla banka hesaplarına ulaşılıp yapılan hırsızlık" en ağır bilişim suçları olarak göstermişlerdir. Aynı araştırmada akademik aşırmacılık eyleminde, akademisyen ve öğrenciler arasındaki algı farklılığı ortaya konulmuştur. Akademisyenler açısından akademik aşırmacılık ciddi bir bilişim suçu iken öğrenciler açısından o kadar önemli değildir.

Yapılan analiz neticesinde en hafif suçların siber ihlali eylemi, internet aracılığıyla makale, rapor çalınması ya da şahsi bilgisayara bir şekilde ulaşılıp verileri değiştirmeksizin geri çıkılması olduğu belirlenmiştir. Bu konudaki algı eksikliği ile alakalı Türkoğlu, Özdemir, Kalkan, Varol ve Tokdemir (2013)'in üniversite ve lise öğrencileri üzerinde yaptıkları bir araştırmada; lise öğrencilerinin % 21'lik bölümünün, üniversite öğrencilerinin ise % 11'lik bölümünün bilişim suçlarıyla alakalı herhangi bir bilgiye sahip olmadıkları saptanmıştır. Dijle ve Doğan (2011) tarafından benzer bir araştırma yapılmıştır. Üniversite öğrencileri ve öğretim görevlilerinin katıldığı bu araştırmaya göre katılımcıların %35,6' sının siber suçu ilk defa duyduklarını, %29.6'sının İnternet aracılığıyla film ve müzik gibi dosyaları indirmenin suç unsuru teşkil ettiğini bilmediğini, %42.2' sinin yeterli miktarda bilgi ve birikime sahip olduğunda hackerlik yapabilecekleri neticesine ulaşmışlardır.

Araştırmaya katılan öğrenciler müstehcen içerikli internet sitesi yayını yapılması davranışını %66.3 ile en ağır ikinci suç olarak belirtmişlerdir. Suçun farklı bir boyutu olan müstehcen çizim ve animasyonların yayınlanması ve müstehcen yayın yapan sitelere erişim davranışı ise birinci en ağır suç olarak belirtilmiştir. Analizlerin cinsiyete göre dağılımı değerlendirilirse müstehcen yayınlarına erişme

filinde kadın katılımcılar erkelere göre %7.3 daha fazla en ağır suç olarak seçim yapmıştır. Müstehcen çizim ve animasyon yapan sitelerin yayınlanması sorusunda ise kadınlar erkelere oranla %16.2 daha fazla en ağır suç olarak seçim yapmıştır. Kadın katılımcılar müstehcenlik konusunda erkelere oranla daha duyarlı ve bilinçli olduğu görülmektedir. Araştırmaya katılan öğrencilerin bir diğer en ağır suç saydığı yüksek oran ise banka hesap bilgilerinin elde edilmesi konusundadır. Bu konuda öğrencilerin algılarının daha çok bu konuda suç işlenmesi ve medya kuruluşları tarafından sürekli uyarı yapılmasının etkili olduğu ortaya çıkmaktadır.

Yapılan analiz sonucunda siber ihlal fiili, internet yolu ile makale, rapor çalınması veya bilgisayarlara erişim yapıp bilgi değişimi olmadan geri çıkılması, bir devlet aleyhinde web sitesi yayını yapılması, yine bir ülke ya da devlet aleyhinde yapılan web sitesinin bir kişi veya gruplar tarafından kapatılması suçları en hafif suçlar arasında görülmektedir. Ülkemizin bu konudaki suçlar hakkında daha fazla bilgilendirici çalışmalar yapması gerekmektedir. Bu konudaki algı eksikliği fark edilmiştir.

ALTINCI BÖLÜM

6. ÖNERİLER

Bilişim teknolojisi ile gerçekleştirilen bir değişim, ülkeler için devrim niteliği taşımaktadır. Şöyle ki artık ulaşım, iletişim, sağlık, güvenlik gibi birçok alanda bilişim teknolojileri kullanılmaktadır. Bu da ülkelerin gelişmişliklerini ortaya koymaktadır. Bu gelişmişlik beraberinde de birçok problemleri ortaya çıkarmaktadır. En önemli problemlerin başında da siber suçlar gelmektedir. Siber suçlarla mücadele noktasında insanların bilişim ve teknolojik gelişimle ilgili bilinçlendirilmesi ve bilgilendirilmesi gerekir. Bu bilgilendirmeler ve farkındalık eğitimleri erken yaşta çocuklara aşılanmalıdır. Şöyle ki yapmış olduğumuz çalışmada lise öğrencileri üzerinde bu eksiklikler görülmektedir. Bu eksikliklerin giderilmesi noktasında ülkemizde bilişim teknolojileri eğitimlerine okullarımızda daha çok yer verilmelidir. Bu eğitimlerin arttırılmasıyla siber suçlara bulaşma riski azaltılabilir ve kişiler üzerinde farkındalık oluşturulabilir. Diğer taraftan siber suç farkındalığının artırılması için eğitim sistemindeki hâlihazırdaki bilişim teknolojiler dersinin saatleri artırılmalıdır.

Siber suçların bir kısmının suç olarak algılanıp bir kısmının sadece yanlış olarak algılanması genel olarak internette kötü bilgiler sebebiyledir. İnternet ortamındaki siteler ve hacker bilgileri içeren siteler daha fazla kontrol altına alınmalıdır.

Orta öğretim öğrencilerine verilen bilgisayar ve internet ile alakalı derslerde siber suçların yasal sınırlarını öğretecek biçimde müfredat değişikliği yapılması tavsiye edilebilir.

Eğitimcilerin siber suçlar konusunda hizmet içi eğitim alması önerilebilir. Böylelikle okullarda öğrencilerin siber suçlara bulaşma riskleri önlenebilir ve kontrol altına alınabilir.

Siber suçlarla mücadele konusunda emniyet teşkilatın da bu alanla ilgili uzman kişilerce okullarda bilgilendirme eğitimleri verilmelidir. Emniyet teşkilatının vereceği bu eğitimler gençlerde farkındalık oluşturabilir ve suça meyil eden

öğrencilerde caydırıcılık ortaya koyabilir. Diğer taraftan kolluk kuvvetlerinin siber suçlar alanında önleyici hizmet anlayışına ağırlık vermesi toplumda siber suç farkındalığı oluşturması önerilebilir.

Gençlerin ve halkın yoğun olduğu yerlerdeki ilan panolarına bilgilendirici afişler asılabilir ve bu alanda yapılan çalışma ve araştırmalar derlenerek bilgilendirme amaçlı okullara dağıtılabilir.

YEDİNCİ BÖLÜM

7. KAYNAKÇA

Akarslan, H. (2012). Yeni Tasarı Çerçevesinde Bir Bilişim Suçu Operasyonunun Değerlendirilmesi, Bolu.

Akdağ, P. (2009). Siber Suçlar ve Türkiye'nin Ulusal Politikası. Yüksek Lisans Tezi, Polis Akademisi Güvenlik Bilimleri Enstitüsü, Ankara.

Akıncı, H. Alıç, E. ve Er, C. (2004). Türk Ceza Kanunu ve Bilişim Suçları. İnternet ve Hukuk, (Der. Yeşim M. Atamer). İstanbul Bilgi Üniversitesi Yayınları.

Aktürk, A.O, Emlek, B. ve Çelik İ. (2017) "Üniversite Öğrencilerinin Facebook Bağlanma Stratejilerinin ve Yaşam Doğumlarının İncelenmesi" Mersin Üniversitesi.

Alaca, B. (2008). Ülkemizde Bilişim Suçları ve İnternetin Suça Etkisi (Antropolojik ve Hukuki Boyutları İle), Yüksek Lisans Tezi, Ankara Üniversitesi Sosyal Bilimler Enstitüsü Antropoloji Anabilim Dalı, Ankara.

Aslantürk, Z. (1999). *Araştırma Metot ve Teknikleri.* İstanbul: Emre Matbaası.

Aslantürk, Z.2004 (6. Baskı) Sosyal Bilimler İçin Araştırma Metod ve Teknikleri, İstanbul: Çamlıca

Atıcı, B. ve Gümüş, Ç. (2003). Sanal Ortamda Gerçek Tehditler: Siber Terör. *Polis Dergisi.*

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

Bilek, B. T. (2012). Bilişim Suçları ve Üniversite Lisans Öğrencilerinin Bilişim Suçlarına Yönelik Görüşleri, Yüksek Lisans Tezi. Gazi Üniversitesi Bilişim Enstitüsü, Ankara.

Bayraktar, K. (2000). *"Banka Kredi Kartları İle Ortaya Çıkan Ceza Hukuku Sorunları", Prof. Dr. M. Kemal Oğuzman'ın Anısına Armağan.* İstanbul: Beta Yayınevi.

Çakmak, H. ve Demir, C. K. (2009), *Siber Dünyadaki Tehdit ve Kavramlar, Suç, Terör ve Savaş Üçgeninde Siber Dünya* (1. Baskı). Anakara: Barış Platini. Kitabevi.

Çepni, S. (2008). *Kuramdan Uygulamaya Fen ve Teknoloji Öğretimi* (7.Baskı). Ankara: Pegem Akademi Yayıncılık.

Çepni, S. 2001. *Araştırma ve Proje Çalışmalarına Giriş*, Trabzon: Erol Ofset Matbaacılık.

Değirmenci, O. (2002). Bilişim Suçları, Yüksek Lisans Tezi, Marmara Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul.

Değirmenci, O. (2003). Ceza Hukuku Açısından Kredi ve Banka Kartları, *Legal Hukuk Dergisi*, S.3, Mart 2003, ss.592-609.

Demir, Ö. (2002). İnternet Servis Sağlayıcılarının Hukuki Sorumluluğu, *Dokuz Eylül Üniversitesi Uluslararası İnternet Sempozyumu*, ss.471-484, İzmir, 2002.

Dijle, H. ve Doğan, N. (2011). Türkiye'de Bilişim Suçlarına Eğitimli İnsanların Bakışı. *Bilişim Teknolojileri Dergisi*, 4(2), 43-53.

Doğan, K. (Ekim-2005). Bilişim Suçları ve Yeni Türk Ceza Kanunu. *Hukuk ve Adalet: Eleştirel Hukuk Dergisi,* Y:2, S:6-7, 290-319.

Durmaz, Ş. (2006). Bilişim Suçlarının Sosyolojik Analizi, Yayımlanmamış Yüksek Lisans Tezi, Gazi Üniversitesi Sosyal Bilimler Enstitüsü Kamu Yönetim Ana Bilim Dalı, Ankara.

Dülger, M. V. (2004) *Bilişim Suçları,* Ankara: Seçkin Yayıncılık.

EGM, (2015), "2014 Yılı Faaliyet Raporu", EGM Strateji Geliştirme Daire Başkanlığı, Ankara.

Ekinci, M. (2002). *Banka Kartları ve Kredi Kartları*, Ankara: Adalet Yayınları

Europol, (2014). İnternet Organize Suç Tehdidi Değerlendirmesi (İOCTA), Avrupa

Polis Teşkilatı Yayını. net/haber/356996/:(11.03.2015).

Hennessy J. L., P. David A. ARPACİ-DUSSEAU Andrea (2007).“Computer Architecture”, *Morgan Kaufmann*.

İçel, K. (2001). Avrupa Konseyi Siber Suç Sözleşmesi Bağlamında Avrupa Siber Suç Politikasının Ana İlkeleri, İÜHFM, Cilt. LIX, S. 1-2, İstanbul.

İlbaş, Ç. (2009). Bilişim Suçlarının Sosyo-Kültürel Seviyelere Göre Algı Analizi. Yüksek Lisans Tezi, Başkent Üniversitesi Fen Bilimleri Enstitüsü, Ankara.

Kangal, Z. T. (2001). Fransa’da İnternet Yoluyla İşlenen Suçlardan Doğan Ceza Sorumluluğu, İÜHFM, C.LIX, S.1-2, İstanbul.

Karagülmez, A. (2011). *Bilişim Suçları ve Soruşturma - Kovuşturma Evreleri*, Ankara: Seçkin Yayıncılık.

Karasar, N. (2002) Bilimsel Araştırma Yöntemi, Ankara: Nobel Yayın Dağıtım Ltd. Şti.

Karasar, N. (2004). *Bilimsel Araştırma Yöntemi (13. Baskı).* Ankara: Nobel Yayın Dağıtım.

Kazancı, B.E. (2007) Kişilerin İzinsiz Görüntülerinin Alınmasının TCK m. 134 Çerçevesinde Korunması, *Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi,* C. 9., 1. SY., 2007, 131-164.

Köksal, M.A. ve İlbaş, Ç. (2015), Türkiye’de Bilişim Suçları: 1990-2011, http://www.slideshare.net/melihbayramdede/trkiyenin-siber-su-haritas-19902011 (10.02.2015).

Kurt, L. (2005) *Açıklamalı-İçtihatlı Tüm Yönleriyle Bilişim Suçları ve Türk Ceza Kanunundaki Uygulaması*, Ankara: Seçkin Yayıncılık.

Martin, N., Rice, J. (2011). Cybercrime: Understanding and addressing the concerns of stakeholders. Computers & Security, 30(8), p.803-814.

Nacar, F. B. (2010). Avrupa Birliği Ülkeleri ve Türkiye'de bilişim Suçlarının Ceza Hukukundaki Uygulamaları. Yüksek lisans tezi. Atılım Üniversitesi Sosyal Bilimler Enstitüsü, Ankara.

Oğuz, H. (2013) Elektronik Ortamda Kişisel Verilerin Korunması, Bazı Ülke Uygulamaları ve Ülkemizdeki Durum, *Uyuşmazlık Mahkemesi Dergisi, S:3*

Ömercioğlu, A. (2016). Vergi Denetim Müesseseleri Açısından Hayatın Gizli Alanına Karşı Suçlar, *Ankara Üniversitesi Hukuk Fakültesi Dergisi*, S:65 (4), SS: 2277-2304.

Önok, M. (2013). Avrupa Konseyi Siber Suç sözleşmesi Işığında Siber Suçlarla Mücadelede Uluslararası İşbirliği*, Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi,* C: 19, S: 2, ss. 1229-1270.

Özel, C. (2001). Bilişim Suçları ile İletişim Faaliyetleri Yönünden Türk Ceza Kanunu Tasarısı, *İstanbul Barosu Dergisi*, C.LVI, S.7-8-9.

Özgür, U. ve Beceni, Y. (2004). Bilişim-İletişim Teknolojileri ve Ceza Hukuku, İnternet ve Hukuk (derleyen Yeşim M. Atamer), İstanbul Bilgi Üniversitesi Yayınları, İstanbul, 2004

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, Yüksek Lisans Tezi, Erciyes Üniversitesi Sosyal Bilimler Enstitüsü, Kayseri.

Philippsohn, S. Samanta T. (2003) E-fraud - What Companies Face, *Computer Fraud &Security,* Volume.2003, Issue.1.

Polat, A. (2008). Suç İstatistiklerine İlişkin Sorunlar ve Öneriler, *Polis Bilimleri Dergisi,* C: 10, S: 1, ss: 1-24.

Sınar, H. İstanbul Bilgi Üniversitesi ve İstanbul Barosu tarafından 16 Mart 2002

tarihinde düzenlenen İnternet ve Ceza Hukuku konulu panelde yapılan konuşması. İntern"et ve Hukuk, (der. Yeşim ATAMER), ss.277-299, İstanbul Bilgi Üniversitesi Yayınları, İstanbul, 2004, ss. 659-669.

Şen, B. (2011). Bilişim Suçlarıyla Mücadele. http://www.tbmm.gov.tr/arastirma_komisyonlari/bilisim_internet/docs/sunumlar/egm_bilisim_suclari.pptx. 18.05.2015

Taşkın Ş.C. (2009) Bilişim Hukuku Uluslararası Uyuşmazlıklar, *Türkiye Barolar Birliği Dergisi,* S:85, ss:332-372.

Topaloğlu, M. (1997). *Bilgisayar Programları Üzerindeki Haklar ve Bu Hakların Korunması.* İstanbul: TBV Yayınları.

Türkiye Bilişim Dergisi (TBD) (2011). 11 Yıllık Siber Suç Haritamız Çıkarıldı, S: 137, ss. 14-19.

Taşçı, U ve Can, A. (2014) Türkiye'de Polisin Siber Suçlarla Mücadele Politikası: 1997-. *Fırat Üniversitesi Sosyal Bilimler Dergisi,* Elazığ

Turhan, O. (2006). Bilgisayar Ağları ile İlgili Suçlar (Siber Suçlar), Devlet Planlama Teşkilatı Müsteşarlığı Hukuk Müşavirliği, Planlama Uzmanlığı Tezi, Ankara

Ünver, M. ve Canbay, C. (2010). Ulusal ve Uluslararası Boyutlarıyla Siber Güvenlik‖, *Elektrik Mühendisliği Dergisi*, Sayı 438.

Ünver, Y. (2001). TCK VE CK Tasarısının İnternet Açısından Değerlendirilmesi, İÜHFM, Cilt. LIX, S.1-2, İstanbul.

Yayla, M. (2013). Hukuki Bir Terim Olarak "Siber Savaş". Türkiye Barolar Birliği Dergisi, (104), s.177-202.

Yazıcıoğlu, Y. (1997). B*ilgisayar Suçları Kriminolojik, Sosyolojik ve Hukuki Boyutları İle,* İstanbul: Alfa Yayıncılık.

Yazıcıoğlu, Y. (2004). Bilişim Suçları Konusunda 2001 Türk Ceza Kanunu

Tasarısının Değerlendirilmesi, *Hukuk ve Adalet: Eleştirel Hukuk Dergisi*, İstanbul, Y:1, S:1.

Yenidünya, A.C. ve Değirmenci, O. (2003). Bilişim Suçları(1.Baskı). İstanbul: Legal Yayıncılık

Yetim, S. (2014). "Siber Suçlar, Yargılama Yetkisi ve Yeni Bir Model Önerisi", *Türkiye Adalet Akademisi Dergisi,* S: 17.

Zarplı, Ç. (2008). İfade Özgürlüğü: İçeriği ve Sınırları. Yayımlanmamış Yüksek Lisans Tezi, Dumlupınar Üniversitesi Sosyal Bilimler Enstitüsü, Kütahya.

bilgem.tubitak.gov (2015). http://bilgem.tubitak.gov.tr/tr/haber/siber-suclarla mucadelede-tubitak-ve- emniyet-işbirliği, Erişim Tarihi: 17.05.2017

bilişimsurasi. org.tr, (2015), "Bilişim Suçları Çalışma Grubu",

http://www.Bilişimsurasi.org.tr/ dosyalar/9.doc, , Erişim Tarihi: 20.11.2016

egm.gov.tr (2015) ,"2014 Yılı Performans Programı", http://www.egm.gov.tr/Documents/ PERFORMANS-PROGRAMI-2014.pdf, Erişim Tarihi: 09.03.2015

egm.gov.tr (2015), http://www.egm.gov.tr/Sayfalar/DaireBaskanliklari.aspx Erişim Tarihi: 09.03.2015

memurlar.net, (2015). Bilişim Suçları ve Sistemleri Şube Müdürlüğü Kuruldu, http://www.memurlar.net/haber/88791/, Erişim Tarihi: 25.03.2015.

internetworldstats. com. , Erişim Tarihi: 14.02.2015.

http://tdkterim.gov.tr/bts/?kategori=veritbn&kelimesec=45464,

turkhackteam.org(2015), "Polisten nasıl Korunuruz? (Polis Nasıl Takip Eder) Sosyal Mühendislik" http://www.turkhackteam.org/sosyal-muhendislik/1038307-polis-ten-nasil-korunuruz-polis-nasil-takip- eder.html Erişim Tarihi: 11.03.2015

EKLER

EK-1

KİŞİŞEL BİLGİ FORMU

Bu anket, lise öğrencilerinin siber suç algı düzeylerinin belirlenmesine yönelik olarak hazırlanmıştır. Kişisel bilgileriniz ve ifadeler için duygu ve düşünceleriniz kesinlikle bireysel olarak yayınlanmayacak, sadece toplu rakamlar açıklanacaktır.

Araştırmaya gösterdiğiniz ilgi ve katkılarınız için şimdiden teşekkür ederiz.

Erdal LAFVERMEZ

Yüksek Lisans Öğrencisi

1) Cinsiyet

○ Kız ○ Erkek

2) Kaçıncı Sınıfta Öğrenim Görüyorsunuz?

○ 1.Sınıf ○ 3.Sınıf
○ 2.Sınıf ○ 4.Sınıf

3) Kaç yıldır internet kullanıyorsunuz?

○ 1-2 ○ 3-4 ○ 5-6 ○ 7-8
○ 9-10 ○ 10 ve daha fazla

4) Günde ortalama kaç saat internet kullanıyorsunuz?

○ 1 saatten daha az ○ 1-2 ○ 3-4 ○ 5-6
○ 7-8 ○ 8 saatten daha fazla

5) Facebook, Twitter, WordPress, Friendster, Instagram gibi Sosyal Ağları Kullanıyor musunuz?

○ Evet ○ Hayır

6) Ailenizin Eğitim Seviyesi Nedir?

Anne Eğitim Seviyesi	**Baba Eğitim Seviyesi**
○ İlkokul	○ İlkokul
○ Ortaokul	○ Ortaokul
○ Lise	○ Lise
○ Üniversite	○ Üniversite
○ Yüksek Lisans	○ Yüksek Lisans
○ Doktora	○ Doktora
○ Okur-Yazar Değil	○ Okur-Yazar Değil

	Aşağıdaki fiiller çeşitli ülkelerin ceza sistemlerinde suç olarak tanımlanmaktadır. Lütfen bu fiilleri kişisel görüşünüze göre, suç derecesine göre 1'den 5 'e kadar numaralandırınız. **(1: En Hafif Suç, 5: En Ağır Suç)**	**(1)**	**(2)**	**(3)**	**(4)**	**(5)**
1	Bir ülke veya devlet aleyhinde web sitesi yayını yapılması,					
2	Bir ülke veya devlet aleyhinde yayın yapan bir web sitesinin, bir kişi ya da grup tarafından kapatılması, erişimin engellenmesi (deface/hack),					
3	Bir banka müşterilerinin hesap bilgileri elde edilerek yetkisiz para transferinin yapılması,					
4	Sahte Loto, şirket ortaklığı gibi tuzaklarla dolandırıcılık yapılması,					
5	Kimlik numarası, telefon numarası ve adres gibi kişisel bilgilerin web sitesi aracılığı ile toplanıp üçüncü şahıslara sunulması veya satılması,					
6	Bir kişisel bilgisayara uzaktan müdahale ederek kişisel dosya, belge ve dokümanların elde edilmesi,					
7	Bilgisayar donanımlarına fiziksel zarar verilmesi,					
8	İnternet'te bulunan bir makale ya da raporun referans gösterilmeden kullanılması,					
9	Başkası tarafından hazırlanan bilgisayar yazılımlarında değişiklik yaparak yazılım üzerinde hak iddia edilmesi,					
10	Çocuk pornografisi konulu fotoğraf ve video içeriği bulunan internet sitesi yayınlarının yapılması,					
11	Çocuk pornografisini temsil eden çizim ve animasyonlara yönelik içeriği bulunan internet sitesi yayınlarının yapılması,					
12	Çocuk pornografisi konulu içeriği bulunan internet sitesi yayınlarına erişilmesi,					
13	Bilgisayar sistemine zarar veren kodlar yazılması ve yayınlanması,					
14	Bir bilişim sistemindeki verilere yetkisiz olarak erişip herhangi bir zarar vermeden sistemden çıkılması,					

EK-2: İZİN B ELGESİ

T.C.
KIRŞEHİR VALİLİĞİ
İl Millî Eğitim Müdürlüğü

Sayı :24512418-605.01-E.4209178 29/03/2017
Konu: Erdal LAFVERMEZ'in
Araştırma İzni

VALİLİK MAKAMINA

Necmettin Erbakan Üniversitesi Öğrenci İşleri Daire Başkanlığı'nın 15.03.2017 tarih ve 3298 sayılı yazıları ile; Eğitim Bilimleri Enstitüsü Bilgisayar ve Öğretim Teknolojileri Eğitimi Anabilim Dalı Bilgisayar ve Öğretim Teknolojileri Eğitimi Bilim Dalı Tezli Yüksek Lisans öğrencisi Erdal LAFVERMEZ'in "Lise Öğrencilerinin Siber Suç Algı Düzeylerinin Farklı Değişkenler Açısından İncelenmesi:Kırşehir İli Örneği" konulu anket çalışması yapma isteği bildirilmektedir.

Eğitim Bilimleri Enstitüsü Bilgisayar ve Öğretim Teknolojileri Eğitimi Anabilim Dalı Bilgisayar ve Öğretim Teknolojileri Eğitimi Bilim Dalı Tezli Yüksek Lisans öğrencisi Erdal LAFVERMEZ'in "Lise Öğrencilerinin Siber Suç Algı Düzeylerinin Farklı Değişkenler Açısından İncelenmesi:Kırşehir İli Örneği" konulu anket çalışmasını, il merkezindeki ortaöğretim öğrencilerine, Milli Eğitim Bakanlığı Yenilik ve Eğitim Teknolojileri Genel Müdürlüğünün 07.03.2013 tarihli ve 3616 sayılı 2012/13 nolu genelge esaslarına göre, araştırmacının sorumluluğunda gönüllülük esasına göre anket şeklinde uygulaması Müdürlüğümüzce uygun görülmektedir.

Makamınızca da uygun görüldüğü takdirde olurlarınıza arz ederim.

Şevket KARADENİZ
İl Milli Eğitim Müdür V.

OLUR
29/03/2017

Servet GÜNGÖR
Vali a.
Vali Yardımcısı

Terme Cad. 40200 Merkez/KIRŞEHİR
Elektronik Ağ:kirsehir.meb.gov.tr
e-posta: kirsehirmem@meb.gov.tr

Ayrıntılı bilgi için: Ahmet DOST Şube Müd.
Tel: (0386)2135150-1315
Faks: (0386) 213 10 03

T. C
SELÇUK ÜNİVERSİTESİ
Eğitim Bilimleri Enstitüsü Müdürlüğü

ÖZ GEÇMİŞ

Adı Soyadı:	Erdal LAFVERMEZ
Doğum Yeri:	Pazarcık/KAHRAMANMARAŞ
Doğum Tarihi:	15.06.1989
Medeni Durumu:	Bekâr
Öğrenim Durumu	
İlköğretim:	Büyüknacar İÖO (Pazarcık/Kahramanmaraş), 1994 – 1999
Ortaöğretim:	Pazarcık YİBO (Pazarcık/Kahramanmaraş), 1999-2002
Lise:	İslâhiye Çok Programlı Lisesi (İslâhiye/Gaziantep), 2002-2005
Lisans.	Bilgisayar ve Öğretim Teknolojileri Eğitimi, Ahi Evran Üniversitesi (Kırşehir), 2008 – 2012
Yüksek Lisans.	Eğitim Bilimleri Enstitüsü, Bilgisayar ve Öğretim Teknolojileri Eğitimi, Selçuk Üniversitesi (Konya), 2015-2018
İş Deneyimi:	Bilgisayar bölümü dönem stajyeri- İslâhiye Sosyal Yardımlaşma ve Dayanışma Fonu (İslâhiye/Gaziantep), 2015 Kırşehir Valiliği İl Proje Koordinasyon Ekibi Proje Araştırmacısı, 2015-2016 Gençlik Liderliği, Bilgi İşlem ve Sosyal Medya Sorumlusu, Bilgisayar Kursu Usta Öğreticisi Gençlik ve Spor İl Müdürlüğü (Kırşehir), 2012 – Devam Ediyor
Proje Deneyimi	Gençlik ve Spor Bakanlığı "Değerlerimiz Geleceğimizdir" Projesi,2014-2015 Aile ve Sosyal Politikalar Bakanlığı EDES "Spor Engel Tanımaz" Projesi,2015 Gençlik ve Spor Bakanlığı "Geçmişten Gelen Işık" Projesi 2016 Gençlik ve Spor Bakanlığı "Türkiye Liseler Öğrenci Meclisi Çalıştayı" Projesi, 2016 Gençlik ve Spor Bakanlığı "Şehit Aileleri ve Gönüllüler" Projesi,2015-2016 İçişleri Bakanlığı Dernekler Dairesi Başkanlığı, " Birlikte Bir Adım Önde" Projesi, 2016
Halen Yaptığı İş:	Gençlik Lideri – Kırşehir Gençlik ve Spor İl Müdürlüğü (2012 –Devam Ediyor)
Tel:	0 506 693 06 73
E-mail:	erdal.lafvermez@gsb.gov.tr, erdallafvermez46@hotmail.com
Adres:	Gençlik ve Spor İl Müdürlüğü- Cacabey Gençlik Merkezi, Kırşehir