BAŞKENT ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

BİLİŞİM SUÇLARININ SOSYO-KÜLTÜREL SEVİYELERE GÖRE ALGI ANALİZİ

ÇIĞIR İLBAŞ

YÜKSEK LİSANS TEZİ
2009

BİLİŞİM SUÇLARININ
SOSYO - KÜLTÜREL SEVİYELERE GÖRE ALGI ANALİZİ

THE PERCEPTION ANALYSIS OF COMPUTER CRIMES WITH RESPECT TO SOCIO-CULTURAL LEVELS

ÇIĞIR İLBAŞ

Başkent Üniversitesi
Lisansüstü Eğitim Öğretim ve Sınav Yönetmeliğinin
İstatistik ve Bilgisayar Bilimleri Anabilim Dalı İçin Öngördüğü
YÜKSEK LİSANS TEZİ
olarak hazırlanmıştır.

2009

Fen Bilimleri Enstitü Müdürlüğü'ne

Bu çalışma, jürimiz tarafından İSTATİSTİK VE BİLGİSAYAR BİLİMLERİ ANABİLİM DALI 'nda YÜKSEK LİSANS TEZİ olarak kabul edilmiştir.

Başkan :.....
Prof. Dr. İsmail ERDEM

Üye (Danışman) :.....
Yrd. Doç. Dr. Mehtap AKÇİL

Üye :.....
Prof. Dr. Ali HALICI

ONAY

Bu tez 09 / 06 / 2009 tarihinde, yukarıdaki jüri üyeleri tarafından kabul edilmiştir.

..... / 06 / 2009
Prof. Dr. Emin AKATA
FEN BİLİMLERİ ENSTİTÜSÜ MÜDÜRÜ

TEŞEKKÜR

Sayın Yrd. Doç. Dr. Mehtap AKÇİL'e tez konusu seçiminden sonuçların yorumlanmasına kadar her süreçte yol gösterici, motive edici ve yardımcı olduğu için,

İstatistik ve Bilgisayar Bilimleri Bölümü öğrencileri Çağla ATAGÖREN ve Günsu ARSLANYIKAR' a anket uygulamasında verdikleri destek için,

Teşekkür ederim.

ÖZ

BİLİŞİM SUÇLARININ SOSYO - KÜLTÜREL SEVİYELERE GÖRE ALGI ANALİZİ

ÇIĞIR İLBAŞ
Başkent Üniversitesi Fen Bilimleri Enstitüsü
İstatistik ve Bilgisayar Bilimleri Anabilim Dalı

Bu çalışmada, bilişim suçları algısının demografik faktörlere göre değişimi incelenmiştir. Farklı ülkelerin hukuk sistemlerine göre bilişim suçu sayılan fiilleri bireylerin ahlaki ve hukuksal düzlemde nasıl değerlendirdiklerini ölçmek çalışmanın temel amacıdır.

Başkent Üniversitesi'nde eğitim veren altı fakültenin birer bölümündeki öğretim elemanı ve öğrencilere uygulanan anket araştırması, çalışmanın araştırma yöntemi olarak belirlenmiştir.

Anketteki sorular; demografik bilgiler, teknoloji ilgisinin ölçülmesi, bir grup bilişim suçunun suç şiddeti açısından değerlendirilmesi ve bir grup fiilin ahlaki ve hukuksal açıdan değerlendirilmesi bölümlerinden oluşmaktadır.
Anket sonuçları, demografik faktörler, eğitim alanı ve akademik konuma göre gruplanarak çapraz tablo analizleri uygulanmıştır.

Çalışmanın bulguları, bilişim suçları konusundaki genel algı seviyesinin ve farklı nitelikteki gruplar arasındaki anlamlı farklılıkların belirlenmesini sağlamıştır.

ANAHTAR SÖZCÜKLER : Bilişim Teknolojileri, Bilişim Suçları, Bilişim Hukuku, Algı Analizi

Danışman : Yrd. Doç. Dr. Mehtap AKÇİL
Başkent Üniversitesi Fen Edebiyat Fakültesi İstatistik ve Bilgisayar Bilimleri Bölümü

ABSTRACT

THE PERCEPTION ANALYSIS OF COMPUTER CRIMES WITH RESPECT TO SOCIO-CULTURAL LEVELS

ÇIĞIR İLBAŞ
Başkent University Institute of Science
The Department Of Statistics and Computer Science

In this study, it was analyzed the changes in the perception of computer crimes with respect to the demographic factors. It aims at measuring how the individuals evaluate the actions, which are accepted as informatics crimes in different countries and legal systems, on moral and legal grounds. In this study we employed survey method as our research methodology. The questionnaires were applied on the academic staff and students of the six different departments of Başkent University.

The questionnaire involved four different parts, including demographics, technology involvement, the evaluation of computer crimes according to the intensiveness of the crime, and the evaluation of activities with respect to moral and legal frameworks. The results were grouped according to the demographic variables, the field of education, and the academic positions. They were evaluated by the implementation of cross-table analysis.

The findings enabled us to analyze and evaluate the general perception level with regard to computer crimes as well as the meaningful differences between varying groups.

KEYWORDS: Information Technologies, Computer Crimes, Information Technologies Law, Perception Analysis

Supervisor : Asst. Prof. Mehtap AKÇİL
Başkent University Faculty of Science and Letters, Department of Statistics and Computer Science

İÇİNDEKİLER LİSTESİ

Sayfa

ÇİZELGELER LİSTESİ

Sayfa

KISALTMALAR LİSTESİ

AET	Avrupa Ekonomik Topluluğu
CIA	Central Intelligence Agency
DOS	Denial Of Service Attack
DDOS	Distributed Denial Of Service Attack
EFT	Elektronik Fon Transferi
FBI	Federal Bureau of Investigation
FSEK	Fikir ve Sanat Eserleri Kanunu
NCCS	National Computer Crime Squad
TCK	Türk Ceza Kanunu
USCL	Unıted States Criminal Law
YFCK	Yeni Fransız Ceza Kanunu

1. GİRİŞ

Bilişim teknolojilerinin toplumsal ve ekonomik süreçlerdeki önemi artmaya başladıkça, bazı klasik suçların işleniş biçimlerinde teknoloji araç olarak kullanılmaya başlamış ve teknolojik sistemlere yönelik yeni suç türleri oluşmaya başlamıştır.

Teknolojideki hızlı gelişmenin yarattığı süreç değişimleri ve bilişim sistemlerinin mevcut süreçlere entegrasyonu, suç işleme niyetindeki bazı birey ve grupların teknolojiyi hem araç hem de hedef olarak kullanmasına yol açmış ve neticede bilişim suçları günümüz modern toplumlarının önemli bir sorunu haline gelmiştir.

Hukuk ve teknoloji gibi birbirine oldukça uzak mesafede duran iki disiplinin kesişim noktası olan "bilişim suçları" konusunda hukuksak düzenlemelerin çok yeni, yapılan araştırma ve çalışmaların da yetersiz olduğu bilinmektedir.

Bilişim suçları konusundaki temel kavramlar, tarihsel gelişimi, farklı devletlerin ve Türkiye'nin hukuk sisteminde bilişim suçlarına ilişkin düzenlemelerin incelenmesinden sonra; anket çalışması ile farklı eğitim ve yaş düzeylerindeki bireylerin bilişim suçu sayılan fiilleri ahlaksal ve hukuksal boyutlarda nasıl algıladıkları incelenecektir. Bireylerin kendilerine yönelen fiiller veya kendi fiillerinin suç unsuru taşıyıp taşımadığı konularındaki bilgi ve algılarının ölçümü de bu çalışmanın öncelikli amaçlarından birisi olarak belirlenmiştir.

2. BİLİŞİM KAVRAMI

Bilişim, bilmek fiilinin türevi olan bilişmek fiilinden türetilmiş bir sözcüktür ve ilk kez 1968 yılında Prof. Dr. Aydın Köksal tarafından kullanılmıştır. Bilişim sözcüğünün Almanca'daki karşılığı olan Informatik, Fransızca'daki karşılığı olan informatique ve bunlardan türetilmiş olan Türkçe enformatik sözcükleri İngilizce'deki informatics sözcüğüyle birlikte computer science (bilgisayar bilimi) ve information systems (bilgi sistemleri) gibi alanları da kapsamaktadır [1].

Sözcük anlamı olarak bilişim; akışkan ve değişken bilgi anlamına gelmektedir. Bir öğrencinin akademik dönem sonu not ortalaması, bir şahıs ya da işletmenin banka hesap bakiyesi, döviz ve menkul kıymetlerin TL değerleri bilişim sözcüğü ile ifade

edilen değişken bilginin günlük yaşantıdaki örnekleridir.

Modern yaşamın çok önemli bir unsuru olan iletişim teknolojilerinin gelişmesi ile birlikte bilgi kavramının niteliği de değişmektedir. İletişim teknolojilerinin yaygın olarak kullanılmadığı dönemlerde durağan ve stabil nitelikler taşıyan bilgi, günümüz koşullarında daha devingen ve takibi için özel sistemlere ihtiyaç duyulan bir biçime dönüşmektedir. Bilişim kavramının teknik bilimsel anlamı bilişim sistemlerinin tarifini yapmaktadır.

Teknik bilimsel anlamda bilişim, "İnsanoğlunun teknik, ekonomik ve toplumsal alanlardaki iletişiminde kullandığı ve bilimin dayanağı olan bilginin özellikle elektronik makineler aracılığıyla düzenli ve akla uygun bir biçimde işlenmesi bilimi" olarak tanımlanmıştır [1]. Bilişim sözcüğü bilimsel anlamda; teknoloji, bilgisayar ve iletişim sözcükleriyle yakınlaşmaktadır.

Bilgisayar ve iletişim teknolojilerindeki gelişmeler günümüzde insanlık tarihi açısından çok önemli bir devrim olarak kabul edilmekte ve bilişim çağı, tarım ve endüstri çağlarından sonraki üçüncü küresel dönüşüm olarak kabul edilmektedir.

Bilişim ve internet teknolojilerinin gelişmesi ve yaygınlaşması, bilginin ekonomik, sosyal, ve siyasal değerlerinin artması, bu değerler üzerinde kolay yoldan söz hakkına sahip olmak isteyen kişileri bilişim teknolojileri kullanarak suç işlemeye yöneltmiştir. Bu noktada bilişim suçu kavramı ortaya çıkmıştır. Bilişim suçları olgusu bütün ülkelerin ortak sorunu haline gelmektedir.

3. BİLİŞİM SUÇU KAVRAMI

Türkçe'ye bilişim suçu olarak yerleşen kavram, İngilizce'de; bilgisayar bağlantılı suç, bilgisayarla işlenen suç, yüksek teknoloji suçu, bilgisayar suçu, siber suç anlamına gelen terimlerle ifade edilmektedir.

Bilişim suçları konusunda en geniş kabul gören tarif AET Uzmanlar Komisyonu'nun Mayıs 1983 yılında Paris Toplantısında yaptığı tanımlamadır. Bu tanımlamaya göre bilişim suçları; "Bilgileri otomatik işleme tabi tutan veya verilerin nakline yarayan bir sistemde gayri kanuni, gayri ahlaki ve yetki dışı gerçekleştirilen her türlü davranıştır." denmektedir [2].

Bilişim suçlarını, bilişim sistemlerinin yalnızca suç işleme aracı olarak kullanıldığı suçlar ve bilişim sistemlerinin hedef alındığı suçlar olarak iki grupta değerlendirmek mümkündür.

Bir şahsa karşı hakaret veya tehdit suçunun internet, cep telefonu gibi sistemlerle işlenmesi, kitap, müzik eseri gibi materyallerin bilişim sistemleri ile çoğaltılıp yayınlanması gibi fiiller bilişim sistemlerinin aracı olarak kullanıldığı suçlara örnek olarak gösterilebilir. Bu tür suçlar için yasalarda ayrıca bilişim suçu maddeleri eklenmesi yerine klasik suçlara verilecek olan cezalarda kapsam genişletilmesi yöntemi uygulanmaktadır.

Bir bilişim sistemindeki verileri bozma, değiştirme, bilişim sistemine erişimi engelleme gibi fiiller ise doğrudan bilişim sistemlerinin hedef alındığı suçlardır ve hukuk sistemlerinde ayrı kanunlar veya kanun maddeleri ile bu tür suçların çerçevesini belirlemektedir.

3.1 Bilişim Suçu Türleri

Bilişim suçlarını farklı açılardan değerlendirerek çeşitli kategorilere ayırmak mümkündür. Literatürde fiillerin hedefine göre, suçun işleniş yöntemine göre veya suçun etkilerine göre farklı sınıflandırmalar yapılmıştır. Amerika Birleşik Devletler hükümeti Federal Bureau of Investigation (FBI) tarafından hazırlanan National Computer Crime Squad (NCCS) çalışmasında bilişim suçları;

- Genel telefon şebekesinin ihlali
- Büyük bilgisayar ağlarının ihlali
- Ağ bütünlüğünün ihlali
- Özel hayatın ihlali
- Endüstriyel / kurumsal casusluk
- Yazılım korsancılığı
- İşlenmesinde bilgisayarların rol oynadığı diğer suçlar.

biçiminde sınıflandırılmıştır.

Shinder and Tittel [3], bilişim suçları kapsamındaki suç türlerinin sınıflandırmasını şiddet unsuruna göre iki grupta değerlendirmiştir. Potansiyel şiddet / şiddet içeren suçlar ve şiddet içermeyen suçlar olarak iki grupta toplanan suç türleri, detaylı

olarak listelenmekte ve en geniş kapsamlı sınıflandırmalardan birisi olarak kabul görmektedir. Ancak bu listede yer alan suçların tamamı bütün hukuk sistemlerinde suç olarak kabul edilmektedir. Benzer şekilde suçlara uygulanan yaptırımlar da ülkeler arasında büyük farklılıklar göstermektedir.

Söz konusu sınıflandırmaya göre bilişim suçu türleri çizelge1.1'de yer almaktadır.

Çizelge 1.1 Bilişim Suçları Sınıflandırması

Potansiyel Şiddet / Şiddet İçeren Suçlar	**Şiddet İçermeyen Suçlar**
Siber terörizm	Siber ihlal
Tehditle saldırı	Siber hırsızlık
İnernet üzerinden taciz, hakaret	Siber dolandırıcılık
Çocuk Pornografisi	Yıkıcı bilişim suçları
	Diğer şiddet içermeyen suçlar

3.1.1. Potansiyel şiddet veya şiddet içeren suçlar

Bilişim sistemleri kullanılarak kişilere ya da gruplara karşı ölümcül sonuçlara yol açabilecek, fiziki veya ruhsal çöküntü yaratabilecek fiilleri tanımlamaktadır. Söz konusu suç tipi, bilişim sistemlerini suç işleme aracı olarak kullanan suçlar kategorisindedir [3].

Siber terörizm (cyberterrorism)

Bilişim sistemleri kullanılarak terör suçu işleme, planlama ve koordine etme sonucunda ölüm ve yaralanmaya sebep olabilecek suçlardır. Bilişim suçları arasında örneklerine en az rastlanan suç tipidir. Hava trafik kontrol sistemlerinin dışarıdan müdahaleyle bozulması, hastane bilişim sistemlerine yapılan müdahalelerle hasta bilgilerinin değiştirilmesi gibi açılımları bulunmaktadır.

Tehditle saldırı (assault by threat)

Bilişim sistemleri kullanılarak kişi veya grupları tehdit etme davranışıdır. Potansiyel şiddet içeren bir suç türüdür.

İnternet üzerinden taciz, hakaret (cyberstalking)

Bilişim sistemleri kullanılarak bir kişi ya da gruba karşı taciz, hakaret, şantaj gibi davranışlardır. Potansiyel şiddet içeren bir suç türüdür.

Çocuk pornografisi (child pornography)

Çocukların veya çocukları temsil eden çizim ve animasyonların pornografik materyal olarak kullanılmasını ifade eden bir fiildir. Bu tür materyallerin oluşturulması, yayımlanması ve bilgisayarlarda bulundurulması uluslararası anlaşmalar çerçevesinde düzenlenmiş bir suçtur. Suç çerçevesi uluslararası anlaşmalarla belirlenmiş olmasına rağmen; çocukları temsil eden görüntü ve animasyonlar konusunda Japonya'nın yaklaşımı ve gereken önlemlerin bu ülke tarafından alınmaması tartışma konusu olmaktadır.

3.1.2. Şiddet İçermeyen Suçlar

Bilişim suçlarının büyük bir bölümü şiddet içermeyen suçlar kategorisindedir. Şiddet içermeyen bilişim suçları bilişim sistemlerinin aracı olarak kullanıldığı suçlar ve bilişim sistemlerinin hedef alındığı suçlar (yıkıcı siber suçlar) olarak iki bölümde incelenmektedir [3].

Siber ihlal (cybertrespass)

Bir bilişim sistemine yetkisiz olarak giriş yapmak, verileri kopyalamak ya da incelemek şeklinde tanımlanmaktadır. Siber ihlal suçu verilerin bozulması ya da sisteme girişin engellenmesi koşullarını gerektirmemektedir. Bir çok bilişim suçunun temelinde ve başlangıcında siber ihlal suçu bulunması nedeniyle Türk Ceza Kanunu dahil pek çok ülkenin bilişimle ilgili kanun bölümlerinde düzenlenen ilk madde olarak yer almaktadır.

Sanal Hırsızlık (cybertheft)

Bilişim sistemi kullanarak para veya değerli bilgilerin haksız biçimde elde edilmesi fiilidir. Pek çok farklı türünden başlıcaları ;

- Zimmete Geçirme (Embezzlement)
- Kanunsuz Ödenek (Unlawful Appropriation)
- Endüstri Casusluğu (Corporate/Industrial Espionage)

- Eser Hırsızlığı (Plagiarism)
- Korsancılık (Piracy)
- Kimlik Hırsızlığı (Identity Theft)

biçiminde tanımlanmıştır.

Sanal dolandırıcılık (cyberfraud)

Sanal ihlal ve siber hırsızlıktan farklı olarak herhangi bir bilişim sistemine yetkisiz erişimde bulunmadan, bir kişi ya da grubu aldatmaya yönelik davranışlar neticesinde çıkar sağlamak şeklinde tanımlanmaktadır. Siber hırsızlıktan farklı olarak siber dolandırıcılıkta kişiler kendi rızalarıyla para ve değerli eşya transferi yapmaktadırlar. İnternet üzerindeki loto tuzakları, ABD göçmenlik hakkı sağlayan yeşil kart çekilişi aracı siteleri, kara para aklama konusundaki yardım istekleri en yaygın örnekleridir.

Yıkıcı siber suçlar (destructive cybercrimes)

Ağ sistemlerini etkisiz kılma, veriye zarar verme veya yok etme gibi amaçlarla işlenen siber suçlardır. Bilgisayar sistemlerini bozmaya yönelik virüs, worm yazılımları, internet sitelerine erişimi engellemeye yönelik DOS ve DDOS atakları (hizmet engelleme saldırıları) söz konusu suçu oluşturan teknikler arasındadır.

Diğer şiddet içermeyen suçların yaygın örnekleri;

- İnternet üzerinden fahişelik servisi verme veya fahişelik reklamı yapma işlemleri (Advertising / Soliciting prostitution services over Internet)
- İnternet üzerinden kumar oynatma işlemleri(Internet Gambling)
- İnternet üzerinden ilaç, uyuşturucu madde satımı (Internet drug sales - both illegal drugs and prescription drugs)
- Siber kara para aklama işlemleri (Cyberlaundering - using electronic transfers of funds to launder illegally obtained money)
- Siber kaçak mal ticareti (Cybercontraband - transferring illegal items, such as encryption technology that is banned in some jurisdictions, over the Internet)

olarak tanımlanmaktadır [3].

Yukarıda sıralanan fiillerin de suç olarak kabulü ve yaptırımların türleri ülkelerin hukuk sistemlerine göre belirgin farklılıklar göstermektedir.

3.2 Bilişim Suçlarının Tarihçesi ve Uluslararası Çalışmalar

Kayıtlara geçen ilk bilişim suçu, 18 Ekim 1966 tarihli Minneapolis Tribune gazetesinde yayınlanan "Bilgisayar Uzmanı Banka Hesabında Tahrifat Yapmakla Suçlanıyor" isimli makale ile kamuoyuna yansımıştır. 1973 yılında kayıtlara geçen en büyük bilişim suçu Los Angeles eyaletinde bulunan "Equity Funding" adlı sigorta şirketinde 64 bin sahte müşteri kaydı ile gerçekleşen dolandırıcılık olayıdır [4].

Bilişim suçları konusundaki ilk kanun teklifi, ABD senatosu Operasyon Komitesi başkanı Senatör Abe Ribicoff tarafından Şubat 1977' de yapılmıştır. Kanun teklifi kabul edilmemiş olmasına rağmen bilgisayar suçu kavramının ABD ve uluslararası platformlarda tartışılmasını ve düşünülmesini sağlamıştır [5].

Avrupa Konseyi 1970'li yıllarda, elektronik bilgi bankalarında işlenen veriler dolayısıyla, bireylerin özel hayatının korunması için gereken ilkeleri belirlemek üzere bir çalışma başlatmıştır. Bu çalışmalar sonucunda, Avrupa Konseyi Bakanlar Komitesi, 1973 ve 1974 yıllarında, özel sektör ve kamu sektöründeki elektronik bilgi bankalarında uygulanacak ilkeleri gösteren iki tavsiye kararı kabul etmiştir. Bunun üzerine, başta Almanya olmak üzere, Avusturya, Fransa, Danimarka, Norveç gibi Konsey üyesi ülkeler verilerin korunması konusunda özel yasaları kabul etmişlerdir. "Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması"na ilişkin 108 sayılı sözleşme, 28 Ocak 1981 tarihinde imzaya açılmış ve aynı tarihte Avrupa Konseyi üyesi ülkelerle birlikte Türkiye tarafından da imzalanmıştır [6].

Bilişim suçlarına ilişkin en kapsamlı düzenleme Avrupa Konseyi bünyesinde gerçekleştirilen "Avrupa Siber Suç Sözleşmesi"dir. Hazırlanması 4 yıl kadar süren sözleşme, 23 Kasım 2001'de konsey üyesi olmayan ülkeler de dahil olmak üzere Budapeşte'de imzaya açılmıştır. Mayıs 2006 itibariyle, 12 ülkenin herhangi bir çekince koymadan imzaladığı sözleşme, 30 ülke tarafından çeşitli çekinceler konarak imzalanmıştır. Türkiye henüz söz konusu sözleşmeyi imzalamamıştır [7].

4. FARKLI ÜLKELERİN HUKUK SİSTEMLERİNDE BİLİŞİM SUÇLARI

4.1. ABD Hukukunda Bilişim Suçları

A.B.D. bilişim alanında işlenen ilk suçların ve buna bağlı olarak yasal düzenlemelerin yapıldığı ilk ülkedir. ABD'de bilişim suçlarının tespiti ve önlenmesine ilişkin federal düzeyde ve eyalet düzeyinde pek çok düzenleme yapılmıştır. Federal düzeyde CIA, "Information Warfare Center" adında 24 saat hizmet veren bir birim oluşturmuştur. Benzer şekilde FBI tarafından bilişim suçlarını takip etmek amacıyla kurulan "National Infrastructure Protection Center" ve "Computer Crime Squad" birimleri hizmet vermektedir. Adalet Bakanlığı bünyesinde oluşturulan "Computer Crime and Intellectual Property Section" birimi de bu alanda çalışmalar yapmakta, gerekli eğitim faaliyetlerinde bulunmakta ve diğer birimlere destek vermektedir.

ABD'de ilk defa 1984 yılında "Counterfeit Access Device and Computer Fraud and Abuse Act" (Erişim Aygıtlarını Taklit Etme, Bilgisayar Dolandırıcılığı ve Bilgisayarı Kötüye Kullanma Kanunu) ile "Credit Card Fraud Act" (Kredi Kartı Sahteciliği Kanunu) yürürlüğe girmiş, bu kanunda 1986 yılında "Computer Fraud and Abuse Act" (Bilgisayar Dolandırıcılığı ve Kötüye Kullanımı Kanunu) ile değişiklik yapılmıştır. Bunlarla birlikte bilişim suçlarında mücadelede;

- 18. U.S.C. 1029 sayılı Erişim Aygıtlarıyla İlgili Sahtecilik ve Bağlı eylemler,
- 18. U.S.C. 1030 sayılı Bilgisayarlarla İlgili Sahtecilik ve Bağlı Eylemler,
- 18. U.S.C. 2511 sayılı Telli, Telsiz ve Elektronik İletişime Müdahale ve İletişimin Açıklanmasının Yasaklanması,
- 18. U.S.C. 2701 sayılı Depolanmış İletişime Yetkisiz Erişim,
- 18. U.S.C. 2702 İçeriğin Açıklanması,
- 18. U.S.C. 2703 Yasal Erişim İçin Gerekli Şartlar

isimli kanunlar da kullanılmaktadır [8]. Söz konusu kanunlara ek olarak;

- Bilgisayar Sahtekarlığı ve Bilgisayarların Kötüye Kullanılması Yasası
- İletişim Ahlak Yasası
- Çocuk Pornografisinin Önlenmesi Yasası
- Çocukların Online Yayınlardan Korunması Yasası

- Elektronik Haberleşmenin Gizliliği Yasası
- İnternette Kumarın Önlenmesi Yasası
- Kimlik Hırsızlığı Yasası
- Terörizmle Mücadele Yasası

Kanunları da bilişim suçları konusunda yürürlüğe girmiş ve halen uygulanmakta olan kanunlardır [9].

4.2. Alman Hukukunda Bilişim Suçları

Bilişim suçları konusunda kara Avrupa'sındaki ilk düzenlemeler Almanya'da yapılmıştır. Alman hukuk sisteminde bilişim suçu kapsamında yürürlüğe giren kanunlar ve bilişim suçu olarak kabul edilen fiiller aşağıda belirtilmiştir [9].

- Verilerin depolandığı ve işlendiği bilişim ağına hukuka aykırı olarak girmek ve burada bulunan verileri hukuka aykırı olarak ele geçirmek (siber ihlal).
- Bilişim sistemleri aracılığıyla sahtekarlık ve dolandırıcılık (siber dolandırıcılık).
- Bilişim sistemlerinde bulunan verilere zarar verme fiilleri (yıkıcı siber suçlar)
- Telekomünikasyon yasası
- Bilişim ve iletişim servisleri yasası
- Teleservisler yasası

4.3. Avusturya Hukukunda Bilişim Suçları

Avusturya Ceza kanununda bilişim suçları ile ilgili maddeler;

- Verilere zarar verilmesi suçu (126 a)
- Bilişim sisteminin kullanılmasıyla işlenen dolandırıcılık suçu (148 a)
- İspat araçlarının kovuşturma organlarına verilmesinden kaçınma, bunlara zarar verme ve bunları gizleme suçu (293)

şeklinde tanımlanmıştır [9].

4.4. Danimarka Hukukunda Bilişim Suçları

Danimarka Ceza Kanunu'nda bilişim suçlarıyla ilgili maddeler;

- Çocuk pornografisi materyallerinin bulundurulması, üretilmesi, yayılması ya da çoğaltılması (235/1-2)
- Bilişim sistemlerine yetkisiz erişim (263/2) (siber ihlal).
- Bilişim sistemleri kullanılarak dolandırıcılık (279a) (siber dolandırıcılık).
- Bilişim sistemlerine zarar verme (291) (yıkıcı siber suçlar)

şeklinde tanımlanmıştır [10].

4.5. Fransız Hukukunda Bilişim Suçları

Fransa'da 01.03.1993 tarihinde yürürlüğe giren Yeni Ceza Kanunu ile bilişim alanına ilişkin düzenlemeler yapılmış ve yeni suç tipleri oluşturulmuştur. Buna göre YFCK'nın 226-16 ile 226-24 maddelerinde bilişim sistemleri aracılığıyla kişilik haklarına yapılan saldırılar düzenlenmiştir. YFCK'nın 277-3. maddesiyle küçüklerin resminin pornografik amaçla kullanılması, 277-24. maddesiyle ise küçükler tarafından erişilebilecek şiddet ya da pornografi içeren mesaj yayınlanması suç haline getirilmektedir [9].
Aynı kanunun bilişim suçlarını düzenleyen diğer maddeleri aşağıda belirtilmiştir.

- YFCK 323-1. maddesinde bilişim sistemlerine tamamen veya kısmen hukuka aykırı şekilde erişim düzenlenmekte, bu erişim sonucu sistemde bulunan verilerin silinmesi, değiştirilmesi ya da sistemin işlevinin değiştirilmesi ağırlatıcı neden olarak öngörülmektedir. (siber ihlal)
- YFCK 323-2. maddesinde bilişim sistemlerinin engellenmesi ya da tahrif edilmesi suç tipi olarak düzenlenmektedir.
- YFCK 323-3. maddesinde ise bilişim sistemi aracılığıyla işlenen dolandırıcılık eylemleri yaptırım altına alınmaktadır.
- YFCK 323-4. maddesinde ise bu suçların örgütlü biçimde işlenmesinde uygulanacak yaptırımlar düzenlenmektedir.

Yeni Fransız Ceza Kanunu'nun 323-1, 323-2 maddeleri Türk Ceza Kanunu'nun Bilişim Suçlarıyla ilgili 243 ve 244. maddelerinin düzenlenmesine de örnek olmuştur [9].

4.6. Hollanda Hukukunda Bilişim Suçları

1993 tarihli Computer Crime Act yasalaşmadan önce Hollanda polisi bilgisayar suçları ile mücadele etmek amacıyla özel bir birim kurmuştur. Üç pilot bölgede yapılan başarılı uygulamalardan sonra bölgeler arası bir bilgisayar suçları ile mücadele birimi kurulmuştur. Bilgisayar suçları birimleri Adalet Bakanlığına bağlı kriminal laboratuvarları, Information Technology and Crime Department of the National Criminal Intelligence Division ve Detective's Training Collage ile birlikte çok yakın çalışmalar yapmaktadır [10].

Hollanda ceza kanununda düzenlenen bilişim suçları;

- Verileri ele geçirme şartı aramaksızın bilişim sistemlerine hukuka aykırı erişim (madde 138a). (siber ihlal)
- Hukuka aykırı olarak ele geçirilen verinin kullanımı (madde 139a).
- Bilişim sistemleri kullanılarak sahtecilik (madde 232).

şeklinde tanımlanmıştır.

4.7. İngiliz Hukukunda Bilişim Suçları

İngiltere'de Bilişim Suçları, 29.08.1990 tarihinde yürürlüğe giren 29.06.2000 tarihli 'Bilgisayarın Kötüye Kullanılması Yasası' (Computer Misuse Act) ile düzenleme altına alınmıştır. Bu yasa üç ana bölüm ve bunların alt dalları olan on sekiz alt bölümden oluşmaktadır. Bu ana bölümler üçe ayrılmakta ve ilk ana bölüm bazı suç tiplemeleri düzenlenmekte, ikinci ana bölümde ceza mahkemesi hukukuna ilişkin düzenlemeler getirilmekte, üçüncü ana bölümde ise konuyla ilgili bazı genel düzenlemeler getirilmektedir [9].

Söz konusu kanunun düzenlediği bilişim suçları, sonradan yürürlüğe giren özel kanunlar ve bilişim suçlarını içeren kanunlar aşağıdaki listede belirtilmiştir.

- Yetkisiz olarak bilişim cihazlarına veri ve programlarına girilmesi (siber ihlal).
- Başka bir suçun işlenmesini sağlamak veya kolaylaştırmak amacıyla yetkisiz olarak bilişim cihazına girilmesi.
- Bilgisayar veri ve programlarının yetkisiz olarak değiştirilmesi.
- Müstehcen Yayınlar Kanunu
- Çocukların Korunması Kanunu

4.8. İrlanda Hukukunda Bilişim Suçları

İrlanda'da bilgisayar suçları ile mücadele etmek amacıyla 1991 yılında "The Computer Crime Unit" kurulmuş ve bu tür suçlarla mücadelede yetkili kılınmıştır. Temelde spesifik olarak bilgisayar suçları ile ilgili kanunlar olmasa da, 1991 yılında yasalaşan "Criminal Damage Act" bu tür suçlarla ilgili geniş tanımlamalar yapmaktadır [10].

1991 yılında çıkarılan bu yasa dört temel suçu ortaya koymaktadır.

1. Mülkiyete zarar vermek (bilgisayarlar ve veriler dahil).
2. Mülkiyete zarar vermek amacıyla tehdit etmek.
3. Bilişim sistemlerine yetkisiz giriş (siber ihlal).
4. Bilgisayarlara zarar vermek niyetiyle sahip olunan yazılımlar (yıkıcı siber suçlar)

"Criminal Damage Act" haricindeki diğer kanunlar aşağıda sıralanmıştır;

- The Copyright Act 1963
- The Criminal Evidence Act 1992
- The Data Protection Act 1988
- The Postal and Telecommunications Services Act 1983
- The Child Trafficking and Pornography Act 1998

4.9. İspanya Hukukunda Bilişim Suçları

İspanya'da siber suçlara ilişkin mevzuat Ceza Kanunu ile ilgili maddelerden ibarettir. Söz konusu suçlarla mücadelede şirketler, firmalar ve şahıslar tarafından

alınan tedbirler ise bu amaçla hazırlanmış koruma amaçlı yazılımlardan öteye gitmemektedir.

İspanyol Hükümeti yasalardaki düzenlemelere ilaveten, İçişleri Bakanlığı, Emniyet Genel Müdürlüğü bünyesinde bir birim oluşturmuştur. "Enformasyon Teknolojilerindeki Suçları Araştırma Birimi" adı altında faaliyet gösteren emniyet görevlileri teknoloji, iletişim, telekomünikasyon ve çocuk pornografisi alanlarında işlenen suçları ve ortaya çıkan şikayetleri takip etmektedir [10].

4.10. İtalyan Hukukunda Bilişim Suçları

Bu ülkede bilişim suçları İtalyan Ceza Kanunu'nda ve Ceza Usul Kanunu'nda değişiklik yapan 23.12.1993 tarih ve 547 sayılı yasa ile düzenlenmiştir. İCK'nın çeşitli maddelerine yapılan eklerle bilişim alanında gerçekleştirilen pek çok fiil türü suç haline getirilmiştir. Bunlara örnek olarak;

- Yazılımları kısmen veya tamamen tahrip eden, değiştiren, bilgi veya iletişim sistemlerinin doğru çalışmasını engelleyen programlarla saldırıda bulunmak
- Kamu yararına kullanılan tesislerin, bilgi sistemlerinin, veri, bilgi ve yazılımlarının içeriklerini tahrip etmek ve çalışmasını kesintiye uğratmak
- Bilgi veya iletişim sistemlerine fiziki olarak veya yazılım aracılığıyla yetkisiz olarak girmek, bilgi almak, alınan bilgileri yaymak, kayıtlar üzerinde tahribat yapmak veya sisteme maksatlı olarak yeni bilgiler ilave etmek
- Her türlü iletişimin engellenmesi, mahremiyetinin ihlal edilmesi, bu amaçla çeşitli cihaz ve sistemlerin kurularak enformatik ve telematik haberleşmenin kesintiye uğratılması, araya girilmesi veya iletişimin içeriğinin değiştirilmesi,
- Gizli dokümanların içeriğinin açıklanması, gizli kalması gereken kamu veya özel dokümanların içeriğinin yasa dışı olarak ele geçirilmesi ve açıklanması.
- Küçüklerin pornografik materyallerde kullanılması.
- Bilişim sistemlerinde bulunan verilere zarar vermek amacıyla yazılım üretilmesi ya da var olan bu tür yazılımın diğer sistemlere iletilmesi
- Bilişim sistemi aracılığıyla işlenen dolandırıcılık eylemleri
- Bilişim sistemleri marifetiyle kara para aklama eylemleri [9].

4.11. İsveç Hukukunda Bilişim Suçları

Bilişim suçlarına ilişkin olarak İsveç'te mevcut yasal düzenlemeler ceza kanunu içerisinde bulunan "bilgi hırsızlığı" ve "bilgi sistemlerini ihlal etme/bilgisayarlara yasa dışı giriş ya da verileri kötüye kullanma" şeklinde tanımlanabilecek suçlara ilişkin hükümlerdir [10].

İsveç Ceza Kanunu'nda bilişim suçu olarak tanımlanan fiiller;

- Bilişim sistemine yetkisiz erişim ve verilerin değiştirilmesi, yok edilmesi suçları ve bu eylemlere teşebbüs hali (siber ihlal).
- Bilişim sistemleri aracılığıyla işlenen dolandırıcılık suçları (siber dolandırıcılık).
- Çocuk pornografisine ilişkin suçların bilişim sistemleri aracılığıyla işlenmesi eylemleri [9].

4.12. İsviçre Hukukunda Bilişim Suçları

İsviçre'de siber terörizm ve teknolojik suçlarla mücadeleye ilişkin, "federal ceza yasası" ve "haksız rekabet yasası" adında federal iki yasa mevcuttur. "Federal ceza yasası" yasal olmayan yollardan teknolojik bilgi edinme, bilgi çalma ve bilgileri bozma gibi suçların cezalandırılmasını içermekte, "haksız rekabet yasası" ise, ticari amaçlı bilgisayar suçlarını içermektedir [10].

İsviçre Federal Ceza Yasası'nda düzenlenen bilişim suçları;

- Kayıt altına alınmış veya elektronik ortamda iletişime konu olan verilerin hırsızlığı.
- Bilişim sistemine teknik yollar kullanılarak girilmesi suretiyle yapılacak veri hırsızlığı (siber ihlal)
- Bilgisayarın yasa dışı biçimde eksik ve yanlış veriler kullanılarak etkilenmesi yoluyla sahtecilik amaçlı kullanılması.

4.13. Japonya Hukukunda Bilişim Suçları

Japonya'da 22.06.1987 tarihli 'Ceza Hukuku Alanında Bazı Hükümler Değişiklik Yapılmasına İlişkin Kanun' ile ceza kanununa bilişim suçları da dahil edilmiştir.

Bunlardan özellikle Japon CK'nın 246. maddesinde düzenlenen bilgisayar dolandırıcılığı suçu, Alman CK'nın ilgili 263 a paragrafıyla büyük oranda benzerlik göstermektedir. Japonya'da 13.02.2000 tarihinde yürürlüğe giren 'İnternete Haksız Girmenin Yasaklanması Hakkında Kanun' ile ceza hukuku alanında önemli düzenlemeler getirilmiştir. Japonya'da yapılan bu değişikliğin en önemli özelliği, Japon yasa koyucusunun Almanya'da olduğu gibi 'suçla korunan hukuksal değeri' dikkate alarak yasal düzenlemeyi yapmasıdır [9].

4.14. Kanada Hukukunda Bilişim Suçları

Kanada'da siber terörizm ve benzeri teknolojik suçlar halen mevcut ceza kanunu kapsamında işlem görmektedir. Ceza kanununun 1985 yılından itibaren yapılan değişikliklerle bu tür faaliyetler de suç kapsamına alınmıştır. Ceza kanununun 342. maddesi uyarınca hakkı olmadan ve sahtekarlık yoluyla elektromanyetik, akustik, mekanik veya başka bir cihaz yoluyla bir bilgisayar sistemini dolaylı veya doğrudan kesintiye uğratan herkes cezai müeyyideyi gerektiren bir suçun faili durumundadır. [10].

4.15. Malezya Hukukunda Bilişim Suçları

Malezya'da siber suçlarla mücadele, Haberleşme, Multimedya ve Enerji Bakanlığı sorumluluk alanına girmektedir. Malezya'da teknolojik suçlara ilişkin kanunlar:

- Digital Signature Act
- Multimedia Convergence Act
- Computer Crime Act
- Telemedicine Development Act
- Bu kanunlarda yer alan bilgisayar suçları da şöyledir:
- Bilgisayarlara izinsiz nüfuz etme, hasar verme
- Kullanıcı şifresi alışverişi
- Telif haklarının ihlali
- Marka sahteciliği
- Ticari sırları çalma

- Çocuklara yönelik istismar ve müstehcenlik
- İnternet dolandırıcılığı
- İnternet tacizi
- İnternet'le tehdit, korku, panik, huzursuzluk yayma

şeklinde düzenlenmiştir [10].

4.16. Rusya Hukukunda Bilişim Suçları

Rusya Federasyonu Ceza Kanununda Bilişim Suçlarıyla ilgili maddeler;

- Bilişim sistemleri kullanılarak her türlü pornografik materyalin üretimi ve dağıtımı (m242).
- Verilere ve yazılımlara hukuka aykırı etkide bulunma (m272).
- Veri ve yazılımlara zarar verecek yazılımların üretilmesi ve yayınlanması (m273).
- Bilişim sistemlerine ilişkin kuralların ihlali (m274).

şeklinde düzenlenmiştir [9].

4.17. Singapur Hukukunda Bilişim Suçları

Singapur hükümeti, bilgisayar üzerinden işlenen suçlarla mücadele için "Computer Misuse Act" ile elektronik ticareti düzenlemek ve işlemleri hukuki zemine oturtmak için "Electronic Transaction Act" yasalarını çıkarmıştır [10].

Bilişim Suçları "Computer Misuse Act" de şu şekilde sınıflandırılmıştır:

- Yetkisiz olarak bir bilgisayara veya sisteme girmek (siber ihlal).
- Suça yardımcı olmak maksadıyla veya bu amaçla sisteme girmek
- Bilgisayarda saklı bilgileri yetkisiz değiştirmek, silmek
- Bilgisayar kullanımını önlemek ve işlemez hale getirmek (yıkıcı siber suçlar)
- Yetkisiz bir bilgisayar hizmetinden yararlanmak
- Şifreleri çalmak veya bunları açıklamak

5. TÜRK HUKUK SİSTEMİNDE BİLİŞİM SUÇLARI

5.1. Türk Ceza Kanunu'nda Düzenlenen Bilişim Suçları

TCK' da bilişim suçları, esas olarak 'bilişim alanında suçlar' ve 'özel hayata ve hayatın gizli alanına karşı suçlar' bölümünde düzenlenmiştir. TCK'da bilişim suçu olarak nitelendirilebilecek suç tiplerinin yanı sıra bilişim sistemi aracılığıyla işlenebilecek ancak yalnızca bilişim suçu olarak tanımlanamayacak suç tipleri de yer almaktadır [9].

5.1.1. TCK Madde 243 (bilişim sistemine girme)

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

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

(3) Bu fiil nedeniyle sistemin içerdiği veriler yok olur veya değişirse, altı aydan iki yıla kadar hapis cezasına hükmolunur." [11].

Bilişim suçları konusunda yasal düzenlemeye sahip bütün hukuk sistemlerinde düzenlenen siber ihlal suçu, TCK'nın Bilişim Suçları başlığı altında yer alan ilk maddede düzenlenmiştir. Bu maddeye hangi maksatla olursa olsun bir bilişim sistemine girme fiili suç olarak tanımlanmıştır.

Suç unsurunun oluşması için bilişim sistemindeki verileri bozma veya verileri elde etme şartı aranmamaktadır. Fransız Ceza Kanunu'ndaki ilgili madde TCK'daki maddeye örnek olmuştur. Pek çok çağdaş ülkede siber ihlal suçu aynı kapsamda değerlendirilmektedir. Ayrıca bu maddede yer alan suç tipiyle, Avrupa Siber Suç Sözleşmesi'nin 2. maddesinde öngörülen 'hukuka aykırı erişim' düzenlenmesine paralellik sağlanmaktadır.

5.1.2. TCK Madde 244 (sistemi engelleme, bozma, verileri yok etme veya değiştirme)

“MADDE 244. - (1) Bir bilişim sisteminin işleyişini engelleyen veya bozan kişi, bir yıldan beş yıla kadar hapis cezası ile cezalandırılır.

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

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

(4) Yukarıdaki fıkralarda tanımlanan fiillerin işlenmesi suretiyle kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlamasının başka bir suç oluşturmaması halinde, iki yıldan altı yıla kadar hapis ve beşbin güne kadar adli para cezasına hükmolunur.” [11].

244. maddede bilişim sisteminin engellenişi yıkıcı siber suçları ve özellikle de internet sitelerine genel erişimi engelleyen Daniel of Service (DOS) saldırılarını ifade etmektedir. 244. Maddenin 2. fıkrasında Virüsler, Trojanlar, Keylogger ve Screenlogger kategorisindeki casus yazılımlarla yapılan uygulamalar da kapsam dahiline alınmıştır.

5.1.3. TCK Madde 245 (banka ve kredi kartlarını kötüye kullanma)

“MADDE 245. - (1) Başkasına ait bir banka veya kredi kartını, her ne suretle olursa olsun ele geçiren veya elinde bulunduran kimse, kart sahibinin veya kartın kendisine verilmesi gereken kişinin rızası olmaksızın bunu kullanarak veya kullandırtarak kendisine veya başkasına yarar sağlarsa, üç yıldan altı yıla kadar hapis cezası ve adlî para cezası ile cezalandırılır.

(2) 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 yedi yıla kadar hapis cezası ile cezalandırılır.” [11].

Banka veya kredi kartlarının kötüye kullanılması suçu, TCK'DA 525 b/2 maddesi yer alan 'bilişim sistemi aracılığıyla hukuka aykırı yarar sağlamak suçu' içerisinde değerlendirilen 'banka veya kredi kartının yetkisiz kullanımı eylemi' ile örtüşmektedir. İşte TCK'da bir suçun maddi unsuru oluşturan eylemlerden biri olan söz konusu kötüye kullanımlar TCK'nın 245. maddesinde bağımsız bir suç tipi haline getirilmiştir [9].

5.1.4. TCK Madde 246 (tüzel kişiler hakkında güvenlik tedbiri uygulanması)

"MADDE 246. - (1) Bu bölümde yer alan suçların işlenmesi suretiyle yararına haksız menfaat sağlanan tüzel kişiler hakkında bunlara özgü güvenlik tedbirlerine hükmolunur." [11].

5.1.5. TCK Madde 135 (kişisel verilerin kaydedilmesi)

"MADDE 135. - (1) Hukuka aykırı olarak kişisel verileri kaydeden kimseye altı aydan üç yıla kadar hapis cezası verilir.

(2) Kişilerin siyasî, felsefî veya dinî görüşlerine, ırkî kökenlerine; hukuka aykırı olarak ahlâkî eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin bilgileri kişisel veri olarak kaydeden kimse, yukarıdaki fıkra hükmüne göre cezalandırılır." [8].

Gelişen bilişim teknolojisiyle birlikte çok sık karşılaşılan ve aynı zamanda kişilik haklarına bir saldırı niteliği de taşıyan eylem türü, kişilerin rızaları olmaksızın kişisel verilerinin bilişim sistemlerine yerleştirilmesidir. Özellikle hastaneler, hastalarıyla ilgili, finans kurumlarının ve sigorta şirketlerinin müşterilerinin kredi olanağı ve ödeme gücüyle ilgili, ticari şirketlerin ise reklam ve pazarlama amacıyla bu tür verileri toplayıp kullandığı bilinmektedir.

Bu tür bilgilerin sanal ortama veri olarak aktarılması ve bu yapılırken bu verilerin ilgilisinin izni alınmaması inceleme konusu maddeyle suç tipi haline getirilmiştir.

Böylelikle, Avrupa Konseyi tarafından düzenlenen ve Türkiye'nin de taraf olduğu "Kişisel Nitelikli Verilerin Otomatik İşleme Tabi Tutulması Karşısında Şahısların Korunmasına Dair Sözleşme"nin ilgili düzenlemeleri yürürlüğe girmiştir.

5.1.6. TCK Madde 136 (verileri hukuka aykırı olarak verme veya ele geçirme)

“MADDE 136. - (1) Kişisel verileri, hukuka aykırı olarak bir başkasına veren, yayan veya ele geçiren kişi, bir yıldan dört yıla kadar hapis cezası ile cezalandırılır.” [11]. Bu düzenleme özellikle ABD ve İngiltere gibi ülkelerde çok sık karşılaşılan ve en fazla sayıda işlenen bilişim suçu olduğu ifade edilen kimlik hırsızlığı eylemlerine karşı uygulama alanı bulmaktadır.

Günümüzde internet’te pek çok kişisel bilgi bulunmaktadır. Bu bilgilerin çoğu kişilerin verdikleri rızaya dayanılarak çeşitli sitelere verilmektedir. Söz konusu bilgilerin hukuka aykırı olarak üçüncü kişilere verilmesi, yayılması ya da bu verilerin üçüncü kişiler tarafından ele geçirilmesinin suç tipi olarak düzenlenmesi bu madde ile gerçekleşmiştir.

5.1.7. TCK Madde 138 (verileri yok etmeme)

“MADDE 138. - (1) Kanunların belirlediği sürelerin geçmiş olmasına karşın verileri sistem içinde yok etmekle yükümlü olanlara görevlerini yerine getirmediklerinde altı aydan bir yıla kadar hapis cezası verilir.” [11].

Bu kanun maddesi ile hukuka uygun olarak sistemde bulunan kişisel verilerin sürekli olarak bu sistemlerde bulunması ve böylelikle her an ulaşılabilirliğinin sağlanmasının önüne geçilerek, verileri sistemden çıkarmayanlara yani bu konudaki görevlerini ihmal edenlere yaptırım uygulanmaktadır.

Ancak bilişim suçlarının tespitindeki en önemli unsurlardan birisi servis sağlayıcı veya bilişim sistemi log kayıtlarıdır. Yasa koyucunun yönetmelikler çerçevesinde kişisel bilgiler haricindeki kayıtların saklanması için belirli bir minimum süre öngörmesi gerekmektedir. Bu düzenleme, “5651 sayılı İnternet .Yoluyla Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçların Engellenmesi Hakkındaki Kanun” (bkz. Ek2) çerçevesinde gerçekleşmiştir.

5.1.8. TCK Madde 132 (haberleşmenin gizliliğini ihlâl)

“MADDE 132. - (1) Kişiler arasındaki haberleşmenin gizliliğini ihlâl eden kimse, altı aydan iki yıla kadar hapis veya adlî para cezası ile cezalandırılır. Bu gizlilik ihlâli

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 adlî para cezası ile cezalandırılır.

(4) Kişiler arasındaki haberleşmelerin içeriğinin basın ve yayın yolu ile yayınlanması hâlinde, ceza yarı oranında artırılır.” [11].

Günümüzde gelişen teknoloji sayesinde bilişim sistemleri kullanılarak özellikle de internet aracılığıyla elektronik posta, elektronik sohbet, internet üzerinden telefon görüşmesi ya da tele konferans gibi çeşitli yöntemlerle haberleşme sağlanmaktadır. Bilişim sistemi aracılığıyla gerçekleştirilen bu yeni haberleşme yöntemleri de söz konusu maddenin düzenlemesiyle koruma altına alınmakta ve bu tür haberleşmeyi ihlal edenler de cezalandırılmaktadır.

5.1.9. TCK Madde 124 (haberleşmenin engellenmesi)

“MADDE 124. - (1) Kişiler arasındaki haberleşmenin hukuka aykırı olarak engellenmesi hâlinde, altı aydan iki yıla kadar hapis veya adlî 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 hâlinde, ikinci fıkra hükmüne göre cezaya hükmolunur.” [11].

İnternet, modern dünyanın en yaygın ve etkin haberleşme ağı haline gelmiştir. Günümüzde gerçekleştirilen haberleşmenin büyük bir çoğunluğunu elektronik posta ve sohbet oluşturmaktadır. Bunların yanı sıra, iletim veri ağları üzerinden yapılan telefon görüşmeleri ve tele konferanslar da elektronik haberleşmenin diğer çeşitleri olarak görülmektedir.

TCK'nın inceleme konusu maddesiyle yalnızca haberleşme denildiği, bu haberleşme araçları tek tek sayılmadığı için haberleşme hangi araçla gerçekleştirilirse gerçekleştirilsin bunun engellenmesi inceleme konusu suçu oluşturacaktır. Bu nedenle bilişim sistemi aracılığıyla gerçekleştirilen haberleşmenin engellenmesi eylemleri de TCK'nın 124. maddesinde düzenlenen suç tipinin koruma kapsamında değerlendirilmektedir.

5.1.10. TCK Madde 125 (bilişim sistemi kanalıyla hakaret)

"MADDE 125. - (1) Bir kimseye onur, şeref ve saygınlığını rencide edebilecek nitelikte somut bir fiil veya olgu isnat eden ya da yakıştırmalarda bulunmak veya sövmek suretiyle bir kimsenin onur, şeref ve saygınlığına saldıran kişi, üç aydan iki yıla kadar hapis veya adlî para cezası ile cezalandırılır. Mağdurun gıyabında hakaretin cezalandırılabilmesi için fiilin en az üç kişiyle ihtilât ederek işlenmesi gerekir.

(2) Fiilin, mağduru muhatap alan sesli, yazılı veya görüntülü bir iletiyle işlenmesi hâlinde, yukarıdaki fıkrada belirtilen cezaya hükmolunur." [11].

Söz konusu maddenin 2. Fıkrasında fiilin sesli, yazılı veya görüntülü bir iletiyle işlenmesi durumunda da hakaret suçunun gerçekleştirileceği kabul edilmektedir. Bu nedenle hakaret suçunun bilişim sistemleri veya internet aracılığıyla işlenmesi de cezalandırılmaktadır.

5.1.11. TCK Madde 142 (nitelikli hırsızlık)

"MADDE 141. - (1) Zilyedinin rızası olmadan başkasına ait taşınır bir malı, kendisine veya başkasına bir yarar sağlamak maksadıyla bulunduğu yerden alan kimseye bir yıldan üç yıla kadar hapis cezası verilir.

(2) Ekonomik bir değer taşıyan her türlü enerji de, taşınır mal sayılır.

MADDE 142. - (1) Hırsızlık suçunun;
e) Bilişim sistemlerinin kullanılması suretiyle işlenmesi hâlinde, üç yıldan yedi yıla kadar hapis cezasına hükmolunur." [11].

Bu maddede, hırsızlık fiilinin tanımında “taşınır bir mal” ifadesinin kullanılmış olması hukuk öğretisinde tartışmalara konu olmaktadır. Bilişim sistemleri aracılığıyla taşınır bir malın bulunduğu yerden alınması fiilinin olabilirliği tartışılmakla birlikte “siber hırsızlık” kapsamındaki suçun unsurlarını karşılamadığı düşünülmektedir. Ekonomik bir değer taşıyan her türlü enerjinin de taşınır mal olarak kabul edilmesi her ne kadar suçun klasik anlam ve kapsamını genişletmiş olsa da; bilişim sistemlerinde bulunan verilerin enerji olarak tanımlanması uygun görülmemektedir.

Bu tartışmalara rağmen, bilişim sistemleri kullanılarak banka hesaplarında yapılan yetkisiz para transferlerini, paranın bulunduğu yerden alınması fiili kapsamında düşünmek mümkündür.

5.1.12. TCK Madde 158 (nitelikli dolandırıcılık)

“MADDE 157. - (1) Hileli davranışlarla bir kimseyi aldatıp, onun veya başkasının zararına olarak, kendisine veya başkasına bir yarar sağlayan kişiye bir yıldan beş yıla kadar hapis ve beşbin güne kadar adlî para cezası verilir.

Nitelikli dolandırıcılık;
MADDE 158. - (1) Dolandırıcılık suçunun;
f) Bilişim sistemlerinin, banka veya kredi kurumlarının araç olarak kullanılması suretiyle işlenmesi hâlinde, iki yıldan yedi yıla kadar hapis ve beşbin güne kadar adlî para cezasına hükmolunur.” [11].

Türk Ceza Kanunu, siber dolandırıcılık fiilini ayrı bir kanun maddesinde düzenlemek yerine, nitelikli dolandırıcılık kapsamında bir suç olarak tanımlamıştır.

5.1.13. TCK Madde 226 (müstehcenlik)

“MADDE 226. - (1) a) Bir çocuğa müstehcen görüntü, yazı veya sözleri içeren ürünleri veren ya da bunların içeriğini gösteren, okuyan, okutan veya dinleten,
b) Bunların içeriklerini çocukların girebileceği veya görebileceği yerlerde ya da alenen gösteren, görülebilecek şekilde sergileyen, okuyan, okutan, söyleyen, söyleten Kişi, altı aydan iki yıla kadar hapis ve adlî para cezası ile cezalandırılır.

(3) Müstehcen görüntü, yazı veya sözleri içeren ürünlerin üretiminde çocukları kullanan kişi, beş yıldan on yıla kadar hapis ve beşbin güne kadar adlî para cezası ile cezalandırılır. Bu ürünleri ülkeye sokan, çoğaltan, satışa arz eden, satan, nakleden, depolayan, ihraç eden, bulunduran ya da başkalarının kullanımına sunan kişi, iki yıldan beş yıla kadar hapis ve beşbin güne kadar adlî para cezası ile cezalandırılır." [11].

Müstehcenlikle ilgili söz konusu madde hukuk çevrelerinde sürekli tartışma konusu olmaktadır. Müstehcenlik kavramının zamana ve aynı toplum içerisindeki farklı kültür gruplarına göre değişim göstermesi kanun maddesinin bir eksikliği olarak yorumlanmakta ve müstehcenlik sözcüğü yerine pornografi sözcüğünün seçilmesi gerektiği vurgulanmaktadır. Ayrıca çocuk pornografisinin Avrupa Siber Suç Sözleşmesi'nin ilgili maddeleri örnek alınarak ayrı bir suç tipi olarak düzenlenmeyişi de kanun maddesine yönelik eleştiriler arasında yer almaktadır.

5.2. 5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun

Ülkemizde bilişim suçlarının önlenmesi kapsamında yürürlüğe giren kanunlar arasında en çok tartışılanı 5651 sayılı kanundur (Bkz. Ek 2). Bilişim suçları konusunda geniş kapsamlı bir yasa taslağı hazırlanmışken; Ulaştırma Bakanlığı tarafından hazırlanıp yürürlüğe konulan 5651 sayılı kanun, bilişim suçu türlerini ve yaptırımlarını tanımlamak yerine "erişimin engellenmesi" yöntemini tercih eden çözümler getirmiştir.

Erişimin engellenmesi kararı, soruşturma evresinde hâkim, kovuşturma evresinde ise mahkeme tarafından verilmektedir. Soruşturma evresinde, gecikmesinde sakınca bulunan hallerde Cumhuriyet Savcısı tarafından da erişimin engellenmesine karar verilebilir. Erişimin engellenmesi kararına neden olan fiiller aşağıda belirtilmiştir.

5.2.1. Erişimin engellenmesi kararı ve yerine getirilmesi

MADDE 8 – (1) İnternet ortamında yapılan ve içeriği aşağıdaki suçları oluşturduğu hususunda yeterli şüphe sebebi bulunan yayınlarla ilgili olarak erişimin engellenmesine karar verilir:

a) 26/9/2004 tarihli ve 5237 sayılı Türk Ceza Kanununda yer alan;
1) İntihara yönlendirme (madde 84),
2) Çocukların cinsel istismarı (madde 103, birinci fıkra),
3) Uyuşturucu veya uyarıcı madde kullanılmasını kolaylaştırma (madde 190),
4) Sağlık için tehlikeli madde temini (madde 194),
5) Müstehcenlik (madde 226),
6) Fuhuş (madde 227),
7) Kumar oynanması için yer ve imkân sağlama (madde 228),
suçları.
b) 25/7/1951 tarihli ve 5816 sayılı Atatürk Aleyhine İşlenen Suçlar Hakkında Kanunda yer alan suçlar.

Müstehcenlik maddesi TCK 226. maddede olduğu gibi tartışmalara neden olmakta ve çerçevesi belirli olmayan bir suçu tanımladığı düşünülmektedir.

5.3. Fikir ve Sanat Eserleri Kanunu'nda Düzenlenen Bilişim Suçları

Ülkemizde kişilerin emek sarf ederek ortaya çıkardığı düşün ve sanat ürünlerinin 'eser' kavramıyla tanımlandığı ve koruma altına alındığı 5846 sayılı Fikir ve Sanat Eserleri Kanunu'nda, 07.06.1995 tarih ve 4110 sayılı yasa ile kapsamlı bir değişiklik yapılmıştır. Bu değişiklik ile ülkemiz hukukuna getirilen yeniliklerden biri de FSEK'in 2. maddesinde eser kavramının tanımı yapılırken bilişim yazılımlarının da bu kavram içinde sayılması ve yasanın koruma kapsamına alınmasıdır. Buna bağlı olarak yasanın 71., 72. ve 73. maddelerinde de eser sahibinin haklarının korunması açısından düzenlenen suç tiplerinin konusunda bilişim yazılımları da dahil edilmiştir [9].

Söz konusu değişiklik yasasıyla bilişim yazılımlarının da eser kavramı içine alınmasına gerekçe olarak, ülkemizde hızla gelişen yazılım endüstrisinin ürünleri

olan bilişim yazılımları üzerindeki fikri hakların FSEK tarafından açık ve net bir şekilde korunmaması gösterilmektedir. Bu değişikliğin zorunluluğu konusunda ise 4110 sayılı değişiklik yasasının hükümet gerekçesinde şu ifadelere yer verilmektedir: “Bilgisayar program teknolojisi ülkemiz endüstriyel gelişimi için temel öneme sahip bir konu haline gelmektedir. Bir bilgisayar programı gerçekleştirmek için insan gücüne, teknik ve mali yatırıma ihtiyaç vardır. Buna karşılık ortaya çıkan programın haksız kullanılması çok kolay ve çok az maliyetle yapılabilmektedir. Bu durum bilgisayar programlarının fikri haklarının çok iyi korunmasını gerektirmiştir” [9].

Uluslararası hukukta ve karşılaştırmalı hukukta, bilişim yazılımlarının da ‘eser’ olarak kabul edilmesi için çok sayıda çalışma yapılmış ve bu konuda çeşitli metinler hazırlanmıştır. FSEK’de gerçekleştirilen bu değişikliğe de Avrupa Yazılım Yönergesi kaynak oluşturmuş ve böylece yapılan değişiklik ile 14.05.1995 tarihli Avrupa Konseyi Direktifi ile FSEK’in ilgili maddeleri uyumlu hale getirilmiştir.

FSEK’in bu çalışma açısından inceleme konusunu oluşturan 71., 72. ve 73. maddelerinde, sırası ile manevi haklara tecavüz, mali haklara tecavüz ve diğer suçlar başlığı altında üç farklı suç tipi düzenlenmiştir. Bunlardan 71. maddede eserle ilgili hak sahibinin manevi haklarına yönelik eylemleri içeren suç tipleri, 72. maddede eserle ilgili hak sahibinin maddi haklarına yönelik eylemleri içeren suç tipi ve son olarak 73. madde de eserin, hak sahibinin çıkarları aleyhine kullanıldığı diğer eylemleri içeren suç tipi yer almaktadır. Böylece FSEK’in 2. maddesinde yapılan değişiklik sonucu bilişim yazılımlarının hukuka aykırı olarak çoğaltılması ve kullanılması eylemleri suç tipi olarak düzenlenmiştir [9].

5.3.1. FSEK Madde 71

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

depolayan kişi hakkında bir yıldan beş yıla kadar hapis veya adlî para cezasına hükmolunur.

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

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

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

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

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

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

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

5.3.2. FSEK Madde 72

Bir bilgisayar programının hukuka aykırı olarak çoğaltılmasının önüne geçmek amacıyla oluşturulmuş ilave programları etkisiz kılmaya yönelik program veya teknik donanımları üreten, satışa arz eden, satan veya kişisel kullanım amacı dışında elinde bulunduran kişi altı aydan iki yıla kadar hapis cezasıyla cezalandırılır

6. SİBER İHLAL YÖNTEMLERİ

Bilişim sistemlerine yetkisiz erişim fiili, en eski, en yaygın ve en çok bilinen bilişim suçu türüdür. Ülkemizde yürürlükte bulunan Türk Ceza kanununun bilişim suçları bölümünde yer alan dört madde olan 243, 244, 245 ve 246. maddelerden 243. madde yetkisiz erişim fiilini suç olarak tanımlamakta ve verilecek cezayı düzenlemektedir. Ayrıca bilişim suçlarıyla ilgili yasal düzenlemesi bulunan tüm hukuk sistemlerinde öncelikli bir suç olduğu için söz konusu suçun açılımı ve türleri bu bölümde detaylı olarak incelenecektir.

6.1. Kullanıcı Tabanlı Siber İhlal Yöntemleri

Kullanıcı tabanlı siber ihlal yöntemleri, bilişim sistemlerine herhangi bir saldırgan yazılım veya sistemdeki güvenlik açıkları gibi teknik unsurlar kullanmadan doğrudan kullanıcıların dikkatsizlik, dalgınlık veya tecrübesizlik gibi zayıf yönlerini dikkate alarak uygulanan erişim teknikleridir.

6.1.1. Şifre ve gizli soru tahmini

Yetkisiz erişim amacıyla en yaygın olarak kullanılan yöntem, şifre veya şifreye erişim için kullanılan gizli soru yanıtının tahmin edilmesidir. Bir çok bilişim sistemi, kullanıcıların şifrelerini unutmaları durumunda kullanılmak üzere bir gizli soru ve yanıt ikilisinin tanımlanmasını istemektedir. Günümüzde telefon bankacılığı işlemlerinde banka yetkilileri tarafından sorulan anne kızlık soyadı, gizli soru ve yanıt ilişkisinin en yaygın örneğidir.

6.1.2. Omuz sörfü

Kullanıcıların bilişim sistemlerine erişim şifrelerini yazarken gözlenmesi, gizlice izlenmesi, ajanda post-it, not kağıtları gibi şifre yazılabilecek materyallerin incelenmesi şeklinde uygulanan bir yöntemdir.

6.2. Yazılım Tabanlı Siber İhlal Yöntemleri

Yazılım tabanlı yetkisiz erişim yöntemlerinde bir bilişim sistemine erişim için kullanılan temel araçlar şifreyi sözlük atağı (dictionary attack) ya da kaba kuvvet algoritmaları (brute force attack) yöntemleriyle çözmek olarak uygulanmaktadır. İnternet teknolojisinin gelişmesiyle birlikte söz konusu temel yetkisiz erişim araçlarına trojan, keylogger ve screen logger algoritmaları da eklenmiştir.

6.2.1. Sözlük atağı (dictionary attack)

Bir bilişim sistemini koruyan şifrenin, sözlükte bulunan bir sözcükle eşdeğer olduğu varsayımına dayanan bir saldırı yöntemidir. Şifre denemelerini otomatik olarak tekrarlayan bir algoritmanın bir metin dosyasındaki sözcükleri denemesiyle çalışan sözlük atağı yöntemi, uzak sistemlere yetkisiz erişim amacıyla kullanılmaktadır.

6.2.2. Kaba kuvvet algoritmaları (brute force attack)

Bir bilişim sistemini veya bir belgeyi koruyan şifrenin, bütün harf, rakam ve özel karakter kombinasyonlarını kullanan bir algoritma aracılığıyla çözülmesini sağlayan bir saldırı yöntemidir. Sözlük atağından farklı olarak anlamlı anlamsız bütün harf, rakam ve karakter kombinasyonları kullanılmakta ve şifre ne kadar karmaşık ve uzun olursa olsun mutlak suretle çözülmektedir.
Kaba kuvvet algoritmaları, çok uzun süren işlemler olduğu ve gelişen teknolojiyle birlikte önleyici teknikler geliştiği için uzak sistemleri tehdit etmemektedir. Ancak şifreli belgelerin (word, excel, pdf) şifrelerini çözmek için halen kullanılmakta olan bir yöntemdir

6.2.3. Tuş kaydedici yazılımlar (keylogger)

Kullanıcının klavye'de basmış olduğu tuşları, basım sırasına göre bir metin dosyası içerisine yazıp daha sonra e-posta ya da uzaktan erişim yöntemiyle uzak sisteme transfer eden yazılım türüne keylogger adı verilmektedir.

6.2.4. Ekran kaydedici yazılımlar (screenlogger)

Kullanıcının fare ile her tıklama hareketi sonucunda, farenin ekranda durduğu noktanın köşegen merkezi olan ve 100x100 (bu değer değişebilmektedir) piksel büyüklüğündeki bir grafiği düşük çözünürlükte kaydederek kullanıcı bilgisayarının sabit diskinde daha sonra alınmak üzere saklayabilen veya e-posta yolu ile uzak sisteme transfer eden yazılım türüne verilen addır.

6.2.5. Truva atları (trojanlar)

Kullanıcı bilgisayarında, açılışta çalışma özeliği bulunan gizli bir sunucu (server) oluşturarak bütün sistem kaynaklarını uzak sistemdeki kişinin kullanmasını sağlayan, bilgisayarda yapılan bütün işlemleri izleme, dinleme ve müdahale etme yetkisini uzak sisteme devreden yazılım türüne trojan adı verilmektedir.

6.3. Yazılım Tabanlı Siber İhlal Önlemleri

Şifre ve gizli soru tahmini yöntemine karşı kullanıcının tanımladığı şifre, bilişim sistemlerinde bulunan sözlük dosyaları ile karşılaştırılarak kullanıcının sözlükte bulunan sözcükleri şifre olarak tanımlaması engellenmektedir. Ayrıca kullanıcı adıyla tanımlanan şifre arasındaki uyumlar da farklı algoritmalar tarafından kontrol edilmektedir.

Sözlük atağı algoritmalarının bilişim sistemlerine tekrarlanan otomatik şifre deneme yöntemini etkisiz hale getirmek için günümüzde bazı güvenlik önlemleri kullanılmaktadır.

Sunucuya gönderilen şifre denemelerine sınırlama getiren algoritmalar, güvenlik resmi ya da güvenlik kodu olarak bilinen CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) algoritmaları, tek kullanımlık şifre üreten token cihazları, mobil imza, e-imza gibi yöntemler şifrelerin saldırganlar tarafından robot algoritmalar aracılığı ile elde edilmesini engellemektedir.

7. Sosyal Mühendislik (Social Engineering)

Bilgisayar ve ağ güvenliği açısından sosyal mühendislik, insan davranışındaki unsurları güvenlik açıkları olarak değerlendirip, bu açıklardan faydalanma yöntemiyle güvenlik süreçlerini aşarak sistem yöneticisi ya da kullanıcıların yetkilerine erişim tekniklerini kapsayan bir terimdir.

Sosyal mühendislik kavramını tanımlayan ve bilişim dünyasında konuyla ilgili en temel kaynaklardan biri olarak kabul edilen 'Art Of Deception' adlı kitabın yazarı Kevin Mitnick, kitabında insan unsurunu ağ güvenliğinin en zayıf halkası olarak tanımlamaktadır [12].

Bilişim teknolojilerinin gelişimine paralel olarak bilişim sistemlerine yönelik saldırılarda ve bilişim suçlarında önemli artışlar gözlenmektedir. Bilişim sistemlerindeki gelişmeler, kullanımı yaygınlaşan yeni platformlar (mobil teknolojiler, cep bilgisayarları) yeni güvenlik açıklarını da beraberinde getirmektedir. Ayrıca, bilişim teknolojisindeki yeni araçlar (bilgisayar dilleri, veri tabanı yapıları) yeni saldırı yöntemlerinin gelişmesine olanak sağlamaktadır. Bilişim teknolojisindeki hızlı gelişim, bilişim suçlarının çeşitliliği ve yaygınlığının daha büyük oranlarda artmasına neden olmaktadır.

7.1. Tersine Sosyal Mühendislik

Sosyal mühendislik kavramının farklı bir açılımı olan 'tersine sosyal mühendislik (reverse social engineering)' kavramı ise; sosyal mühendislik yöntemi ile saldırıya uğrayan mağdurun, yardım almak amacıyla farkında olmadan sistemine saldırı düzenleyen kişiyle temas kurması olarak tanımlanmıştır [12].

7.2. Sosyal Mühendislik Kanalları

Sosyal mühendislik yöntemiyle yapılan yetkisiz erişim denemeleri yalnızca bir kullanıcının hedef alınması veya kullanıcıların toplu halde hedef alınması şeklinde iki farklı biçimde gerçekleşmektedir.

Yalnızca bir kullanıcının hedef alındığı yetkisiz erişim denemelerinde; yüz yüze, telefon, faks veya e-posta iletişim kanalları kullanılmaktadır. Söz konusu iletişim

yöntemleri doğrudan hedef alınan kişiye karşı olduğu gibi, kimlik taklidi yöntemiyle sistem yöneticilerine yönelik olarak da uygulanabilmektedir.

İletişim kanallarının kitlesel hedeflere yönelik olduğu durumlarda genellikle aldatıcı web sitesi ve yığın e-posta iletişim kanalının birleşimi tercih edilmektedir. Fake mail, phishing, e-posta aldatmacaları ve hoax e-postaları kitlesel hedefleri aldatmaya yönelik olarak uygulanan yöntemlerin başlıcalarıdır.

7.3. Sosyal Mühendislik Yönteminde Senaryolar (Pretexting)

Sosyal mühendislik yöntemi, bireylerin davranış karakteristikleri ve niteliklerindeki unsurları güvenlik açıkları olarak değerlendirerek sistemlere yetkisiz erişim olanağı elde etmektedirler. Aşağıda söz konusu genel geçer davranış modellerinden bazıları ve modellerdeki rol aktör davranışları örnek olarak verilmiştir;

- Otoriter tavırlar insan davranışlarını yönlendirir ve etkiler.

Sosyal mühendislik yönteminin en yaygın kullanım biçimlerinden birisi saldırının hedefi olan kişiye karşı otoriter bir kimlikle yaklaşmaktır. Genellikle kamu görevlisi ya da kolluk kuvveti rolüyle iletişim kuran saldırgan, şifre ya da kişisel bilgileri elde etmek amacıyla mağdurun farkında olmadan adli bir kovuşturmaya maruz kaldığını veya hesap bilgilerini elde eden bir kişi tarafından zor durumda bırakıldığını öne sürerek kişisel bilgilerini almaya çalışır.

- Aynı karakteristik özelliklere, zevk ve tercihlere sahip kişiler birbirlerini daha kolay etkiler.

Sosyal mühendislik yönteminin diğer yaygın kullanım biçimi şifre veya kişisel bilgileri elde edilmek istenen kişiye ortak ilgi alanlarının var olduğu hissi yaratılarak güven verilmesi ve diyalog sonrası elde edilen bilgiler yardımıyla özel bilgilere ulaşılması şeklinde gerçekleşmektedir.

- Yardımsever tavırlar güven telkin eder

Sosyal mühendislik yöntemlerinde kullanılan bir diğer rol, güven vermeye yönelik olarak uygulanan yardımsever tavırlardır. Özellikle ATM cihazlarında işlem yapan kişileri hedef alan senaryolarda mağdurun ATM cihazında kalması sağlanan banka kartının iptali için şifre bilgisinin istenmesi söz konusu rolün en yaygın örneğidir.

- İnsanlar az bilgiye sahip oldukları konularda kendilerine söylenen sözlere inanma eğilimindedir.

Otoriter tavırların insan davranışları üzerindeki etkisi ve yardımsever tavırların güven telkin etmesi varsayımlarının birleşimi olan senaryolarda genellikle teknik konularda bilgisi yetersiz olan kişiler seçilmekte ve söz konusu davranış niteliği otoriter veya yardımsever bir tavırla suistimal edilebilmektedir.

- İnsanlar zor durumdaki kişilere yardımcı olmaktan hoşlanırlar.

Bireylerin yardımseverliğini hedef alan aldatıcı senaryolarda kullanılan varsayımlardan birisi de zor durumdaki kişilere yardımcı olma davranışıdır. Özellikle ATM cihazlarında işlem yapan kişileri hedef alan senaryolarda, para çekme limiti dolduğu için parasız kalan mağdur rolünü oynayan kişilerin, başkalarının hesabını havale veya EFT için kullanmaları söz konusu davranış niteliğinin kötü niyetle kullanımının örneğidir.

7.4. Teknoloji Tabanlı Sosyal Mühendislik Yöntemleri

Sosyal mühendislik yöntemlerinin günümüzde hızla yaygınlaşan kullanım biçimleri, iletişim teknolojilerini ve karmaşık olmayan algoritmaları destek unsur olarak içermesi veya teknoloji odaklı zarar verici uygulamalara (virüs, yığın e-posta vb.) yardımcı unsur olarak tercih edilmesi şeklinde gözlenmektedir.

7.4.1. Fake mail

Genellikle e-posta servislerindeki kullanıcı şifrelerine ulaşmak amacıyla kullanılan bir sosyal mühendislik yöntemidir. Gönderildiği e-posta sunucusunun bir hata sonucunda kullanıcıya şifre sorması için hazırlanan web sayfasının görünüş olarak kopyasının açılabilir bir web bağlantısı olarak gönderilmesi şeklinde gerçekleştirilmektedir. Açılan sahte web sayfasına girilen şifre bilgileri sunucu yerine ortadaki adam (man in the middle) olarak adlandırılan saldırgana ulaşmaktadır.

Fake mail saldırılarının sayısı, yeni yıl ve bayram gibi özel günlerde çoğalmakta ve genellikle elektronik kart, promosyon duyurusu şeklinde düzenlenerek kullanıcının dalgınlığından faydalanma yöntemi seçilmektedir.

7.4.2. Phishing

Açılımı password harvesting fishing sözcüklerinden oluşan phishing yöntemi oltacılık olarak da adlandırılmaktadır. Genellikle banka ve finans sitelerinden gönderilmiş gibi hazırlanan ve kullanıcıları tedirgin edecek ifadeler ile birlikte ilgili kurum ya da kuruluşun sahte web site bağlantısını içeren e-posta iletileridir. İletiler açıldığında kullanıcıların girdiği bilgiler, ortadaki adam olarak tanımlanan saldırgana iletilmekte, kullanıcıya ise sistemin geçici olarak servis dışı olduğuna ilişkin bir mesaj görüntülenmektedir.

7.4.3. Elektronik dolandırıcılık (cyberfraud) ve sosyal mühendislik

Günümüzde sosyal mühendislik uygulamaları sistemlere yetkisiz erişim ve kişisel bilgi temini amacıyla olduğu kadar, haksız kazanç elde etmek için de kullanılmaktadır. Çeşitli ve sürekli olarak yenilenen senaryolar aracılığıyla yapılan saldırıların en yaygın örnekleri arasında yeşil kart, loto, kara para transfer, sahte ürün tuzakları bulunmaktadır.

7.4.4. Sosyal mühendislik ve bilgisayar virüsleri

Bazı bilgisayar virüsleri yayılma hızlarını artırmak için sosyal mühendislik tekniklerini kullanmaktadırlar. İlk örneği Win32/Sober adlı virüs olan söz konusu virüsler yerleştikleri bilgisayar sistemlerindeki belge adlarını inceleyerek bilgisayar kullanıcısının iş veya hobi niteliklerine uygun bir isimle kopyalarını adres defterindeki kişilere göndermektedir.

Sober virüsü için Microsoft'un web sitesinde 'Bu solucan, kullanıcıları sosyal mühendislik yoluyla e-postadaki ekli bir dosyayı veya yürütülebilir dosyayı açmaya ikna etmeye çalışır. Alıcı dosyayı ve yürütülebilir dosyayı açarsa, solucan kendisini sistemin adres defterindeki tüm kişilere gönderir.' açıklaması yapılmıştır [13].

7.4.5. Sosyal mühendislik ve yığın e-postalar (spam)

Yığın e-postaların küresel bir sorun haline gelmesi sonucu kullanıcıların e-postaları açmadan silme davranışlarını geliştirmeleri nedeniyle, posta göndericileri sosyal mühendislik yöntemlerini uygulamaya başlamıştır. E-postaların konu başlığında re: ibaresinin bulunması, bir başvurunun tamamlanması ya da bir hizmet veya servisin süresinin dolmasına ilişkin sahte mesajların yer alması gibi örnekler yığın e-postaların yayılmasında sosyal mühendislik yöntemlerinin uygulama örnekleridir.

7.4.6. E-posta aldatmacaları (hoax)

E-posta adreslerini yığın e-posta gönderen kişi ve kuruluşlara temin etmek için hazırlanan sahte içerikli e-postalarda sosyal mühendislik teknikleri yaygın olarak kullanılmaktadır. Bu tür e-postalar, toplumsal açıdan tepki yaratması amaçlanan aldatıcı, yanlış bilgiler içermekte ve genellikle son bölümlerinde çok sayıda kişiye iletilmesi için telkinler yer almaktadır. Bir ülke ya da kuruma yönelik gerçek dışı bilgiler, sağlıkla ilgili tehditler, kan aranması, zor durumdaki kişilere yardım talebi gibi çeşitleri bulunan e-posta aldatmacaları uzun yıllardır kullanılmakta olan etkin bir yöntemdir.

8. BİLİŞİM SUÇLARIYLA MÜCADELEDE KARŞILAŞILAN GÜÇLÜKLER

8.1 İnternet'in Yapısından Kaynaklanan Güçlükler

İnternet'in merkezi bir otoriteye bağlı olmayışı, dolayısıyla da sistemin bütününü kapsayan bir yasanın bulunmayışı, bilişim suçlarıyla mücadelede karşılaşılan en önemli engellerden birisidir.

İnternet'in yapısından kaynaklanan bir diğer sorun, internete bağlı herhangi bir bilgisayardan yapılan sunum hizmetinin dünya üzerinde internete bağlı bütün bilgisayarlar tarafından eşit şekilde erişilebilir olmasından kaynaklanmaktadır. Ülkelerin hukuk sistemleri arasında farklılıklar bulunmaktadır. Özellikle küçük ada devletlerinin yasaları, diğer devletlere göre belirgin ölçülerde noksanlıklara sahiptir. Bilişim suçlarının kaynağı olan bölgeler incelendiğinde, kumar ve bahis sitesi

yayınlarının, sanal dolandırıcılık e-postalarının kaynağının yoğunlukla küçük ada devletleri olduğu görülmektedir [14].

İnternet bağlantısı ile yapılan bir erişimin izini kaybettiren yöntemlerin varlığı da internet kaynaklı sorunlar arasında büyük önem taşımaktadır.

8.2. Sayısal Delillerin Yapısından Kaynaklanan Güçlükler

Bilişim suçlarının tespitinde büyük öneme sahip olan sayısal delillerin çabuk bozulabilir, değiştirilebilir ve yanıltıcı durumlara yol açabilir olması (uzaktan erişimle bilgisayara dosya yüklenebilmesi gibi) bilişim suçlarıyla mücadelede engel yaratan önemli etkenlerden biri olarak kabul edilmektedir.

8.3. Uygulamadaki Eksikliklerden Kaynaklanan Güçlükler

Bilişim suçlarıyla mücadele için yasal düzenlemelerin yanı sıra uygulama ve yönetmeliklerin de güncel ve gelişen koşullara uyum sağlayabilecek nitelikte olması gerekmektedir. İnternet kafelerde ve kablosuz internet erişim bölgelerinde kimlik denetimi olmayışı, bilişim suçlarının bu bölgelerden işlenmesine yol açmakta ve suçluya ulaşma aşamasında önemli engeller yaratmaktadır. Bilişim suçlarıyla mücadele için kablosuz internet kullanım noktalarında ücretli veya ücretsiz şifre tahsis edilmesi zorunlu hale getirilmelidir. Ülkemizde yıllardır kimler tarafından kullanıldığı denetlenmeyen internet kafelere kablosuz erişim noktalarının da eklenmesi sonucunda bilişim suçlarında belirgin artışlar olacağına kesin gözüyle bakılmaktadır [15].

8.4. Diğer Güçlükler

Bilişim suçlarıyla mücadele konusunda bir başka önemli engel, konu hakkındaki bilgi ve bilinç yoksunluğundan kaynaklamaktadır. Bireylerin kendilerine yöneltilen fiillerin suç kapsamında olup olmadığı konusunda yetersiz bilgiye sahip olmaları, bazı suçların yargıya intikal etmesini ve suçluların tespitini engellemektedir.

9. ANKET ÇALIŞMASI

Bilişim suçlarının sosyo-kültürel seviyelere göre algı analizi konusu için çalışma alanı olarak Başkent Üniversitesi öğrencileri ve akademik çalışanlarından oluşan bir örneklem seçilmiştir. Çalışma alanının üniversite olarak seçilmesinin nedeni; Türkiye'nin Ortadoğu Teknik Üniversitesi üzerinden ilk İnternet erişim günü olan 12 Nisan 1993 tarihinden itibaren ilk üç sene süresince İnternet'i yalnızca üniversite çalışanları ve öğrencilerinin kullanmış olması, günümüzde de İnternet'i en çok kullanan sosyal kesimin akademisyenler ve öğrenciler olmasıdır.

Anket araştırması için bilgisayar donanım ve yazılım eğitimi veren Bilgisayar Mühendisliği, İstatistik ve Bilgisayar Bilimleri, Yönetim Bilişim Sistemleri, Bilgisayar ve Öğretim Teknolojileri bölümleri, konunun hukuksal algılaması açısından Hukuk Fakültesi ve diğerlerinden bağımsız eğitim aldığı için kontrol grubu olarak Türk Dili ve Edebiyatı bölümü seçilmiştir.

Anket dört bölümden oluşmaktadır;

1. Demografik bilgiler
2. Teknoloji, bilgisayar ve İnternet konularına yönelik ilginin ölçülmesi ve beraberinde katılımcının İnternet kullanım profilinin belirlenmesi
3. Farklı ülkelerin hukuk sistemlerine göre bilişim suçu sayılan 14 fiillin kişisel algı düzeyinde suç şiddeti açısından değerlendirilmesi
4. Bilişim suçu olan veya olmayan 24 fiilin kişisel algı düzeyinde ahlaki açıdan doğru ve hukuksal açıdan suç olup olmamasının farklı düzeylerde belirlenmesidir.

9.1. Hipotezler

Bu çalışmada veriler, öncelikle eğitim gruplarına göre; bilgisayar bilimleri, hukuk ve kontrol grubu olarak seçilen Türk dili ve edebiyatı bölümlerine ayrılmıştır. Bu bölümlerin bilişim suçları algısı açısından homojen bir yapıda olacağı öngörülmüştür. Bölümlerin eğitim programlarında bilişim suçlarıyla ilgili derslerin bulunmayışı ve konuya ilişkin eğitim faaliyetlerinin yetersizliği, grupların homojen olacağı hipotezinin temel dayanağı olarak belirlenmiştir.

Anket verilerinin diğer gruplanma biçimleri katılımcıların akademik konumları (öğretim elemanı – öğrenci) ve cinsiyet şeklindedir. Söz konusu iki grubun yapısal özellikleri nedeniyle kontrol grupları oluşturulmamış ve bilişim suçu algısının bu gruplarda da genel olarak homojen bir yapıya sahip olduğu hipotezi belirlenmiştir.

9.2. Anketin Pilot Çalışması

Anket soruları taslak olarak hazırlandıktan sonra, İstatistik ve Bilgisayar Bilimleri Bölümü öğretim üyeleri, Hukuk Fakültesi'nde Bilişim Hukuku alanında çalışan öğretim görevlileri, Ankara Barosu Avukatlık Akademisi'nde Bilişim Hukuku Sertifika eğitimi veren öğretim elemanları ve avukatlar tarafından incelenmiş ve önerileri doğrultusunda yeni eklemeler ya da açıklamalar yapılarak ankete son hali verilmiştir.

9.3. Örneklemin Belirlenmesi ve Analiz Yöntemi

Anket araştırması için bilgisayar bilimleri eğitimi veren Bilgisayar Mühendisliği, İstatistik ve Bilgisayar Bilimleri, Yönetim Bilişim Sistemleri, Bilgisayar ve Öğretim Teknolojileri bölümleri, Hukuk Fakültesi ve kontrol grubu olarak Türk Dili ve Edebiyatı bölümü seçilmiştir. Başkent Üniversitesi Öğrenci İşleri Daire Başkanlığından 2007-2008 yılları arasında, belirlenen fakülte ve bölümlerde kayıtlı öğrenci sayıları alınmış ancak, o dönem içinde izinli olan (kayıt dondurmuş öğrenciler), hazırlıkta ve 1.sınıfta okuyan öğrenciler kapsam dışı bırakılmıştır. İlgili fakülte ve bölümlerdeki akademik personel sayısının fazla olmaması nedeniyle tümüne ulaşılmaya çalışılmıştır. Araştırmada örneklem birimi öğrenci olarak alınmış ve tabakalı örnekleme yöntemi kullanılarak örneklem büyüklüğü belirlenmeye çalışılmıştır.

Bu konuda benzer bir araştırma olmaması nedeniyle, anket sorularından herhangi birine cevap verme oranı 0.5 olarak alınmış ve heterojen bir dağılım gösterdiği varsayımı altında varyans σ^2=0.25 olarak alınmıştır. Anketteki bir sorudan tahmin edilecek bir oran tahmini ile gerçek oran değeri arasındaki farkı ortaya çıkarmada 0.04'lık bir hata hoş görüldüğünde (tolere edildiğinde), %95 güven olasılığı ile yapacağımız parametre tahminleri için toplam örneklem büyüklüğü aşağıdaki gibi hesaplanmıştır ;

Başlangıç örneklem büyüklüğü;

$$n_0 = \frac{z_{\alpha/2}^2 PQ}{d^2} = \frac{(1.96)^2 (0.5)(0.5)}{(0.04)^2} = 600$$

Toplam öğrenci sayısı (N=1322) dikkate alındığında nihai örneklem büyüklüğü aşağıdaki gibi belirlenmiştir;

$$n = \frac{n_0}{1 + \frac{n_0}{N}} = \frac{600}{1 + \frac{600}{1322}} = 415 + \%10 = 450$$

(Öğrencilere ulaşılamama ve ret durumu için %10'luk kayıp bilgi oranı ile örneklem büyüklüğü artırılmıştır)

İlgili fakülte ve bölümlerde 2. 3. ve 4.sınıflarda okuyan ve her sınıfta yaklaşık 25 öğrencinin olduğu görülmüştür. Toplam örneklem büyüklüğüne göre cevaplanması gereken ve gerçekte cevaplayanların dağılımı Çizelge 9.1'de verilmiştir.

.

Çizelge 9.1 Fakülte / Bölümlere Göre Araştırmaya Katılması Gereken ve Anketi Tamamlayan Katılımcı Sayısının Dağılımı

Fakülte / Bölüm	Toplam Katılımcı sayısı	Örnekleme Alınacak Katılımcı Sayısı	Anketi Tamamlayan Katılımcı Sayısı
Fen Edebiyat / İstatistik ve Bilgisayar Bilimleri	125	75	54
Mühendislik / Bilgisayar Mühendisliği	203	75	75
Ticari Bilimler / Yönetim Bilişim Sistemleri	125	75	58
Eğitim / Bilgisayar ve Öğretim Teknolojileri	115	75	82
Hukuk	630	75	52
Fen Edebiyat / Türk Dili ve Edebiyatı	124	75	80
Toplam	1322	450	401

Öğrencilerin %11'inin anketi boş bırakması, geçersiz sayılacak düzeyde doldurması yada anketi doldurmayı kabul etmemesi sonucunda, anketi tamamlayan 401 öğrenci olmuştur Dolayısıyla bu araştırmada anketin cevaplanma oranı %89'dur.

Anket sorularına verilen yanıtların frekans dağılımları oluşturulmuş, değişkenler arasındaki ilişkileri görebilmek için çapraz tablolar oluşturulmuş ve ki-kare testi uygulanmıştır.

9.4. Frekans Dağılımları

Çizelge 9.2 Katılımcıların Üniversitedeki Konumlarına Göre Yaş (yıl) İstatistikleri

Üniversitedeki Konum	Ort. Yaş	Std. Sapma
Öğrenci (n=355)	22,68	1,867
Öğretim Üyesi (n=17)	47,00	15,859
Öğretim Görevlisi (n=16)	36,06	14,007
Araştırma Görevlisi (n=13)	26,15	1,994
Genel	24,36	7,106

Anket çalışmasına katılan Başkent Üniversitesi öğrencilerinin yaş ortalaması 22,6 olarak hesaplanmıştır. Öğretim elemanlarının yaş ortalaması 37,2 genel yaş ortalaması ise 24,3 olarak hesaplanmıştır. Katılımcılarda en küçük yaş 19, en büyük yaş ise 76 olarak belirlenmiştir.

Çizelge 9.3 Katılımcıların Doğum Yerlerine Göre Dağılımı

Coğrafi Bölge	Sayı	%
İç Anadolu	230	57,4
Karadeniz	34	8,5
Akdeniz	28	7
Marmara	26	6,5
Doğu Anadolu	24	6
Ege	20	5
Güneydoğu Anadolu	13	3,2
Yurt dışı	12	3
Belirtilmemiş	14	3,5
Toplam	401	100

Katılımcıların doğum yerleri bilgileri il bazında toplanmış, analiz aşamasında 7 coğrafi bölge ve yurt dışı olmak üzere 8 bölgeye ayrılmıştır. Katılımcıların 14'ü

doğum yerini belirtmemiş olup, 5 katılımcı Almanya, 3 katılımcı Hollanda, birer katılımcı KKTC, Birleşik Arap Emirlikleri, Yunanistan ve Kosova olmak üzere 12 kişi yurtdışı doğumlu olarak belirlenmiştir.

Çizelge 9.4 Katılımcıların İkamet Ettikleri Semtlere Göre Dağılımı

İlçe / Semt	**Sayı**	**%**
Çankaya	83	20,7
Çayyolu	60	16
Emek	50	12,5
Dikmen	30	7,5
Yenimahalle	25	6,2
Etimesgut	22	5,5
Etlik	19	4,7
Keçiören	15	3,7
Küçükesat	15	3,7
Anıttepe	14	3,5
Batıkent	14	3,5
Mamak	9	2,2
Bilkent	8	2
Diğer	8	2
Belirtilmemiş	25	6,2
Toplam	401	100

Katılımcıların Ankara ilinde ikamet ettikleri yerler, semt olarak sorulmuş, sonuçlara göre ilçe, büyük semt veya yoğun olarak tekrarlanan konumlar esas alınarak 14 bölge olarak gruplandırılmıştır. Katılımcıların %6,2 si oturduğu semti belirtmemiş, en yoğun bölgenin %20,7 oranı ile Çankaya bölgesi olduğu belirlenmiştir.

Çizelge 9.5 Katılımcıların Üniversitedeki Bölümlerine Göre Dağılımı

Fakülte / Bölüm	**Sayı**	**%**
Fen Edebiyat / İstatistik ve Bilgisayar Bilimleri	54	13,5
Mühendislik / Bilgisayar Mühendisliği	75	18,7
Ticari Bilimler / Yönetim Bilişim Sistemleri	58	14,5
Eğitim / Bilgisayar ve Öğretim Teknolojileri	82	20,4
Hukuk	52	13,0
Fen Edebiyat / Türk Dili ve Edebiyatı	80	20,0
Toplam	401	100,0

Başkent Üniversitesi'nde çalışmaya uygun olduğu düşünülen 6 fakülte ve bölüm arasından en çok katılımcı %20,4 ile Eğitim Bilimleri Fakültesi Bilgisayar ve Öğretim Teknolojileri Bölümü olurken, en az katılımcı %13 oranıyla Hukuk Fakültesi olarak belirlenmiştir.

Çizelge 9.6 Katılımcıların Üniversitedeki Konumlarına Göre Dağılımı

Katılımcıların Üniversitedeki Konumları	**Sayı**	**%**
Öğrenci	355	88,5
Öğretim Üyesi	17	4,2
Öğretim Görevlisi	16	4,0
Araştırma Görevlisi	13	3,2
Toplam	401	100,0

Katılımcıların üniversite içerisindeki konumları incelendiğinde öğrencilerin %88,5 ve öğretim elemanlarının %11,4 oranında olduğu belirlenmiştir.

Çizelge 9.7 Katılımcıların Cinsiyete Göre Dağılımı

Cinsiyet	**Sayı**	**%**
Kadın	235	58,6
Erkek	166	41,4
Toplam	401	100,0

Yapılan analizlerde katılımcıların %58,6 sının kadın, %41,4 oranındakilerin de erkek olduğu belirlenmiştir.

Çizelge 9.8 Katılımcıların Medeni Durumlarına Göre Dağılımı

Akademisyenlerde Medeni Durum	**Sayı**	**%**
Bekar	20	43,4
Evli	23	50,0
Dul / Ayrılmış	3	6,6
Toplam	46	100,0

Demografik değişkenlerden birisi olarak belirlenen öğretim elemanlarının medeni durum verileri incelendiğinde katılımcıların %50 oranında evli, %43,4 oranında bekar ve %6,6 oranında dul veya ayrılmış oldukları belirlenmiştir.

Çizelge 9.9 Katılımcıların Çocuk Sahibi Olma Durumlarına Göre Dağılımı

Akademisyenlerde Çocuk Sahibi Olma Durumu	**Sayı**	**%**
Var	21	45,6
Yok	5	54,4
Toplam	26	100,0

Öğretim elemanlarının %54,4 'ü çocuksuz, %45,6 'sı da çocuk sahibi olduklarını belirtmiştir.

Çizelge 9.10 Katılımcıların Teknoloji, Bilgisayar ve İnternet'e Olan İlgisine Göre Dağılımı

Teknoloji, Bilgisayar ve İnternet konularına ilgili misiniz? Bu konularla ilgili güncel gelişmeleri takip ediyor musunuz?	**Sayı**	**%**
Konulara ilgi duymuyorum ve gelişmeleri takip etmiyorum.	25	6,2
Konulara ilgi duymuyorum fakat gelişmeleri yazılı ve görsel medyadan takip ediyorum	49	12,2
Konulara ilgi duyuyorum fakat gelişmeleri takip etmiyorum.	99	24,7
Konulara ilgi duyuyorum ve gelişmeleri yakından takip ediyorum.	228	56,9
Toplam	401	100,0

Anket çalışmasının bilgisayar kullanan, bilgisayar ve internet ile ilgili gelişmeleri takip eden kişilere yönelik olması nedeniyle çalışma alanı üniversite öğrencileri ve öğretim elemanları olarak seçilmiştir. Yapılan analizlerde bilgisayar ve internet ile ilgili konulara olan ilgi seviyesi %81,6 oranında belirlenmiştir.

Bu soruda, bilgisayar bilimleri konusunda eğitim veren bölümler gruplandırılarak Çizelge 9.11' deki sonuçlar elde edilmiştir. Kontrol grubu olarak Türk Dili ve Edebiyatı bölümü alınmıştır.

Çizelge 9.11 Katılımcıların Teknoloji, Bilgisayar ve İnternet'e Olan İlgisinin Dağılımı

Bölümler	İlgi YOK Takip YOK	İlgi YOK Takip VAR	İlgi VAR Takip YOK	İlgi VAR Takip VAR	Toplam
Bilgisayar Bilimleri	(12)4,5%	(24)8,9%	(52)19,3%	(181)67,3%	(269)100,0%
Hukuk	(5)9,6%	(12)23,1%	(15)28,8%	(20)38,5%	(52)100,0%
Kontrol Grubu (Türk Dili ve Edebiyatı)	(8)10,0%	(13)16,3%	(32)40,0%	(27)33,8%	(80)100,0%
Toplam	(25)6,2%	(49)12,2%	(99)24,7%	(228)56,9%	(401)100,0%

Analiz sonuçlarına göre bilgisayar bilimleri eğitimi veren veya alan katılımcıların Teknoloji, Bilgisayar ve İnternet ile ilgili konulara ilgi ve gelişmeleri takip düzeyinin %67,13 ile ilk sırada olduğu. Kontrol grubundaki katılımcılarda en yüksek oranın %40 ile İlgisi olan ancak gelişmeleri takip etmeyen katılımcılar olduğu belirlenmiştir.

Çizelge 9.12 Katılımcıların İnternet Kullanım Sürelerine Göre Dağılımı.

Ne kadar süredir İnternet kullanıyorsunuz ?	Sayı	%
İnternet kullanmıyorum.	5	1,2
1 yıldan az süredir kullanıyorum.	7	1,7
2 – 5 yıldır İnternet kullanıcısıyım.	93	23,2
6 – 9 yıldır İnternet kullanıcısıyım.	185	46,1
10 yıldan uzun süredir İnternet kullanıyorum.	111	27,7
Toplam	401	100,0

İnternet kullanım süreleri incelendiğinde en çok katılımcının %46,1 oranı ile 6-9 yıldır İnternet kullandığı belirlenmiştir.

Çizelge 9.13 Katılımcıların İnternete Bağlandıkları Ortama Göre Dağılımı

	Evet		Hayır	
İnternet'e hangi ortamlardan bağlanıyorsunuz?	Sayı	%	Sayı	%
İnternet'e evden bağlananlar	374	93,3	27	6,7
İnternet'e işyeri veya okuldan bağlananlar	272	67,8	129	32,2
İnternet'e İnternet kafelerden bağlananlar	75	18,7	326	81,3
İnternet'e ortak kullanım alanlarından bağlananlar	128	31,9	273	68,1

İnternet'e bağlanma ortamı sonuçları incelendiğinde katılımcıların %93,3 ü evden bağlandığını belirtmiştir. İnternet kafelerden bağlananlar ise %18,7 oranındadır.

Çizelge 9.14 Katılımcıların İnternet'i Kullanım Amaçlarına Göre Dağılımı

	Evet		Hayır	
İnternet'i hangi amaçlar için kullanıyorsunuz?	**Sayı**	**%**	**Sayı**	**%**
İş / ders ile ilgili konularda araştırma yapmak	375	93,5	26	6,5
İlgi duyulan kişisel konularda araştırma yapmak	363	90,5	38	9,5
Haber ve güncel gelişmeleri takip etmek	328	81,8	73	18,2
İletişim amaçlı kullanım	346	86,3	55	13,7
Sosyal çevre edinme amaçlı kullanım	100	24,9	301	75,1
Oyun ve eğlence amaçlı kullanım	231	57,6	170	42,4

Katılımcıların İnternet'i kullanım amaçları incelendiğinde en büyük oran %93,5 ile iş/ders konularında araştırma yapmak olarak belirlenmiş; en düşük oran ise %24,9 ile sosyal çevre edinme amaçlı kullanım olarak belirlenmiştir.

Çizelge 9.15 Katılımcıların İnternet'i Kullanım Sıklıklarına Göre Dağılımı

İnternet'i ortalama olarak kullanım sıklığınız nedir ?	**Sayı**	**%**
İş / Okul saatleri dışında kullanmıyorum.	10	2,5
Haftada 1 günden daha seyrek olarak kullanıyorum.	4	1,0
Haftada bir gün kullanıyorum	6	1,5
Haftada birkaç gün kullanıyorum	38	9,5
Hemen hemen her gün kullanıyorum.	343	85,5
Toplam	401	100,0

İnternet'i ortalama kullanım sıklığı açısından hemen her gün kullanan katılımcılar %85,5 ile en büyük orana sahip grubu oluşturmaktadır.

9.5. Katılımcıların Bilişim Suçu Algıları

Anketimizde farklı ülkelerin hukuk sistemlerine göre bilişim suçu sayılan fiillerin kişisel algı düzeyinde suç şiddeti açısından değerlendirilmesi amacıyla sorulan soruda 14 adet madde bulunmaktadır. Söz konusu sorular sık rastlanan bilişim suçu türlerine göre aşağıdaki biçimde gruplanmıştır ;

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

Yapılan analizler sonucunda sorulara verilen yanıtların dağılımı Çizelge 9.16 da yer almaktadır.

Çizelge 9.16 Katılımcıların Bilişim Suçu Algılarına Göre Dağılımı

Soru 6	En Hafif		Hafif		Orta		Ağır		En ağır	
Madde	Sayı	%	Sayı	%	Sayı	%	Sayı	%	Sayı	%
1	28	**7,0**	23	**5,7**	84	**20,9**	90	**22,4**	176	**43,9**
2	102	**25,4**	57	**14,2**	95	**23,7**	74	**18,5**	73	**18,2**
3	3	**0,7**	1	**0,2**	12	**3,0**	36	**9,0**	349	**87,0**
4	3	**0,7**	4	**1,0**	22	**5,5**	62	**15,5**	310	**77,3**
5	4	**1,0**	8	**2,0**	26	**6,5**	72	**18,0**	291	**72,6**
6	4	**1,0**	12	**3,0**	43	**10,7**	100	**24,9**	242	**60,3**
7	22	**5,5**	34	**8,5**	103	**25,7**	118	**29,4**	124	**30,9**
8	55	**13,7**	70	**17,5**	106	**26,4**	84	**20,9**	86	**21,4**
9	11	**2,7**	19	**4,7**	87	**21,7**	132	**32,9**	152	**37,9**
10	2	**0,5**	5	**1,2**	10	**2,5**	24	**6,0**	360	**89,8**
11	4	**1,0**	2	**0,5**	18	**4,5**	31	**7,7**	346	**86,3**
12	4	**1,0**	12	**3,0**	29	**7,2**	49	**12,2**	307	**76,6**
13	4	**1,0**	24	**6,0**	76	**19,0**	150	**37,4**	147	**36,7**
14	56	**14,0**	70	**17,5**	102	**25,4**	93	**23,2**	80	**20,0**

Ülkemizde yürürlükte bulunan Türk Ceza Kanunu çerçevesinde en ağır suç 6. sorunun 10 numaralı maddesinde (Bkz. Ek1) yer alan Çocuk pornografisi konulu fotoğraf ve video içeriği bulunan İnternet sitesi yayınlarının yapılması fiilidir. Soruya yanıt veren katılımcıların %89,8 'i söz konusu fiili en ağır suç olarak işaretlemiştir. Son yıllarda basın ve yayın organları tarafından çocuk pornografisi suçunun gündemde tutulması ve söz konusu suçun uluslararası anlaşmalar çerçevesinde kovuşturmaya tabi tutulan bir nitelikte olmasının bu suçun belirgin olarak diğer suçlardan ayrışmasının temel nedenleri olduğu düşünülmektedir.

Benzer şekilde basın ve yayın organlarında sıklıkla karşılaşılan bir diğer suç biçimi internet üzerinden banka hesap bilgilerine ulaşılması yoluyla hırsızlık suçudur. Katılımcılar 6. sorunun 3 numaralı maddesinde (Bkz. Ek1) bahsi geçen suçu %87

ile en ağır ikinci 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 ağır bir suç olarak belirlemişlerdir.

Katılımcıların En Hafif suç olarak belirlediği 6. sorunun 2 numaralı maddesi (Bkz. Ek1) “Bir ülke veya devlet aleyhinde yayın yapan bir web sitesinin, bir kişi ya da grup tarafından kapatılması, erişiminin engellenmesi” suçu, genel düşüncenin aksine siber İhlal türünde bir suçtur. Diğer ülkelerin hukuk sistemlerinde de ceza olarak değerlendirilen bu fiil Türk Ceza Kanunu’nun 243. ve 244. maddeleri tarafından çerçevesi çizilen, bir bilişim sistemine yetkisiz olarak girme, bilişim sistemindeki verileri bozma ve bilişim sistemine genel erişimi engelleme suçuna örnektir.

Katılımcıların %14 oranı ile En Hafif ikinci suç olarak belirledikleri 6. sorunun 14. maddesi (Bkz. Ek1) Bir bilişim sistemindeki verilere yetkisiz olarak erişip herhangi bir zarar vermeden sistemden çıkılması fiili de siber ihlal kapsamında bir suçu tanımlamaktadır. Bütün ülkelerin hukuk sistemlerinde ve ceza kanunlarında genellikle ilk düzenlenen bilişim suçu olma özelliğine sahiptir.

Dikkati çeken bir başka sonuç, akademik aşırmacılık (plagiarism) fiilinin sorulduğu 6. soru 8. madde (Bkz. Ek1) ye verilen yanıtlardır. Söz konusu soruya verilen yanıtlarda katılımcıların %13,7 si akademik aşırmacılık fiilinin En Hafif suç olarak belirlemişlerdir. Aşırmacılık fiili En Hafif suçlar arasında üçüncü sırada yer almaktadır.

Çizelge 9.17 Katılımcıların Ahlaki Değer ve Bilişim Suçu Algılarına Göre Dağılımı (Ek1 Soru 7 Madde 1-24)

	Yanlış		Doğru		Fikrim Yok		Suç Değil		Suç		Fikrim Yok	
	Sayı	%	Sayı	%	Sayı	%	Sayı	%	Sayı	%	Sayı	%
1	300	**74,8**	68	**17,0**	33	**8,2**	131	**32,7**	180	**44,9**	90	**22,4**
2	322	**80,3**	38	**9,5**	41	**10,2**	224	**55,9**	85	**21,2**	92	**22,9**
3	42	**10,5**	329	**82,0**	30	**7,5**	311	**77,6**	26	**6,5**	64	**16,0**
4	245	**61,1**	54	**13,5**	102	**25,4**	210	**52,4**	72	**18,0**	119	**29,7**
5	200	**49,9**	85	**21,2**	116	**28,9**	202	**50,4**	67	**16,7**	132	**32,9**
6	64	**16,0**	213	**53,1**	124	**30,9**	268	**66,8**	23	**5,7**	110	**27,4**
7	356	**88,8**	7	**1,7**	38	**9,5**	168	**41,9**	116	**28,9**	117	**29,2**
8	243	**60,6**	78	**19,5**	80	**20,0**	86	**21,4**	246	**61,3**	69	**17,2**
9	243	**60,6**	95	**23,7**	63	**15,7**	92	**22,9**	245	**61,1**	64	**16,0**
10	141	**35,2**	168	**41,9**	92	**22,9**	158	**39,4**	146	**36,4**	97	**24,2**
11	242	**60,3**	84	**20,9**	75	**18,7**	99	**24,7**	188	**46,9**	114	**28,4**
12	300	**74,8**	22	**5,5**	79	**19,7**	65	**16,2**	206	**51,4**	130	**32,4**
13	241	**60,1**	61	**15,2**	99	**24,7**	103	**25,7**	156	**38,9**	142	**35,4**
14	138	**34,4**	138	**34,4**	125	**31,2**	162	**40,4**	92	**22,9**	147	**36,7**
15	92	**22,9**	215	**53,6**	94	**23,4**	223	**55,6**	60	**15,0**	118	**29,4**
16	240	**59,9**	60	**15,0**	101	**25,2**	115	**28,7**	137	**34,2**	149	**37,2**
17	350	**87,3**	11	**2,7**	40	**10,0**	77	**19,2**	247	**61,6**	77	**19,2**
18	363	**90,5**	9	**2,2**	29	**7,2**	76	**19,0**	258	**64,3**	67	**16,7**
19	365	**91,0**	5	**1,2**	31	**7,7**	53	**13,2**	297	**74,1**	51	**12,7**
20	256	**63,8**	73	**18,2**	72	**18,0**	77	**19,2**	238	**59,4**	86	**21,4**
21	334	**83,3**	27	**6,7**	40	**10,0**	51	**12,7**	282	**70,3**	68	**17,0**
22	320	**79,8**	21	**5,2**	60	**15,0**	131	**32,7**	160	**39,9**	110	**27,4**
23	238	**59,4**	47	**11,7**	116	**28,9**	126	**31,4**	113	**28,2**	162	**40,4**
24	117	**29,2**	141	**35,2**	143	**35,7**	160	**39,9**	86	**21,4**	155	**38,7**

Katılımcıların ahlaki açıdan yanlış bulup, suç olmadığını düşündükleri fiillerden en belirgini yanlış %88,8 ve suç değil %41,9 oranlarıyla çevrimiçi forum ve ansiklopedi sitelerine kasıtlı olarak hatalı bilgi eklenmesi (Bkz Ek1. Soru 7 Madde 6) fiili olarak tanımlanan siber vandalizm suçudur. Ülkemiz hukuk sisteminde bilişim sistemlerine yönelik vandalizm fiilleri suç kapsamında değildir. Sorulara verilen yanıtlar, İnternet'in bilgiye ulaşma amaçlı kullanımının yaygın olduğunu ve bu konudaki haksız fiillere karşı katılımcıların duyarlı olduklarını göstermektedir.

Ahlaki açıdan yanlış fakat suç olmadığı düşünülen fiiller arasında dikkati çeken bir diğer davranış ise yanlış %80,3 ve suç değil %55,9 oranlarıyla eş, çocuk veya arkadaşların e-postalarını okuma fiili (Bkz. Ek1 Soru 7 Madde 2) olarak tespit edilmiştir. Soruya verilen yanıtlar katılımcıların kişisel verilerin korunması konusundaki duyarlılıklarını göstermektedir.

Katılımcıların ahlaki açıdan doğru bulup, suç olduğunu düşündükleri davranışlar arasında en belirgini, doğru %41,9 ve suç %36,4 oranlarıyla eski tarihli film veya müzik eserlerini paylaşım yazılımlarıyla temin etme (Bkz. Ek1 Soru 7 Madde 10) davranışıdır. Katılımcıların algılarının aksine eski tarihli eserlerin fikir ve sanat eserleri yasası kapsamında bulunma durumu nadirdir ve suç algısının basında sıkça yer alan korsan eserlerle mücadele konulu ilan reklam ve haberlerden kaynaklanmış olabileceği düşünülmektedir.

Katılımcıların ahlaki açıdan yanlış ve suç olduğunu düşündükleri fiillerden en belirgini ise, yanlış %91 ve suç %74,1 oranlarıyla kişisel bilgilerin üçüncü kişilere sunulması (Bkz. Ek1. Soru 7 Madde 19) davranışıdır. Katılımcılar, kişisel verilerin korunması konusundaki duyarlılıklarını bu soruda da belirtmişlerdir.

Bilişim suçu olan ve olmayan fiillerin karışık halde bulunduğu Çizelge 9.17 de (Bkz. Ek1 Soru 7) katılımcıların hukuksal açıdan fikrim yok seçeneğini işaretledikleri sorular yüzde oranlarına göre büyükten küçüğe sıralandığında; suç unsuru konusunda katılımcıların bilgisiz olduğu veya yanlış bilgiye sahip olduğu fiiller aşağıda belirtilmiştir.

- E-posta hesabına gelen, şahıs ve firmalara yönelik eleştiri, hakaret içerikli e-postaları başkalarına iletmek (Bkz. Ek1 Soru 7 Madde 23)

Bu fiil suç unsuru taşımasına rağmen katılımcıların %31,4'ü suç değil, %40,4'ü ise fikrim yok seçeneğini işaretlemişlerdir. Suç olduğunu belirten katılımcıların oranı %28,2 dir.

- Bir menkul kıymet hakkında internet yolu ile manipulasyon yapma fiili (Bkz. Ek1 Soru 7 Madde 24)

Fiil suç unsuru taşımasına rağmen katılımcıların %39,9'u suç değil, %38,7'si fikrim yok, %21,4'ü suç olarak belirlemiştir.

- Bir web sitesine genel erişimi engelleyici teknikler kullanmak (Bkz. Soru 7 Madde 16)

Fiil TCK Madde 244 de açık bir şekilde suç olarak tanımlanmış olmasına rağmen katılımcıların %28,7'si suç değil, %37,2'si fikrim yok seçeneğini işaretlemişlerdir.

- Açık kaynak kodlu yazılımları ticari kar sağlamak amacıyla kullanmak (Bkz. Ek1 Soru 7 Madde 13)

Fiilde hiçbir suç unsuru bulunmamasına rağmen katılımcıların %38,9'u tarafından suç, %35,4'ü tarafından fikrim yok olarak belirlenmiştir. Suç olmadığını bilen katılımcı sayısı %25,7 olarak hesaplanmıştır.

Çizelge 9.18 Bilgisayar Bilimleri ve Hukuk Eğitimi Açısından Bilişim Suçu Algıları *

	Bir ülke veya devlet aleyhinde web sitesi yayını yapılması					
Eğitim Grupları	**En Hafif**	**Hafif**	**Orta**	**Ağır**	**En Ağır**	**Toplam**
Bilgisayar Bilimleri	16	12	67	60	114	269
	5,9%	4,5%	24,9%	22,3%	42,4%	100,0%
Hukuk	6	7	6	12	21	52
	11,5%	13,5%	11,5%	23,1%	40,4%	100,0%
Kontrol Grubu	6	4	11	18	41	80
(Türk Dili ve Edebiyatı)	7,5%	5,0%	13,8%	22,5%	51,3%	100,0%
	28	23	84	90	176	401
Toplam	7,0%	5,7%	20,9%	22,4%	43,9%	100,0%
χ^2 = 15,7 p =0,47						
	Bir ülke veya devlet aleyhinde yayın yapan bir web sitesinin, bir kişi ya da grup tarafından kapatılması, erişiminin engellenmesi					
Eğitim Grupları	**En Hafif**	**Hafif**	**Orta**	**Ağır**	**En Ağır**	**Toplam**
Bilgisayar Bilimleri	56	44	68	50	51	269
	20,8%	16,4%	25,3%	18,6%	19,0%	100,0%
Hukuk	19	4	10	12	7	52
	36,5%	7,7%	19,2%	23,1%	13,5%	100,0%
Kontrol Grubu	27	9	17	12	15	80
(Türk Dili ve Edebiyatı)	33,8%	11,3%	21,3%	15,0%	18,8%	100,0%
	102	57	95	74	73	401
Toplam	25,4%	14,2%	23,7%	18,5%	18,2%	100,0%
χ^2 = 12,6 p =0,12						
	Bir banka müşterilerinin hesap bilgileri elde edilerek yetkisiz para transferi yapılması					
Eğitim Grupları	**En Hafif**	**Hafif**	**Orta**	**Ağır**	**En Ağır**	**Toplam**
Bilgisayar Bilimleri	3	0	11	22	233	269
	1,1%	0,0%	4,1%	8,2%	86,6%	100,0%
Hukuk	0	0	0	9	43	52
	0,0%	0,0%	0,0%	17,3%	82,7%	100,0%
Kontrol Grubu	0	1	1	5	73	80
(Türk Dibi ve Edebiyatı)	0,0%	1,3%	1,3%	6,3%	91,3%	100,0%
	3	1	12	36	349	401
Toplam	0,7%	0,2%	3,0%	9,0%	87,0%	100,0%
	Sahte Loto, şirket ortaklığı gibi tuzaklarla dolandırıcılık yapılması					
Eğitim Grupları	**En Hafif**	**Hafif**	**Orta**	**Ağır**	**En Ağır**	**Toplam**
Bilgisayar Bilimleri	3	4	15	42	205	269
	1,1%	1,5%	5,6%	15,6%	76,2%	100,0%
Hukuk	0	0	3	15	34	52
	0,0%	0,0%	5,8%	28,8%	65,4%	100,0%
Kontrol Grubu	0	0	4	5	71	80
(Türk Dili ve Edebiyatı)	0,0%	0,0%	5,0%	6,3%	88,8%	100,0%
	3	4	22	62	310	401
Toplam	0,7%	1,0%	5,5%	15,5%	77,3%	100,0%

Çizelge 9.18 Bilgisayar Bilimleri ve Hukuk Eğitimi Açısından Bilişim Suçu Algıları (devam ediyor)

Eğitim Grupları	Kimlik numarası, telefon numarası ve adres gibi kişisel bilgilerin web siteleri aracılığıyla toplanıp üçüncü şahıslara sunulması veya satılması					
	En Hafif	**Hafif**	**Orta**	**Ağır**	**En Ağır**	**Toplam**
Bilgisayar Bilimleri	3	6	23	60	177	269
	1,1%	2,2%	8,6%	22,3%	65,8%	100,0%
Hukuk	0	1	2	7	42	52
	0,0%	1,9%	3,8%	13,5%	80,8%	100,0%
Kontrol Grubu	1	1	1	5	72	80
(Türk Dili ve Edebiyatı)	1,3%	1,3%	1,3%	6,3%	90,0%	100,0%
	4	8	26	72	291	401
Toplam	1,0%	2,0%	6,5%	18,0%	72,6%	100,0%

Eğitim Grupları	Bir kişisel bilgisayara uzaktan müdahale ederek kişisel dosya, belge ve dökümanların elde edilmesi					
	En Hafif	**Hafif**	**Orta**	**Ağır**	**En Ağır**	**Toplam**
Bilgisayar Bilimleri	4	10	35	71	149	269
	1,5%	3,7%	13,0%	26,4%	55,4%	100,0%
Hukuk	0	1	2	17	32	52
	0,0%	1,9%	3,8%	32,7%	61,5%	100,0%
Kontrol Grubu	0	1	6	12	61	80
(Türk Dili ve Edebiyatı)	0,0%	1,3%	7,5%	15,0%	76,3%	100,0%
	4	12	43	100	242	401
Toplam	1,0%	3,0%	10,7%	24,9%	60,3%	100,0%

Eğitim Grupları	Bilgisayar donanımlarına fiziksel zarar verilmesi					
	En Hafif	**Hafif**	**Orta**	**Ağır**	**En Ağır**	**Toplam**
Bilgisayar Bilimleri	16	23	70	77	83	269
	5,9%	8,6%	26,0%	28,6%	30,9%	100,0%
Hukuk	5	6	18	14	9	52
	9,6%	11,5%	34,6%	26,9%	17,3%	100,0%
Kontrol Grubu	1	5	15	27	32	80
(Türk Dili ve Edebiyatı)	1,3%	6,3%	18,8%	33,8%	40,0%	100,0%
	22	34	103	118	124	401
Toplam	5,5%	8,5%	25,7%	29,4%	30,9%	100,0%
$\chi^2 = 14,4$ p =0,07						

Eğitim Grupları	İnternet'de bulunan bir makale ya da raporun referans gösterilmeden kullanılması					
	En Hafif	**Hafif**	**Orta**	**Ağır**	**En Ağır**	**Toplam**
Bilgisayar Bilimleri	46	56	80	47	40	269
	17,1%	20,8%	29,7%	17,5%	14,9%	100,0%
Hukuk	5	5	10	17	15	52
	9,6%	9,6%	19,2%	32,7%	28,8%	100,0%
Kontrol Grubu	4	9	16	20	31	80
(Türk Dili ve Edebiyatı)	5,0%	11,3%	20,0%	25,0%	38,8%	100,0%
	55	70	106	84	86	401
Toplam	13,7%	17,5%	26,4%	20,9%	21,4%	100,0%
$\chi^2 = 39,5$ p =0,00						

Çizelge 9.18 Bilgisayar Bilimleri ve Hukuk Eğitimi Açısından Bilişim Suçu Algıları (devam ediyor)

Eğitim Grupları	Bilgisayar yazılımlarında değişiklik yaparak yazılım üzerinde hak iddia edilmesi					
	En Hafif	**Hafif**	**Orta**	**Ağır**	**En Ağır**	**Toplam**
Bilgisayar Bilimleri	8	15	61	101	84	269
	3,0%	5,6%	22,7%	37,5%	31,2%	100,0%
Hukuk	1	3	13	15	20	52
	1,9%	5,8%	25,0%	28,8%	38,5%	100,0%
Kontrol Grubu	2	1	13	16	48	80
(Türk Dili ve Edebiyatı)	2,5%	1,3%	16,3%	20,0%	60,0%	100,0%
	11	19	87	132	152	401
Toplam	2,7%	4,7%	21,7%	32,9%	37,9%	100,0%
$\chi^2 = 23,7$ p =0,002						

Eğitim Grupları	Çocuk pornografisi konulu fotoğraf ve video içeriği bulunan İnternet sitesi yayınlarının yapılması					
	En Hafif	**Hafif**	**Orta**	**Ağır**	**En Ağır**	**Toplam**
Bilgisayar Bilimleri	2	4	7	20	236	269
	0,7%	1,5%	2,6%	7,4%	87,7%	100,0%
Hukuk	0	0	2	2	48	52
	0,0%	0,0%	3,8%	3,8%	92,3%	100,0%
Kontrol Grubu	0	1	1	2	76	80
(Türk Dili ve Edebiyatı)	0,0%	1,3%	1,3%	2,5%	95,0%	100,0%
	2	5	10	24	360	401
Toplam	0,5%	1,2%	2,5%	6,0%	89,8%	100,0%

Eğitim Grupları	Çocuk pornografisini temsil eden çizim ve animasyonlara yönelik içeriği bulunan İnternet sitesi yayınlarının yapılması					
	En Hafif	**Hafif**	**Orta**	**Ağır**	**En Ağır**	**Toplam**
Bilgisayar Bilimleri	4	1	14	27	223	269
	1,5%	0,4%	5,2%	10,0%	82,9%	100,0%
Hukuk	0	0	3	3	46	52
	0,0%	0,0%	5,8%	5,8%	88,5%	100,0%
Kontrol Grubu	0	1	1	1	77	80
(Türk Dili ve Edebiyatı)	0,0%	1,3%	1,3%	1,3%	96,3%	100,0%
	4	2	18	31	346	401
Toplam	1,0%	0,5%	4,5%	7,7%	86,3%	100,0%

Eğitim Grupları	Çocuk pornografisi konulu içeriği bulunan İnternet sitesi yayınlarına erişilmesi					
	En Hafif	**Hafif**	**Orta**	**Ağır**	**En Ağır**	**Toplam**
Bilgisayar Bilimleri	4	7	22	39	197	269
	1,5%	2,6%	8,2%	14,5%	73,2%	100,0%
Hukuk	0	3	6	6	37	52
	0,0%	5,8%	11,5%	11,5%	71,2%	100,0%
Kontrol Grubu	0	2	1	4	73	80
(Türk Dili ve Edebiyatı)	0,0%	2,5%	1,3%	5,0%	91,3%	100,0%
	4	12	29	49	307	401
Toplam	1,0%	3,0%	7,2%	12,2%	76,6%	100,0%

Çizelge 9.18 Bilgisayar Bilimleri ve Hukuk Eğitimi Açısından Bilişim Suçu Algıları (devam ediyor)

Eğitim Grupları	Bilgisayar sistemine zarar veren kodlar yazılması ve yayılması					
	En Hafif	**Hafif**	**Orta**	**Ağır**	**En Ağır**	**Toplam**
Bilgisayar Bilimleri	4	19	55	105	86	269
	1,5%	7,1%	20,4%	39,0%	32,0%	100,0%
Hukuk	0	4	10	22	16	52
	0,0%	7,7%	19,2%	42,3%	30,8%	100,0%
Kontrol Grubu	0	1	11	23	45	80
(Türk Dili ve Edebiyatı)	0,0%	1,3%	13,8%	28,8%	56,3%	100,0%
	4	24	76	150	147	401
Toplam	1,0%	6,0%	19,0%	37,4%	36,7%	100,0%

Eğitim Grupları	Bir bilişim sistemindeki verilere yetkisiz olarak erişip herhangi bir zarar vermeden sistemden çıkılması					
	En Hafif	**Hafif**	**Orta**	**Ağır**	**En Ağır**	**Toplam**
Bilgisayar Bilimleri	44	51	70	61	43	269
	16,4%	19,0%	26,0%	22,7%	16,0%	100,0%
Hukuk	6	12	13	13	8	52
	11,5%	23,1%	25,0%	25,0%	15,4%	100,0%
Kontrol Grubu	6	7	19	19	29	80
(Türk Dili ve Edebiyatı)	7,5%	8,8%	23,8%	23,8%	36,3%	100,0%
	56	70	102	93	80	401
Toplam	14,0%	17,5%	25,4%	23,2%	20,0%	100,0%
$\chi^2 = 22,0$ p =0,005						

* Bazı çapraz tablolarda 5 den küçük beklenen değer sayısının %30 ve üzerinde olması nedeniyle ki-kare testi uygulanamamıştır.

Bilgisayar bilimleri ve hukuk eğitimi açısından yapılan anket analizlerinde, gruplar arasındaki en belirgin farklılık, χ^2 = 39,5 p =0,00 değerleriyle, akademik aşırmacılık (plagiarism) davranışını ölçen soruda (Bkz. Ek1. Soru 6 Madde 8) hesaplanmıştır. Sonuçlara göre hukuk eğitimi grubu plagiarism fiilini %32,7 oranı ile ağır, %28,8 oranı ile en ağır suç olarak belirlerken; Bilgisayar bilimleri eğitimi grubunda söz konusu davranış, %17,5 oranında ağır ve %14,9 oranında en ağır suç olarak belirlenmiştir. Kontrol grubunda bu değerler 25,0% oranında ağır ve 38,8% oranında en ağır olarak hesaplanmıştır. Eğitim grupları arasındaki homojenliği sağlamayan grubun (χ^2 = 23,61) çalışmanın kontrol grubu olarak belirlenen Türk Dili ve Edebiyatı bölümü olduğu tespit edilmiştir.

Eğitim grupları arasında bir diğer önemli farklılık, bilgisayar donanımlarına fiziksel zarar verilmesi davranışında görülmektedir (Bkz Ek1. Soru 6 Madde 7). Bilgisayar grubundaki katılımcılar söz konusu davranışı %30,9 oranı ile en ağır suç olarak

belirlerken; hukuk grubundaki katılımcılar %34,6 oranı ile orta dereceli suç olarak belirlemiştir.

Bilgisayar yazılımlarında değişiklik yaparak yazılım üzerinde hak iddia edilmesi davranışını (Bkz Ek1. Soru 6 Madde 9) ölçen soruda ise gruplar arasındaki homojenliği sağlamayan grup, (χ^2 = 17,5) çalışmanın kontrol grubu olarak belirlenen Türk Dili ve Edebiyatı bölümü olduğu tespit edilmiştir. Benzer şekilde bir bilişim sistemindeki verilere yetkisiz olarak erişip herhangi bir zarar vermeden sistemden çıkılması (Bkz Ek1. Soru 6 Madde 14) davranışını ölçen soruda da gruplar arasındaki homojenliği sağlamayan grup, (χ^2 = 16,6) kontrol grubu olan Türk Dili ve Edebiyatı bölümüdür.

Çizelge 9.19 Akademik Konumlara Göre Bilişim Suçu Algıları *

	Bir ülke veya devlet aleyhinde web sitesi yayını yapılması					
Akademik Konum	**En Hafif**	**Hafif**	**Orta**	**Ağır**	**En Ağır**	**Toplam**
Öğrenci	22	21	75	83	154	355
	6,2%	5,9%	21,1%	23,4%	43,4%	100,0%
Öğretim Elemanı	6	2	9	7	22	46
	13,0%	4,3%	19,6%	15,2%	47,8%	100,0%
Toplam	28	23	84	90	176	401
	7,0%	5,7%	20,9%	22,4%	43,9%	100,0%

$\chi^2 = 4,34$ p =0,36

	Bir ülke veya devlet aleyhinde yayın yapan bir web sitesinin, bir kişi ya da grup tarafından kapatılması, erişiminin engellenmesi					
Akademik Konum	**En Hafif**	**Hafif**	**Orta**	**Ağır**	**En Ağır**	**Toplam**
Öğrenci	92	55	83	63	62	355
	25,9%	15,5%	23,4%	17,7%	17,5%	100,0%
Öğretim Elemanı	10	2	12	11	11	46
	21,7%	4,3%	26,1%	23,9%	23,9%	100,0%
Toplam	102	57	95	74	73	401
	25,4%	14,2%	23,7%	18,5%	18,2%	100,0%

$\chi^2 = 5,73$ p =0,22

	Bir banka müşterilerinin hesap bilgileri elde edilerek yetkisiz para transferi yapılması					
Akademik Konum	**En Hafif**	**Hafif**	**Orta**	**Ağır**	**En Ağır**	**Toplam**
Öğrenci	2	1	12	32	308	355
	0,6%	0,3%	3,4%	9,0%	86,8%	100,0%
Öğretim Elemanı	1	0	0	4	41	46
	2,2%	0,0%	0,0%	8,7%	89,1%	100,0%
Toplam	3	1	12	36	349	401
	0,7%	0,2%	3,0%	9,0%	87,0%	100,0%

	Sahte Loto, şirket ortaklığı gibi tuzaklarla dolandırıcılık yapılması					
Akademik Konum	**En Hafif**	**Hafif**	**Orta**	**Ağır**	**En Ağır**	**Toplam**
Öğrenci	2	3	22	56	272	355
	0,6%	0,8%	6,2%	15,8%	76,6%	100,0%
Öğretim Elemanı	1	1	0	6	38	46
	2,2%	2,2%	0,0%	13,0%	82,6%	100,0%
Toplam	3	4	22	62	310	401
	0,7%	1,0%	5,5%	15,5%	77,3%	100,0%

Çizelge 9.19 Akademik Konumlara Göre Bilişim Suçu Algıları (devam ediyor)

	Kimlik numarası, telefon numarası ve adres gibi kişisel bilgilerin web siteleri aracılığıyla toplanıp üçüncü şahıslara sunulması veya satılması					
Akademik Konum	**En Hafif**	**Hafif**	**Orta**	**Ağır**	**En Ağır**	**Toplam**
Öğrenci	3	8	24	59	261	355
	0,8%	2,3%	6,8%	16,6%	73,5%	100,0%
Öğretim Elemanı	1	0	2	13	30	46
	2,2%	0,0%	4,3%	28,3%	65,2%	100,0%
Toplam	4	8	26	72	291	401
	1,0%	2,0%	6,5%	18,0%	72,6%	100,0%

	Bir kişisel bilgisayara uzaktan müdahale ederek kişisel dosya, belge ve dökümanların elde edilmesi					
Akademik Konum	**En Hafif**	**Hafif**	**Orta**	**Ağır**	**En Ağır**	**Toplam**
Öğrenci	3	12	41	92	207	355
	0,8%	3,4%	11,5%	25,9%	58,3%	100,0%
Öğretim Elemanı	1	0	2	8	35	46
	2,2%	0,0%	4,3%	17,4%	76,1%	100,0%
Toplam	4	12	43	100	242	401
	1,0%	3,0%	10,7%	24,9%	60,3%	100,0%

	Bilgisayar donanımlarına fiziksel zarar verilmesi					
Akademik Konum	**En Hafif**	**Hafif**	**Orta**	**Ağır**	**En Ağır**	**Toplam**
Öğrenci	19	29	95	105	107	355
	5,4%	8,2%	26,8%	29,6%	30,1%	100,0%
Öğretim Elemanı	3	5	8	13	17	46
	6,5%	10,9%	17,4%	28,3%	37,0%	100,0%
Toplam	22	34	103	118	124	401
	5,5%	8,5%	25,7%	29,4%	30,9%	100,0%

$\chi^2 = 2,47$ p =0,64

	İnternet'de bulunan bir makale ya da raporun referans gösterilmeden kullanılması					
Akademik Konum	**En Hafif**	**Hafif**	**Orta**	**Ağır**	**En Ağır**	**Toplam**
Öğrenci	54	66	97	73	65	355
	15,2%	18,6%	27,3%	20,6%	18,3%	100,0%
Öğretim Elemanı	1	4	9	11	21	46
	2,2%	8,7%	19,6%	23,9%	45,7%	100,0%
Toplam	55	70	106	84	86	401
	13,7%	17,5%	26,4%	20,9%	21,4%	100,0%

$\chi^2 = 22,6$ p =0,00

	Başkası tarafından hazırlanan bilgisayar yazılımlarında değişiklik yaparak yazılım üzerinde hak iddia edilmesi					
Akademik Konum	**En Hafif**	**Hafif**	**Orta**	**Ağır**	**En Ağır**	**Toplam**
Öğrenci	10	19	81	118	127	355
	2,8%	5,4%	22,8%	33,2%	35,8%	100,0%
Öğretim Elemanı	1	0	6	14	25	46
	2,2%	0,0%	13,0%	30,4%	54,3%	100,0%
Toplam	11	19	87	132	152	401
	2,7%	4,7%	21,7%	32,9%	37,9%	100,0%

$\chi^2 = 8,12$ p =0,08

Çizelge 9.19 Akademik Konumlara Göre Bilişim Suçu Algıları (devam ediyor)

Akademik Konum	Çocuk pornografisi konulu fotoğraf ve video içeriği bulunan İnternet sitesi yayınlarının yapılması					
	En Hafif	Hafif	Orta	Ağır	En Ağır	Toplam
Öğrenci	1	5	10	19	320	355
	0,3%	1,4%	2,8%	5,4%	90,1%	100,0%
Öğretim Elemanı	1	0	0	5	40	46
	2,2%	0,0%	0,0%	10,9%	87,0%	100,0%
Toplam	2	5	10	24	360	401
	0,5%	1,2%	2,5%	6,0%	89,8%	100,0%

Akademik Konum	Çocuk pornografisini temsil eden çizim ve animasyonlara yönelik içeriği bulunan İnternet sitesi yayınlarının yapılması					
	En Hafif	Hafif	Orta	Ağır	En Ağır	Toplam
Öğrenci	3	2	13	26	311	355
	0,8%	0,6%	3,7%	7,3%	87,6%	100,0%
Öğretim Elemanı	1	0	5	5	35	46
	2,2%	0,0%	10,9%	10,9%	76,1%	100,0%
Toplam	4	2	18	31	346	401
	1,0%	0,5%	4,5%	7,7%	86,3%	100,0%

Akademik Konum	Çocuk pornografisi konulu içeriği bulunan İnternet sitesi yayınlarına erişilmesi					
	En Hafif	Hafif	Orta	Ağır	En Ağır	Toplam
Öğrenci	2	10	23	42	278	355
	0,6%	2,8%	6,5%	11,8%	78,3%	100,0%
Öğretim Elemanı	2	2	6	7	29	46
	4,3%	4,3%	13,0%	15,2%	63,0%	100,0%
Toplam	4	12	29	49	307	401
	1,0%	3,0%	7,2%	12,2%	76,6%	100,0%

Akademik Konum	Bilgisayar sistemine zarar veren kodlar yazılması ve yayılması					
	En Hafif	Hafif	Orta	Ağır	En Ağır	Toplam
Öğrenci	3	22	69	136	125	355
	0,8%	6,2%	19,4%	38,3%	35,2%	100,0%
Öğretim Elemanı	1	2	7	14	22	46
	2,2%	4,3%	15,2%	30,4%	47,8%	100,0%
Toplam	4	24	76	150	147	401
	1,0%	6,0%	19,0%	37,4%	36,7%	100,0%

Akademik Konum	Bir bilişim sistemindeki verilere yetkisiz olarak erişip herhangi bir zarar vermeden sistemden çıkılması					
	En Hafif	Hafif	Orta	Ağır	En Ağır	Toplam
Öğrenci	53	66	89	81	66	355
	14,9%	18,6%	25,1%	22,8%	18,6%	100,0%
Öğretim Elemanı	3	4	13	12	14	46
	6,5%	8,7%	28,3%	26,1%	30,4%	100,0%
Toplam	56	70	102	93	80	401
	14,0%	17,5%	25,4%	23,2%	20,0%	100,0%

$\chi^2 = 7,56$ p =0,10

* Bazı çapraz tablolarda 5 den küçük beklenen değer sayısının %30 ve üzerinde olması nedeniyle ki-kare testi uygulanamamıştır.

Katılımcıların akademik konumlarına göre gruplanmış veriler üzerinde yapılan analizlerde en belirgin fark yine akademik aşırmacılık (plagiarism) davranışını ölçen soruda (Bkz Ek1. Soru 6 Madde 8) görülmektedir. Öğretim elemanı konumdaki katılımcıların %45,7 si söz konusu davranışı ağır suç olarak nitelerken; öğrenci konumundaki katılımcıların %18,3'ü en ağır suç olarak belirlemiştir. Diğer suç davranışları algısında iki grup arasında belirgin farklılıklar görünmemektedir.

Öğretim elemanı ve öğrenci grupları arasında bir diğer anlamlı fark siber ihlal suçu açısından saptanmıştır. Siber ihlal fiili (Bkz. Ek1 Soru 6 Madde 14) öğrencilerin %18,6 sı tarafından en ağır suç olarak belirlenirken; Öğretim elemanlarında bu oran %30,4 olarak hesaplanmıştır.

Çizelge 9.20 Cinsiyet Farklılıklarına Göre Bilişim Suçu Algıları

	Kimlik numarası, telefon numarası ve adres gibi kişisel bilgilerin web siteleri aracılığıyla toplanıp üçüncü şahıslara sunulması veya satılması.					
Cinsiyet	**En Hafif**	**Hafif**	**Orta**	**Ağır**	**En Ağır**	**Toplam**
Kadın	2	2	11	29	191	235
	0,9%	0,9%	4,7%	12,3%	81,3%	100,0%
Erkek	2	6	15	43	100	166
	1,2%	3,6%	9,0%	25,9%	60,2%	100,0%
Toplam	4	8	26	72	291	401
	1,0%	2,0%	6,5%	18,0%	72,6%	100,0%
$\chi^2 = 22,59$	p =0,00					
	Bir kişisel bilgisayara uzaktan müdahale ederek kişisel dosya, belge ve dökümanların elde edilmesi.					
Cinsiyet	**En Hafif**	**Hafif**	**Orta**	**Ağır**	**En Ağır**	**Toplam**
Kadın	0	4	18	53	160	235
	0,0%	1,7%	7,7%	22,6%	68,1%	100,0%
Erkek	4	8	25	47	82	166
	2,4%	4,8%	15,1%	28,3%	49,4%	100,0%
Toplam	4	12	43	100	242	401
	1,0%	3,0%	10,7%	24,9%	60,3%	100,0%
$\chi^2 = 20,71$	p =0,00					

Çizelge 9.20 Cinsiyet Farklılıklarına Göre Bilişim Suçu Algıları (devam ediyor)

	Çocuk pornografisi konulu fotoğraf ve video içeriği bulunan İnternet sitesi yayınlarının yapılması.					
Cinsiyet	**En Hafif**	**Hafif**	**Orta**	**Ağır**	**En Ağır**	**Toplam**
Kadın	0	1	3	11	220	235
	0,0%	0,4%	1,3%	4,7%	93,6%	100,0%
Erkek	2	4	7	13	140	166
	1,2%	2,4%	4,2%	7,8%	84,3%	100,0%
Toplam	2	5	10	24	360	401
	0,5%	1,2%	2,5%	6,0%	89,8%	100,0%
χ^2 = 11,82	p =0,01					
	Çocuk pornografisini temsil eden çizim ve animasyonlara yönelik içeriği bulunan İnternet sitesi yayınlarının yapılması.					
Cinsiyet	**En Hafif**	**Hafif**	**Orta**	**Ağır**	**En Ağır**	**Toplam**
Kadın	0	1	6	13	215	235
	0,0%	0,4%	2,6%	5,5%	91,5%	100,0%
Erkek	4	1	12	18	131	166
	2,4%	0,6%	7,2%	10,8%	78,9%	100,0%
Toplam	4	2	18	31	346	401
	1,0%	0,5%	4,5%	7,7%	86,3%	100,0%
χ^2 = 15,79	p =0,003					
	Çocuk pornografisi konulu içeriği bulunan İnternet sitesi yayınlarına erişilmesi.					
Cinsiyet	**En Hafif**	**Hafif**	**Orta**	**Ağır**	**En Ağır**	**Toplam**
Kadın	0	6	10	26	193	235
	0,0%	2,6%	4,3%	11,1%	82,1%	100,0%
Erkek	4	6	19	23	114	166
	2,4%	3,6%	11,4%	13,9%	68,7%	100,0%
Toplam	4	12	29	49	307	401
	1,0%	3,0%	7,2%	12,2%	76,6%	100,0%
χ^2 = 15,90	p =0,003					
	Bilgisayar sistemine zarar veren kodlar yazılması ve yayılması.					
Cinsiyet	**En Hafif**	**Hafif**	**Orta**	**Ağır**	**En Ağır**	**Toplam**
Kadın	1	14	31	84	105	235
	0,4%	6,0%	13,2%	35,7%	44,7%	100,0%
Erkek	3	10	45	66	42	166
	1,8%	6,0%	27,1%	39,8%	25,3%	100,0%
Toplam	4	24	76	150	147	401
	1,0%	6,0%	19,0%	37,4%	36,7%	100,0%
χ^2 = 22,19	p =0,00					

Çizelge 9.20 Cinsiyet Farklılıklarına Göre Bilişim Suçu Algıları (devam ediyor)

	Bir bilişim sistemindeki verilere yetkisiz olarak erişip herhangi bir zarar vermeden sistemden çıkılması.					
Cinsiyet	**En Hafif**	**Hafif**	**Orta**	**Ağır**	**En Ağır**	**Toplam**
Kadın	24	40	56	61	54	235
	10,2%	17,0%	23,8%	26,0%	23,0%	100,0%
Erkek	32	30	46	32	26	166
	19,3%	18,1%	27,7%	19,3%	15,7%	100,0%
Toplam	56	70	102	93	80	401
	14,0%	17,5%	25,4%	23,2%	20,0%	100,0%
$\chi^2 = 10,84$ p =0,02						

Cinsiyet gruplarına göre yapılan analizlerde, en belirgin fark kişisel bilgilerin gizliliği ile ilgili soruda (Bkz. Ek1 Soru 6 Madde 5) tespit edilmiştir. Kadın katılımcılar, kişisel bilgilerin gizliliğine yapılan müdahaleyi %81,3 oranında en ağır suç olarak belirlerken; erkek katılımcılarda bu oran %60,2 dir.

Aynı kapsamda, bir kişisel bilgisayara uzaktan müdahale ederek kişisel dosya, belge ve dökümanların elde edilmesi (Bkz. Ek1 Soru 6 Madde 6) davranışı, kadın katılımcıların %68,1'i tarafından en ağır suç olarak nitelenirken; erkek katılımcıların %49,4'ü söz konusu fiili ağır suç olarak tanımlamıştır.

Cinsiyet grupları açısından bir diğer önemli sonuç, çocuk pornografisi konusunun ağır suç olarak algılanma yüzdelerinde tespit edilmiştir. Çocuk pornografisi içerikli web sitelerine erişim fiili (Bkz. Ek1 Soru 6 Madde 12) kadın katılımcıların %82,1'i tarafından en ağır suç olarak algılanırken erkek katılımcıların %68,2'si tarafından en ağır suç olarak tanımlanmıştır. Aynı fiili orta, hafif ve En Hafif suç olarak algılayan erkek katılımcıların oranı %17,4 iken bu oran kadın katılımcılarda %6,9 olarak hesaplanmıştır.

Çocuk pornografisini temsil eden çizim ve animasyonlara yönelik yayın yapılması fiili (Bkz Ek1 Soru 6 Madde 11) kadın katılımcıların %91,5'i tarafından en ağır suç olarak işaretlenirken; erkek katılımcılarda bu oran %78,9 olarak belirlenmiştir.
Çocuk pornografisi içerikli internet yayını yapma fiilini (Bkz Ek1 Soru 6 Madde 10) ağır ve en ağır suç olarak belirleyen kadın katılımcılar %93,4 oranındayken aynı oran erkek katılımcılarda %89,7 olarak hesaplanmıştır.

Cinsiyet gruplarına göre yapılan analizlerde dikkati çeken bir diğer önemli fark, bilgisayar sistemlerine zarar veren yıkıcı siber suçlar (virüs, trojan) konusunda tespit edilmiştir. Bilgisayar sistemine zarar verici kodlar yazmak ve yayınlamakla ilgili anket sorusuna (Bkz Ek1. Soru 6 Madde 13) kadın katılımcıların %44,7'si en ağır suç olarak algılarken; erkek katılımcılarda bu oran %25,3 olarak belirlenmiştir.

10. SONUÇ VE TARTIŞMA

Anket çalışmasının analizlerinde, katılımcıların bilişim suçu türleri arasında en çok çocuk pornografisi, özel hayatın gizliliği, akademik aşırmacılık ve siber hırsızlık konularında duyarlı oldukları tespit edilmiştir.

Çocuk pornografisi içerikli internet yayını yapılması davranışını katılımcıların %89,8'i en ağır suç olarak belirtmişlerdir. Suçun uluslararası anlaşmalar çerçevesinde diğer iki boyutu olan çocukları temsil eden çizim ve animasyonların yayınlanması ve çocuk pornografisi sitelerine erişim fiillerinin banka hesap hırsızlığı fiili kadar ağır bir suç olmadığı düşünülmüştür. Veri setinin gruplara ayrılması aşamasında çocuk pornografisi açısından en belirgin farklılık cinsiyete göre yapılan analizlerde tespit edilmiştir. Buna göre kadın katılımcılar, yayın yapılması fiilini erkek katılımcılardan %3,7 fazlalıkla, temsili çizim ve animasyon yayınlarını %12,6 fazlalıkla, sitelere erişim fiilini %13,9 fazlalıkla en ağır suç olarak belirtmişlerdir.

Katılımcıların en ağır bilişim suçu olarak seçtikleri ikinci fiil, banka hesap bilgilerinin elde edilmesi yöntemiyle işlenen siber ihlal ve siber hırsızlık davranışıdır. Anket sonuçlarına göre, %87 oranıyla en ağır suçlar arasında ikinci sırada yer alan davranış, en ağır suç sıralamasında çocuk pornografisi suçunun üç farklı biçiminden ikisini geride bırakmıştır.

Analiz sonuçlarına göre, ağır bir bilişim suçu olan ve Türkiye dahil bilişim suçları konusunda yasal düzenlemesi olan tüm hukuk sistemlerindeki en öncelikli konu olan siber ihlal fiili, katılımcılar tarafından En Hafif bilişim suçu olarak seçilmiştir. En Hafif suçlar sıralamasındaki ilk iki davranış siber ihlal suçunun belirgin örnekleridir. Örneklem analizleri, öğretim elemanı ve öğrenci grubu şeklinde

yapıldığında siber ihlal fiilini suç olarak belirten öğretim elemanı oranının öğrenci oranından %11,8 fazlalık gösterdiği tespit edilmiştir.

Siber hırsızlık türleri arasında yer alan akademik aşırmacılık (plagiarism) davranışı, En Hafif suçlardan üçüncüsü olarak belirlenmiştir. Örneklem gruplara ayrıldığında en belirgin farklılıklar akademik aşırmacılık konusunda tespit edilmiştir. Bilgisayar bilimleri ve hukuk eğitimi grupları açısından yapılan anket analizlerinde, hukuk eğitimi grubunun %61,5'i aşırmacılık fiilini ağır ve en ağır suç olarak tanımlarken; bilgisayar eğitimi grubunda bu oran %32,4 olarak belirlenmiştir. Öğretim elemanı, öğrenci gruplarında da en belirgin farklılık akademik aşırmacılık fiilinde tespit edilmiştir. Öğretim elemanları öğrencilere göre %24.7 fazlalıkla söz konusu davranışı ağır suç olarak nitelendirmişlerdir.

Katılımcıların ahlaki açıdan yanlış bulup, suç olmadığını düşündükleri fiillerden en belirgini çevrimiçi forum ve ansiklopedi sitelerine kasıtlı olarak hatalı bilgi eklenmesi fiili olarak tanımlanan siber vandalizm suçudur. İnterneti'in yoğun olarak okul ve işle ilgili konularda araştırma yapmak (%93,5) ve kişisel ilgi alanlarında araştırma yapmak (%90,5) amacıyla kullandıklarını belirten katılımcıların, temiz bilgiye ulaşma konusunda hassasiyet gösterdikleri düşünülmektedir.

Ahlaki açıdan yanlış olduğu düşünülen diğer davranışlar, eş, çocuk veya arkadaşların e-postalarını okuma fiili ve kişisel bilgilerin üçüncü kişilere sunulması olarak tespit edilmiştir. Örneklemde bulunan bireylerin, kişisel bilgilerin gizliliği konusunda hassas olduklarını söylemek mümkündür. Örneklem cinsiyet gruplarına ayrıldığında kadınların %81,3'ünün özel hayatın gizliliği konusunda yapılan ihlalleri en ağır suç olarak nitelendirdikleri; erkeklerde ise bu oranın %60,2 olduğu görülmektedir.

Yıkıcı siber suçların önemi konusundaki algı farklılığı eğitim ve cinsiyet grupları arasında tespit edilmiştir. Bilgisayar eğitimi grubu, fiilleri en ağır suç olarak algılarken hukuk grubunda orta derecede suç olarak belirlenmiştir. Aynı suç kadınlarda erkeklere oranla %19,4 fazlalıkla ağır suç olarak algılanmaktadır.

Bilişim suçu çeşitleri hakkındaki bilginin ölçüldüğü sorularda suç unsuru taşıyan fiillerden bir şahıs ya da firma hakkında hakaret içeren e-postaların başka

kullanıcılara iletilmesi, menkul kıymetler hakkında internet yoluyla manipulasyon yapma ve web sitesine genel erişimi engelleyici teknikler uygulama davranışları katılımcıların çoğunluğu tarafından suç olarak tanımlanmamıştır. Benzer şekilde bilişim sektöründe son derece normal bir davranış olan açık kaynak kodlu yazılımları ticari amaçlarla kullanma davranışının ise suç olduğu düşünülmüştür.

Çalışmanın sonuçları genel olarak incelendiğinde, bilgisayar ve hukuk eğitimi gruplarında suç algısı açısından anlamlı farklılıklar bulunmadığı, özellikle klasik suçların bilgisayar aracılığıyla işlenmesi konusunda hukuk eğitim grubundaki bireylerin diğer gruplardan belirgin şekilde farklılaşmadığı saptanmıştır. Cinsiyet ve akademik konum grupları üzerinde yapılan analizlerde de yalnızca medyada bahsi geçen suçlar konusunda anlamlı algı farkları oluştuğu, konunun teknik ve hukuksal kapsamdaki spesifik açılımlarında katılımcıların genel bir profile sahip olduğu belirlenmiştir.

Araştırma sonuçlarına göre, eğitim, akademik konum ve cinsiyet gruplandırmalarında bilişim suçu algısının popüler niteliği olmayan bilişim suçu türlerinde homojen dağılım göstereceği hipotezi doğrulanmıştır.

Ülkemizde bilişim hukuku gibi disiplinler arası alanlarda eğitim veren lisans ve yüksek lisans programlarının yetersiz olduğu bilinmektedir. Medya, bilişim suçlarına genellikle çocuk pornografisi ve siber dolandırıcılık boyutlarında yaklaşmaktadır. Yasalar tarafından suç olarak tanımlanan fiillerin açılımlarında yaşanan tartışmalar ve suçların tespitinde karşılaşılan engeller bulunmaktadır.

Modern hayatın önemli sorunlardan birisi haline gelen bilişim suçları ile mücadele amacıyla bilinçlendirici faaliyetlerin yaygınlaştırılmasının ve bilişim suçu konusundaki toplumsal bilgi ve algı düzeyinin klasik suçlar ölçüsünde geliştirilmesinin faydalı olacağı düşünülmektedir.

KAYNAKLAR LİSTESİ

[1] KÖKSAL, A., ENIAC'ın 60. Yılında TBD 35 Yaşında, http://www.bilisim.com.tr/akoksal/yayinlar/yazilar/AK_TBD_35yil_14Mr06.html

[2] KESKİN, İbrahim, Bilişim Suçları, Adalet Dergisi, Adalet Bakanlığı Yayın İşleri Başkanlığı. S.6, Sayı:29

[3] SHINDER, Debra Littlejohn and TITTEL, Ed, Scene Of The Cybercrimes, Syngress Publishing Inc, 2002.

[[4] JOHNSON, Thomas A, Forensic Computer Crime Investigation, CRC Press, 2005

[5] CyberCrime Law http://www.cybercrimelaw.net/content/history.html

[6] Elektronik Ticaret Hukuk Çalışma Grubu Raporu http://www.e-ticaret.gov.tr/raporlar/hukuk.htm

[7] Avrupa Konseyi Siber Suçlar Sözleşmesi Taslağı, Ankara Barosu Bilgi İşlem Merkezi Yayınları, 2007.

[8] Bilişim Ağı Hizmetlerinin Düzenlenmesi ve Bilişim Suçları Hakkında Kanun Tasarısı http://www.tbd.org.tr/genel/bizden_detay.php?kod=243&tipi=5&sube=

[9] DÜLGER, Murat Volkan, Bilişim Suçları, Seçkin Yayıncılık, 2004.

[10] Hukuk Çalışma Grubu Raporu, Türkiye Bilişim Şurası, 2002

[11] 5237 Sayılı Türk Ceza Kanunu http://www.tbmm.gov.tr/kanunlar/k5237.html

[12] MITNICK, Kevin, The Art of Deception, John Wiley and Sons, 2002

[13] Microsoft Güvenlik Danışma Belgesi (912920), http://www.microsoft.com/turkiye/guvenlik/bultenler/danisma/912920.mspx

[14] İLBAŞ, Çığır, Korsanlar Ada Sever, Akşam Gazetesi Teknopark , s.5, Sayı 7, 2005

[15] İLBAŞ, Çığır, Bilişim Suçlarının Tespitinde Kablosuz İnternet Engeli, Bilişim ve Hukuk, s34, yıl:1 sayı:1, 2006

Ek 1. Anket Formu

Sayın Katılımcı, Bu ankette, Başkent Üniversitesi, Fen Edebiyat Fakültesi, İstatistik ve Bilgisayar Bilimleri Ana Bilim Dalı, Bilgi Teknolojileri ve Sistem Yönetimi yüksek lisans tez çalışması için "Bilişim Suçları' nın Sosyo-Kültürel Seviyelere Göre Algı Analizi" konusunun araştırılması amaçlanmıştır. Soru formunda verdiğiniz yanıtlar gizli kalacaktır ve tamamen bilimsel bir amaca yönelik olarak kullanılacaktır.

Katkı ve yardımlarınız için teşekkür ederiz.

B u B ö l ü m H e r k e s T a r a f ı n d a n D o l d u r u l a c a k t ı r

Doğum Yeri ve Yılı : _____ / _____

Cinsiyetiniz : □ Kadın □ Erkek
Oturduğunuz Semt : _____

Ö Ğ R E N C İ Y S E N İ Z

Fakülte ve Bölümünüz : _____

Sınıfınız : □ 1 □ 2 □ 3 □ 4

Ö Ğ R E T İ M E L E M A N I Y S A N I Z

Mesleğiniz : □ Öğretim Üyesi □ Öğretim Görevlisi □ Araştırma Görevlisi

Fakülte ve Bölümünüz : _____

Medeni durumunuz : □ Bekar □ Evli □ Ayrılmış / Dul

Çocuğunuz var mı? : □ Evet □ Hayır

01. Teknoloji, Bilgisayar ve İnternet konularına ilgili misiniz? Bu konularla ilgili güncel gelişmeleri takip ediyor musunuz?

□ a) Konulara ilgi duymuyorum ve gelişmeleri takip etmiyorum.
□ b) Konulara ilgi duymuyorum fakat gelişmeleri yazılı ve görsel medyadan takip ediyorum.
□ c) Konulara ilgi duyuyorum fakat gelişmeleri takip etmiyorum.
□ d) Konulara ilgi duyuyorum ve gelişmeleri yakından takip ediyorum.

02. Ne kadar süredir İnternet kullanıyorsunuz?

□ a) İnternet kullanmıyorum. (Lütfen 06. Soruya geçiniz)
□ b) 1 yıldan az süredir kullanıyorum.
□ c) 2 – 5 yıldır İnternet kullanıcısıyım.
□ d) 6 – 9 yıldır İnternet kullanıcısıyım.
□ e) 10 yıldan uzun süredir İnternet kullanıyorum.

03. İnternet'e hangi ortamlardan bağlanıyorsunuz? (Birden fazla seçenek işaretleyebilirsiniz)

- 1) Ev
- 2) İşyeri / Okul
- 3) İnternet evleri (İnternet cafeler)
- 4) Ortak erişim alanları (Kafeterya, havaalanı terminal vb.)

04. İnternet'i hangi amaçlar için kullanıyorsunuz? (Birden fazla seçenek işaretleyebilirsiniz)

- 1) İşimle / derslerimle ilgili konularda araştırma
- 2) Kişisel olarak ilgi duyduğum konularda araştırma
- 3) Haber ve güncel gelişmeleri takip etme
- 4) İletişim
- 5) Sosyal çevre edinme
- 6) Oyun ve eğlence
- 7) Diğer (Açıklayınız :_____)

05. İnternet'i ortalama olarak kullanım sıklığınız nedir?

- a) İş / Okul saatleri dışında kullanmıyorum.
- b) Haftada 1 günden daha seyrek olarak kullanıyorum.
- c) Haftada bir gün kullanıyorum
- d) Haftada birkaç gün kullanıyorum.
- e) Hemen hemen her gün kullanıyorum.

06. 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**
01	Bir ülke veya devlet aleyhinde web sitesi yayını yapılması.					
02	Bir ülke veya devlet aleyhinde yayın yapan bir web sitesinin, bir kişi ya da grup tarafından kapatılması, erişiminin engellenmesi. (deface/hack)					
03	Bir banka müşterilerinin hesap bilgileri elde edilerek yetkisiz para transferi yapılması.					
04	Sahte Loto, şirket ortaklığı gibi tuzaklarla dolandırıcılık yapılması.					
05	Kimlik numarası, telefon numarası ve adres gibi kişisel bilgilerin web siteleri aracılığıyla toplanıp üçüncü şahıslara sunulması veya satılması.					
06	Bir kişisel bilgisayara uzaktan müdahale ederek kişisel dosya, belge ve dökümanların elde edilmesi.					
07	Bilgisayar donanımlarına fiziksel zarar verilmesi.					
08	İnternet'de bulunan bir makale ya da raporun referans gösterilmeden kullanılması.					
09	Başkası tarafından hazırlanan bilgisayar yazılımlarında değişiklik yaparak yazılım üzerinde hak iddia edilmesi.					
10	Çocuk pornografisi konulu fotoğraf ve video içeriği bulunan İnternet sitesi yayınlarının yapılması.					
11	Çocuk pornografisini temsil eden çizim ve animasyonlara yönelik içeriği bulunan İnternet sitesi yayınlarının yapılması.					
12	Çocuk pornografisi konulu içeriği bulunan İnternet sitesi yayınlarına erişilmesi.					
13	Bilgisayar sistemine zarar veren kodlar yazılması ve yayılması.					
14	Bir bilişim sistemindeki verilere yetkisiz olarak erişip herhangi bir zarar vermeden sistemden çıkılması.					

07. Lütfen aşağıdaki soruları, kişisel görüşlerinize göre, ilgili soruda Ahlaki Açıdan ve Hukuksal Açıdan kategorilerinde birer yanıt olmak üzere **HER SORU İÇİN İKİ KUTUYA X İŞARETİ YAZARAK YANITLAYINIZ**		**Ahlaki Açıdan**			**Hukuksal Açıdan**		
		Doğru	**Fikrim Yok**	**Yanlış**	**Suç**	**Fikrim Yok**	**Suç Değil**
01	Başka bir şahsa ait şifresiz bir kablosuz İnternet (wi-fi) erişimini kullanmak.						
02	Eş, çocuk ya da arkadaşların e-postalarını okumak.						
03	Çocukların İnternet kullanımını denetleyen ve takip eden yazılımlar kullanmak.						
04	Müstehcen içerikli web sitelerine bağlanmak.						
05	Reklam tanıtım amaçlı yığın e-posta (spam) göndermek.						
06	Bilgi, uyarı e-postalarını birçok kişiye aynı anda iletmek.						
07	Forum ve ansiklopedi sitelerine yanlış bilgiler eklemek.						
08	Halen gösterimde olan film dosyalarını paylaşım yazılımlarıyla temin etmek.						
09	Piyasaya yeni çıkan müzik albümlerini paylaşım yazılımlarıyla temin etmek.						
10	Eski tarihli film ve müzik albümlerini paylaşım yazılımlarıyla temin etmek.						
11	Başkasına ait bir bilişim sistemindeki güvenlik açıklarını araştırmak.						
12	Başkalarının İnternet trafiğini izleyen yazılımlar (sniffer) kullanmak.						
13	Açık kaynak kodlu yazılımları ticari kar sağlamak amacıyla kullanmak.						
14	Genel Kamu Lisansına (GPL) sahip işletim sistemlerini (Linux vb.) bireysel amaçlar için kullanmak.						
15	Erişimi servis sağlayıcılar tarafından engellenen web sitelerine (Youtube gibi) vekil sunucu (proxy) aracılığıyla ulaşmak.						
16	Bir web sitesine genel erişimi engelleyici teknikler kullanmak.						
17	Başkasına ait bir e-posta şifresini çözerek, şifreyi değiştirmeden hesabı kullanmak.						
18	Başkasına ait bir e-posta hesabının şifresini çözüp değiştirmek.						
19	İnternet kullanıcılarına ait kişisel bilgileri toplayıp üçüncü şahıslara sunmak.						
20	Ücretli lisansa sahip olan bir yazılımı seri numarasını elde etme yöntemiyle ücretsiz olarak kullanmak.						
21	Virüs ve trojan kodları yazmak ve yaymak.						
22	MSN, ICQ, Facebook gibi ücretsiz servislerde başkası adına hesap açmak ve kullanmak.						
23	E-posta hesabına gelen, şahıs ya da firmalara yönelik eleştiri, hakaret içerikli e-postaları başkalarına iletmek						
24	Bir menkul kıymet (hisse senedi vb.) hakkında İnternet kanalıyla kişisel yorumları beyan etmek.						

Ek 2. 5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun

MADDE 1- (1) Bu Kanunun amaç ve kapsamı; içerik sağlayıcı, yer sağlayıcı, erişim sağlayıcı ve toplu kullanım sağlayıcıların yükümlülük ve sorumlulukları ile internet ortamında işlenen belirli suçlarla içerik, yer ve erişim sağlayıcıları üzerinden mücadeleye ilişkin esas ve usûlleri düzenlemektir.

MADDE 3- (1) İçerik, yer ve erişim sağlayıcıları, yönetmelikle belirlenen esas ve usûller çerçevesinde tanıtıcı bilgilerini kendilerine ait internet ortamında kullanıcıların ulaşabileceği şekilde ve güncel olarak bulundurmakla yükümlüdür.
(2) Yukarıdaki fıkrada belirtilen yükümlülüğü yerine getirmeyen içerik, yer veya erişim sağlayıcısına Başkanlık tarafından ikibin Yeni Türk Lirasından onbin Yeni Türk Lirasına kadar idarî para cezası verilir.

İçerik sağlayıcının sorumluluğu

MADDE 4- (1) İçerik sağlayıcı, internet ortamında kullanıma sunduğu her türlü içerikten sorumludur.
(2) İçerik sağlayıcı, bağlantı sağladığı başkasına ait içerikten sorumlu değildir. Ancak, sunuş biçiminden, bağlantı sağladığı içeriği benimsediği ve kullanıcının söz konusu içeriğe ulaşmasını amaçladığı açıkça belli ise genel hükümlere göre sorumludur.

Yer sağlayıcının yükümlülükleri

MADDE 5- (1) Yer sağlayıcı, yer sağladığı içeriği kontrol etmek veya hukuka aykırı bir faaliyetin söz konusu olup olmadığını araştırmakla yükümlü değildir.
(2) Yer sağlayıcı, yer sağladığı hukuka aykırı içerikten, ceza sorumluluğu ile ilgili hükümler saklı kalmak kaydıyla, bu Kanunun 8 inci ve 9 uncu maddelerine göre haberdar edilmesi halinde ve teknik olarak imkân bulunduğu ölçüde hukuka aykırı içeriği yayından kaldırmakla yükümlüdür.

Erişim sağlayıcının yükümlülükleri

MADDE 6- (1) Erişim sağlayıcı;
a) Herhangi bir kullanıcısının yayınladığı hukuka aykırı içerikten, bu Kanun hükümlerine uygun olarak haberdar edilmesi halinde ve teknik olarak engelleme imkânı bulunduğu ölçüde erişimi engellemekle,
b) Sağladığı hizmetlere ilişkin, yönetmelikte belirtilen trafik bilgilerini altı aydan az ve iki yıldan fazla olmamak üzere yönetmelikte belirlenecek süre kadar saklamakla ve bu bilgilerin doğruluğunu, bütünlüğünü ve gizliliğini sağlamakla,
c) Faaliyetine son vereceği tarihten en az üç ay önce durumu Kuruma, içerik sağlayıcılarına ve müşterilerine bildirmek ve trafik bilgilerine ilişkin kayıtları yönetmelikte belirtilen esas ve usûllere uygun olarak Kuruma teslim etmekle,yükümlüdür.
(2) Erişim sağlayıcı, kendisi aracılığıyla erişilen bilgilerin içeriklerinin hukuka aykırı olup olmadıklarını ve sorumluluğu gerektirip gerektirmediğini kontrol etmekle yükümlü değildir.
(3) Birinci fıkranın (b) ve (c) bentlerinde yer alan yükümlülüklerden birini yerine getirmeyen erişim sağlayıcısına Başkanlık tarafından onbin Yeni Türk Lirasından ellibin Yeni Türk Lirasına kadar idarî para cezası verilir.

Toplu kullanım sağlayıcıların yükümlülükleri

MADDE 7- (1) Ticarî amaçla toplu kullanım sağlayıcılar, mahallî mülkî amirden izin belgesi almakla yükümlüdür. İzne ilişkin bilgiler otuz gün içinde mahallî mülkî amir tarafından Kuruma bildirilir. Bunların denetimi mahallî mülkî amirler tarafından yapılır. İzin belgesinin verilmesine ve denetime ilişkin esas ve usûller, yönetmelikle düzenlenir.
(2) Ticarî amaçla olup olmadığına bakılmaksızın bütün toplu kullanım sağlayıcılar, konusu suç oluşturan içeriklere erişimi önleyici tedbirleri almakla yükümlüdür.
(3) Birinci fıkrada belirtilen yükümlülüğe aykırı hareket eden kişiye mahallî mülkî amir tarafından üçbin Yeni Türk Lirasından onbeşbin Yeni Türk Lirasına kadar idarî para cezası verilir.

Erişimin engellenmesi kararı ve yerine getirilmesi

MADDE 8- (1) İnternet ortamında yapılan ve içeriği aşağıdaki suçları oluşturduğu hususunda yeterli şüphe sebebi bulunan yayınlarla ilgili olarak erişimin engellenmesine karar verilir:

a) 26/9/2004 tarihli ve 5237 sayılı Türk Ceza Kanununda yer alan;

1) İntihara yönlendirme (madde 84),

2) Çocukların cinsel istismarı (madde 103, birinci fıkra),

3) Uyuşturucu veya uyarıcı madde kullanılmasını kolaylaştırma (madde 190),

4) Sağlık için tehlikeli madde temini (madde 194),

5) Müstehcenlik (madde 226),

6) Fuhuş (madde 227),

7) Kumar oynanması için yer ve imkân sağlama (madde 228),suçları.

b) 25/7/1951 tarihli ve 5816 sayılı Atatürk Aleyhine İşlenen Suçlar Hakkında Kanunda yer alan suçlar.

(2) Erişimin engellenmesi kararı, soruşturma evresinde hâkim, kovuşturma evresinde ise mahkeme tarafından verilir. Soruşturma evresinde, gecikmesinde sakınca bulunan hallerde Cumhuriyet savcısı tarafından da erişimin engellenmesine karar verilebilir. Bu durumda Cumhuriyet savcısı kararını yirmidört saat içinde hâkimin onayına sunar ve hâkim, kararını en geç yirmidört saat içinde verir. Bu süre içinde kararın onaylanmaması halinde tedbir, Cumhuriyet savcısı tarafından derhal kaldırılır. Koruma tedbiri olarak verilen erişimin engellenmesine ilişkin karara 4/12/2004 tarihli ve 5271 sayılı Ceza Muhakemesi Kanunu hükümlerine göre itiraz edilebilir.

(3) Hâkim, mahkeme veya Cumhuriyet savcısı tarafından verilen erişimin engellenmesi kararının birer örneği, gereği yapılmak üzere Başkanlığa gönderilir.

(4) İçeriği birinci fıkrada belirtilen suçları oluşturan yayınların içerik veya yer sağlayıcısının yurt dışında bulunması halinde veya içerik veya yer sağlayıcısı yurt içinde bulunsa bile, içeriği birinci fıkranın (a) bendinin (2) ve (5) numaralı alt bentlerinde yazılı suçları oluşturan yayınlara ilişkin olarak erişimin engellenmesi kararı re'sen Başkanlık tarafından verilir. Bu karar, erişim sağlayıcısına bildirilerek gereğinin yerine getirilmesi istenir.

(5) Erişimin engellenmesi kararının gereği, derhal ve en geç kararın bildirilmesi anından itibaren yirmidört saat içinde yerine getirilir.

(6) Başkanlık tarafından verilen erişimin engellenmesi kararının konusunu oluşturan yayını yapanların kimliklerinin belirlenmesi halinde, Başkanlık tarafından, Cumhuriyet başsavcılığına suç duyurusunda bulunulur.

(7) Soruşturma sonucunda kovuşturmaya yer olmadığı kararı verilmesi halinde, erişimin engellenmesi kararı kendiliğinden hükümsüz kalır. Bu durumda Cumhuriyet savcısı, kovuşturmaya yer olmadığı kararının bir örneğini Başkanlığa gönderir.

(8) Kovuşturma evresinde beraat kararı verilmesi halinde, erişimin engellenmesi kararı kendiliğinden hükümsüz kalır. Bu durumda mahkemece beraat kararının bir örneği Başkanlığa gönderilir.

(9) Konusu birinci fıkrada sayılan suçları oluşturan içeriğin yayından çıkarılması halinde; erişimin engellenmesi kararı, soruşturma evresinde Cumhuriyet savcısı, kovuşturma evresinde mahkeme tarafından kaldırılır.

(10) Koruma tedbiri olarak verilen erişimin engellenmesi kararının gereğini yerine getirmeyen yer veya erişim sağlayıcılarının sorumluları, fiil daha ağır cezayı gerektiren başka bir suç oluşturmadığı takdirde, altı aydan iki yıla kadar hapis cezası ile cezalandırılır.

(11) İdarî tedbir olarak verilen erişimin engellenmesi kararının yerine getirilmemesi halinde, Başkanlık tarafından erişim sağlayıcısına, onbin Yeni Türk Lirasından yüzbin Yeni Türk Lirasına kadar idarî para cezası verilir. İdarî para cezasının verildiği andan itibaren yirmidört saat içinde kararın yerine getirilmemesi halinde ise Başkanlığın talebi üzerine Kurum tarafından yetkilendirmenin iptaline karar verilebilir.

(12) Bu Kanunda tanımlanan kabahatler dolayısıyla Başkanlık veya Kurum tarafından verilen idarî para cezalarına ilişkin kararlara karşı, 6/1/1982 tarihli ve 2577 sayılı İdarî Yargılama Usulü Kanunu hükümlerine göre kanun yoluna başvurulabilir.

İçeriğin yayından çıkarılması ve cevap hakkı

MADDE 9- (1) İçerik nedeniyle hakları ihlâl edildiğini iddia eden kişi, içerik sağlayıcısına, buna ulaşamaması halinde yer sağlayıcısına başvurarak kendisine ilişkin içeriğin yayından çıkarılmasını ve yayındaki kapsamından fazla olmamak üzere hazırladığı cevabı bir hafta süreyle internet ortamında yayımlanmasını

isteyebilir. İçerik veya yer sağlayıcı kendisine ulaştığı tarihten itibaren iki gün içinde, talebi yerine getirir. Bu süre zarfında talep yerine getirilmediği takdirde reddedilmiş sayılır.

(2) Talebin reddedilmiş sayılması halinde, kişi onbeş gün içinde yerleşim yeri sulh ceza mahkemesine başvurarak, içeriğin yayından çıkarılmasına ve yayındaki kapsamından fazla olmamak üzere hazırladığı cevabın bir hafta süreyle internet ortamında yayımlanmasına karar verilmesini isteyebilir. Sulh ceza hâkimi bu talebi üç gün içinde duruşma yapmaksızın karara bağlar. Sulh ceza hâkiminin kararına karşı Ceza Muhakemesi Kanunu hükümlerine göre itiraz yoluna gidilebilir.

(3) Sulh ceza hâkiminin kesinleşen kararının, birinci fıkraya göre yapılan başvuruyu yerine getirmeyen içerik veya yer sağlayıcısına tebliğinden itibaren iki gün içinde içerik yayından çıkarılarak hazırlanan cevabın yayımlanmasına başlanır.

(4) Sulh ceza hâkiminin kararını bu maddede belirtilen şartlara uygun olarak ve süresinde yerine getirmeyen sorumlu kişi, altı aydan iki yıla kadar hapis cezası ile cezalandırılır. İçerik veya yer sağlayıcının tüzel kişi olması halinde, bu fıkra hükmü yayın sorumlusu hakkında uygulanır.

İdarî yapı ve görevler

MADDE 10- (1) Kanunla verilen görevler, Kurum bünyesinde bulunan Başkanlıkça yerine getirilir.

(2) Bu Kanunla ekli listedeki kadrolar ihdas edilerek Başkanlığın hizmetlerinde kullanılmak üzere 5/4/1983 tarihli ve 2813 sayılı Telsiz Kanununa ekli (II) sayılı listeye eklenmiştir. Başkanlık bünyesindeki iletişim uzmanlarına, Kurumda çalışan Telekomünikasyon Uzmanlarına uygulanan malî, sosyal hak ve yardımlara ilişkin hükümler uygulanır. İletişim Uzmanı olarak Başkanlığa atanan personelin hakları saklı kalmak kaydıyla, kariyer sistemi, Kanunun yürürlüğe girdiği tarihten itibaren altı ay içinde çıkarılacak yönetmelikle düzenlenir.

(3) Başkanlığa Kanunla verilen görevlere ilişkin olarak yapılacak her türlü mal veya hizmet alımları, ceza ve ihalelerden yasaklama işleri hariç, 4/1/2002 tarihli ve 4734 sayılı Kamu İhale Kanunu ile 5/1/2002 tarihli ve 4735 sayılı Kamu İhale Sözleşmeleri Kanunu hükümlerine tâbi olmaksızın Kurum bütçesinden karşılanır.

(4) Kanunlarla verilen diğer yetki ve görevleri saklı kalmak kaydıyla, Başkanlığın bu Kanun kapsamındaki görev ve yetkileri şunlardır:

a) Bakanlık, kolluk kuvvetleri, ilgili kamu kurum ve kuruluşları ile içerik, yer ve erişim sağlayıcılar ve ilgili sivil toplum kuruluşları arasında koordinasyon oluşturarak internet ortamında yapılan ve bu Kanun kapsamına giren suçları oluşturan içeriğe sahip faaliyet ve yayınları önlemeye yönelik çalışmalar yapmak, bu amaçla, gerektiğinde, her türlü giderleri yönetmelikle belirlenecek esas ve usûller dahilinde Kurumca karşılanacak çalışma kurulları oluşturmak.

b) İnternet ortamında yapılan yayınların içeriklerini izleyerek, bu Kanun kapsamına giren suçların işlendiğinin tespiti halinde, bu yayınlara erişimin engellenmesine yönelik olarak bu Kanunda öngörülen gerekli tedbirleri almak.

c) İnternet ortamında yapılan yayınların içeriklerinin izlenmesinin hangi seviye, zaman ve şekilde yapılacağını belirlemek.

ç) Kurum tarafından işletmecilerin yetkilendirilmeleri ile mülkî idare amirlerince ticarî amaçlı toplu kullanım sağlayıcılara verilecek izin belgelerinde filtreleme ve bloke etmede kullanılacak sistemlere ve yapılacak düzenlemelere yönelik esas ve usûlleri belirlemek.

d) İnternet ortamındaki yayınların izlenmesi suretiyle bu Kanunun 8 inci maddesinin birinci fıkrasında sayılan suçların işlenmesini önlemek için izleme ve bilgi ihbar merkezi dahil, gerekli her türlü teknik altyapıyı kurmak veya kurdurmak, bu altyapıyı işletmek veya işletilmesini sağlamak.

e) İnternet ortamında herkese açık çeşitli servislerde yapılacak filtreleme, perdeleme ve izleme esaslarına göre donanım üretilmesi veya yazılım yapılmasına ilişkin asgari kriterleri belirlemek.

f) Bilişim ve internet alanındaki uluslararası kurum ve kuruluşlarla işbirliği ve koordinasyonu sağlamak.

g) Bu Kanunun 8 inci maddesinin birinci fıkrasında sayılan suçların, internet ortamında işlenmesini konu alan her türlü temsili görüntü, yazı veya sesleri içeren ürünlerin tanıtımı, ülkeye sokulması, bulundurulması, kiraya verilmesi veya satışının önlenmesini teminen yetkili ve görevli kolluk kuvvetleri ile soruşturma mercilerine, teknik imkânları dahilinde gereken her türlü yardımda bulunmak ve koordinasyonu sağlamak.

(5) Başkanlık; Bakanlık tarafından 3348 sayılı Ulaştırma Bakanlığının Teşkilat ve Görevleri Hakkında Kanunun ek 1 inci maddesi uyarınca, Adalet Bakanlığı, İçişleri Bakanlığı, çocuk, kadın ve aileden sorumlu Devlet Bakanlığı ile Kurum ve ihtiyaç duyulan diğer bakanlık, kamu kurum ve kuruluşları ile internet servis sağlayıcıları

ve ilgili sivil toplum kuruluşları arasından seçilecek bir temsilcinin katılımı suretiyle teşkil edilecek İnternet Kurulu ile gerekli işbirliği ve koordinasyonu sağlar; bu Kurulca izleme, filtreleme ve engelleme yapılacak içeriği haiz yayınların tespiti ve benzeri konularda yapılacak öneriler ile ilgili gerekli her türlü tedbir veya kararları alır.

Yönetmelikler

MADDE 11- (1) Bu Kanunun uygulanmasına ilişkin esas ve usûller, Adalet, İçişleri ve Ulaştırma bakanlıklarının görüşleri alınarak Başbakanlık tarafından çıkarılacak yönetmeliklerle düzenlenir. Bu yönetmelikler, Kanunun yürürlüğe girdiği tarihten itibaren dört ay içinde çıkarılır.

(2) Yer veya erişim sağlayıcı olarak faaliyet icra etmek isteyen kişilere, telekomünikasyon yoluyla iletişim konusunda yetkilendirme belgesi olup olmadığına bakılmaksızın, yer veya erişim sağlayıcı olarak faaliyet icra etmesi amacıyla yetkilendirme belgesi verilmesine ilişkin esas ve usûller, Kurum tarafından çıkarılacak yönetmelikle düzenlenir. Bu yönetmelik, Kanunun yürürlüğe girdiği tarihten itibaren beş ay içinde çıkarılır.

İlgili kanunlarda yapılan değişiklikler

MADDE 12- (1) 4/2/1924 tarihli ve 406 sayılı Telgraf ve Telefon Kanununun 2 nci maddesinin (f) bendine aşağıdaki cümle eklenmiştir.

“Bu idarî para cezalarına ilişkin kararlara karşı, 6/1/1982 tarihli ve 2577 sayılı İdarî Yargılama Usulü Kanunu hükümlerine göre kanun yoluna başvurulabilir.”

(2) 4/7/1934 tarihli ve 2559 sayılı Polis Vazife ve Salahiyet Kanununun ek 7 nci maddesinin onuncu fıkrasının birinci cümlesinde yer alan “belirtilen” ibaresinden sonra gelmek üzere “telekomünikasyon yoluyla yapılan iletişime ilişkin” ibaresi eklenmiş, ikinci cümlesi “Oluşturulan bu Başkanlık bir başkan ile daire başkanlıklarından oluşur.” şeklinde değiştirilmiştir.

(3) 5/4/1983 tarihli ve 2813 sayılı Telsiz Kanununun 5 inci maddesine aşağıdaki fıkra eklenmiştir.

“Kurulca belirlenecek esas ve usûller çerçevesinde, 4/1/2002 tarihli ve 4734 sayılı Kamu İhale Kanununun 22 nci maddesinde belirtilen doğrudan temin usûlüyle serbest avukatlar veya avukatlık ortaklıklarıyla avukat sözleşmeleri akdedilebilir.”

(4) 1/11/1983 tarihli ve 2937 sayılı Devlet İstihbarat Hizmetleri ve Milli İstihbarat Teşkilatı Kanununun 6 ncı maddesinin ikinci fıkrasının son cümlesi “4/12/2004

tarihli ve 5271 sayılı Ceza Muhakemesi Kanununun 135 inci maddesinin altıncı fıkrasının (a) bendinin (14) numaralı alt bendi kapsamında yapılacak dinlemeler de bu merkez üzerinden yapılır.” şeklinde değiştirilmiş; dördüncü fıkrasında yer alan “Ancak” ibaresinden sonra gelmek üzere “casusluk faaliyetlerinin tespiti ve” ibaresi eklenmiş; altıncı fıkrasının üçüncü cümlesinde geçen “Bu madde” ibaresi “Bu fıkra” olarak değiştirilmiştir.

GEÇİCİ MADDE 1- (1) Başkanlığın kuruluştaki hizmet binasının yapımı, ceza ve ihalelerden yasaklama işleri hariç, Kamu İhale Kanunu ve Kamu İhale Sözleşmeleri Kanunu hükümlerine tâbi olmaksızın Kurum bütçesinden karşılanır.

(2) Halen faaliyet icra eden ticarî amaçla toplu kullanım sağlayıcılar, bu Kanunun yürürlüğe girdiği tarihten itibaren altı ay içinde 7 nci maddeye göre alınması gereken izin belgesini temin etmekle yükümlüdürler.

(3) Halen yer veya erişim sağlayıcı olarak faaliyet icra eden kişilere, Kurum tarafından, telekomünikasyon yoluyla iletişim konusunda yetkilendirme belgesi olup olmadığına bakılmaksızın, yer veya erişim sağlayıcı olarak faaliyet icra etmesi amacıyla bir yetkilendirme belgesi düzenlenir.