YAKIN DOĞU ÜNİVERSİTESİ
EĞİTİM BİLİMLERİ ENSTİTÜSÜ
BİLGİSAYAR VE ÖĞRETİM TEKNOLOJİLERİ EĞİTİMİ ANA BİLİM DALI

BİLİŞİM SUÇLARINA YÖNELİK EĞİTİM FAKÜLTESİ ÖĞRETMEN ADAYLARININ GÖRÜŞLERİNİN İNCELENMESİ

YÜKSEK LİSANS TEZİ

Özmen BOZAT

Lefkoşa
Ocak, 2020

YAKIN DOĞU ÜNİVERSİTESİ
EĞİTİM BİLİMLERİ ENSTİTÜSÜ
BİLGİSAYAR VE ÖĞRETİM TEKNOLOJİLERİ EĞİTİMİ ANA BİLİM DALI

BİLİŞİM SUÇLARINA YÖNELİK EĞİTİM FAKÜLTESİ ÖĞRETMEN ADAYLARININ GÖRÜŞLERİNİN İNCELENMESİ

YÜKSEK LİSANS TEZİ

Özmen BOZAT

Tez Danışmanı
Yrd. Doç. Dr. Kezban OZANSOY

Lefkoşa
Ocak, 2020

JÜRİ ÜYELERİNİN İMZA SAYFASI

Yakın Doğu Üniversitesi Eğitim Bilimleri Enstitüsü Müdürlüğü'ne,

Özmen BOZAT'ın "**Bilişim Suçlarına Yönelik Eğitim Fakültesi Öğretmen Adaylarının Görüşlerinin İncelenmesi**" isimli tezi Ocak 2020 tarihinde jürimiz tarafından Bilgisayar ve Öğretim Teknolojileri Eğitimi Ana Bilim Dalı'nda YÜKSEK LISANS TEZI olarak kabul edilmiştir.

	Adı-Soyadı	**İmza**
Başkan	: Prof. Dr. Zehra ALTINAY GAZİ	.....
Üye	: Yrd. Doç. Dr. Ahmet ARNAVUT	.....
Üye (Danışman)	: Yrd. Doç. Dr. Kezban OZANSOY	.....

Onay

Yukarıdaki imzaların, adı geçen öğretim üyelerine ait olduğunu onaylarım.

…./…./2020

Prof. Dr. Fahriye ALTINAY AKSAL

Enstitü Müdürü

ETİK İLKELERE UYGUNLUK BEYANI

Bu tezin içeriğinde sunulan verileri, bilgileri, dokümanları, akademik ve etik kurallar çerçevesinde elde ettiğimi; tüm bilgi, belge, değerlendirme ve sonuçları bilimsel etik ve ahlak kurallarına uygun olarak sunduğumu; çalışmada bana ait olmayan tüm veri, düşünce, sonuç ve bilgilere, bilimsel etik kuralların gereği olarak, eksiksiz şekilde uygun atıf ve kaynak göstererek belirttiğimi beyan ederim.

Özmen BOZAT

Ocak, 2020

ÖNSÖZ

Araştırma boyunca yardımlarını esirgemeyen, zaman ayırıp bana yol gösteren, destekleyen değerli danışmanım Yrd. Doç. Dr. Kezban OZANSOY'a sonsuz teşekkür ederim. Ayrıca eğitim hayatım boyunca emeği geçen tüm öğretmenlerime teşekkürlerimi sunarım. Son olarak her koşulda yanımda olan anneme, babama, ablama ve enisteme sonsuz teşekkürlerimi sunarım.

Özmen Bozat

ÖZET

BİLİŞİM SUÇLARINA YÖNELİK EĞİTİM FAKÜLTESİ ÖĞRETMEN ADAYLARININ GÖRÜŞLERİNİN İNCELENMESİ

BOZAT, Özmen

Yüksek Lisans, Bilgisayar ve Öğretim Teknolojileri Eğitimi Ana Bilim Dalı

Tez Danışmanı: Yrd. Doç. Dr. Kezban OZANSOY

Ocak 2020, 82 Sayfa

Bu araştırmanın genel amacı, öğretmen adaylarının bilişim suçlarına yönelik görüşlerinin incelenmesidir. Bu amaçla, öğrencilerin bu suçlara karşı önleyici tutum sergilemelerine yönelik görüşlerinin tespit edilmesi hedeflenmiştir. Bu araştırmada, öğretmen adaylarının bilişim suçlarına yönelik görüşlerinin incelenmesi amaçlandığından, nicel araştırma yöntemlerinden genel tarama modeli kullanılmıştır.

Araştırmanın çalışma grubunu 2018-2019 eğitim öğretim yılında Kuzey Kıbrıs'ta bulunan Yakın Doğu Üniversitesi Atatürk Eğitim Fakültesindeki 282 öğretmen adayı oluşturmaktadır. Araştırmada veri toplama araçları olarak, kişisel bilgi formu, geçerliği ve güvenirliği Gözler ve Taşçı (2015) tarafından sağlanıp geliştirilen "Bilişim Kavramları ve Suçlarına Yönelik Öğrenci Görüş Ölçeği" kullanılmıştır. Araştırmada elde edilen bulgulara göre öğretmen adaylarının bilişim kavramları ve suçlarına yönelik genel olarak görüşlerinin orta düzeyde olması, bu konuya ilişkin eğitimlerin artırılması gerektirmektedir.

Anahtar Kelimeler: Bilişim suçu, öğretmen adayları, siber zorbalık, İnternet güvenliği

ABSRACT

INVESTIGATION OF THE VIEWS OF THE TEACHER CANDIDATES OF THE EDUCATION FACULTY FOR INFORMATION CRIMES

BOZAT, Özmen

Master, Computer Education and Instructional Technologies

Education

Thesis Advisor: Assist. Assoc. Dr. Kezban OZANSOY

January 2020, 82 Pages

The general aim of this research is to examine the pre-service teachers' opinions about informatics crimes. For this purpose, it is aimed to determine the views of students towards their preventive attitude towards these crimes. In this research, general screening model, which is one of the quantitative research methods, was used since it was aimed to examine the opinions of prospective teachers on informatics crimes.

The study group of the research consists of 282 prospective teachers at the Near East University Atatürk Education Faculty in Northern Cyprus in the 2018-2019 academic year. In the research, "Information Concepts and Student Opinion Scale for Complications and Crimes", whose personal information form, validity and reliability were provided by Gözler and Taşçı (2015), were used as data collection tools. According to the findings obtained in the research, the fact that the pre-service teachers' opinions about informatics concepts and crimes are at a medium level requires increasing the trainings on this subject.

Key Words: IT crime, prospective teachers, cyberbullying, Internet security

İÇİNDEKİLER

TABLOLAR LİSTESİ

KISALTMALAR

MEB **:** Milli eğitim Bakalığı

TDK **:** Türk Dil Kurumu

TCK **:** Türk Ceza Kanunu

TÜİK **:** Türkiye İstatistik Kurumu

GİRİŞ

Bu bölümünde, araştırmanın problem durumuna ve alt problemlerine amacına, önemine, sınırlılıklarına ve tanımlara yer verilmiştir.

Problem Durumu

Gelişen teknoloji, her geçen zaman ışığında bilgi toplumlarının ve insan yaşamının temel dinamiğini oluşturmuştur. Bununla birlikte sıklıkla görülen bir durum ise bilişim teknolojilerinin, sürekli ve artarak gelişim gösterdiğidir. Her ne kadar da teknolojik yenilikler günümüz için üretilse de kısa zamanda demode olabilmektedir. Teknolojide yaşanan, gelişme ve yenilikler bireyleri ve toplumları etkilerken, insanlığın icat etmiş olduğu teknolojinin peşinden koşan bir özneye çevirmiştir (Balkı ve Saban, 2009).

Teknolojideki gelişmeler farklı amaç ve işlevleri bünyesinde barındırdığından insan yaşamının her evresinde bu teknolojilerle karşılaşmamız mümkün olmuştur. Teknoloji sayesinde istenilen bilgiye zaman ve mekân sınırı olmadan hızlı ve kolay bir şekilde ulaşım sağlanmaktadır.

İlk zamanlarda sıradan suçların bilgisayarlarla işlenmiş olması olarak görülmekte olan bu türden suç türleri, zaman içinde teknolojinin de gelişmesiyle daha önce olmayan yeni suç türünü de karşımıza çıkarmıştır. Bilişim teknolojilerinin, riskli ve kişilerin çıkarlarına uygun, yasa dışı kullanımından dolayı bilişim suçları ortaya çıkmıştır.

Bilişim suçu 1966 yılında ilk olarak "bilgisayar uzmanı banka hesabında tahrifat yapmakla suçlanıyor" isimli makale ile kayıtlara geçmiştir (Aydın, 1992). Alan yazın taramasında bilişim suçu kavramının net tanımına yer verilmemekle birlikte, bir çok benzer özelliğine rastlanılmaktadır. Bunlar; bilginin aktarılması, tekrar edilmesi, değerlendirilmesi, saklanması, dağıtımı ve aynı zamanda bilginin esas kaynağından alnıp kullanıcının kendisine aktarılması genel sistem bilimi olarak sıralanmaktadır. Bilişim suçu kavramı araştırmacılar tarafından farklı terimlerle ifade edilmektedir. Bunlar; siber suç, bilişim suçu ve teknoloji suçudur (Sönmez, 2018). Hekim ve Başıbüyük, (2013)'e göre bilişim suçları; siber suç, bilgisayar suçu, elektronik suç, dijital suç veya ileri teknoloji suçları olarak ifade etmektedir.

Günümüzde bilişim teknolojilerindeki artış, suç oranlarının artmasına ve yeni suç türlerine neden olmaktadır. Kaçakçılık ve Organize Suçlarla Mücadele Daire Başkanlığı tarafından 2011 senesinde yayınlanan rapora incelendiğinde en fazla bilişim suçlarının; kredi ve banka kartı dolandırıcılığında, bilişim sistemleri(sisteme girilmesi, bozma, verilerin yok edilmesi) internet bankacılığı, internet aracılığı ile nitelikli dolandırıcılığın yapılması, müstehcenlik, kumar ve gizliliğin ihlali olarak belirlenmiştir. Bilişim suçlarının günümüzde farklı çeşit ve yöntemlerle işlenildiği görülmektedir. Bunlar zararlı yazılımlar, e-posta bombardımanı, uzaktan yönetim araçları, bireyin sahte adreslere yönelendirilmesi, reklam bedelli yazılımlar ve sql kodlarının kullanılarak sistem kodlarına ulaşılması gibidir (Avşar ve Öngören, 2010).

Bilişim suçları kısa zaman diliminde ve geçmişinde az ipucu bırakarak büyük zararlar oluşturmaktadır (Yaycı, 2007). Bilişim suçlarına yönelik toplumun yeteri kadar farkındalığının olmaması bireylerin mağdur olma olasılığını artırmaktadır. Eğitim düzeyi yüksek olan bireylerin de mağdur olması oldukça çarpıcı bir durumdur (Gözler ve Taşçı, 2015).

Toplumun geleceğini şekilledirecek olan öğretmen adaylarının bilişim suçları konusunda gerekli eğitimleri almaları sağlanmalıdır. Çünkü eğitim lideri olarak görülen başta sınıf öğretmenleri ve diğer ilgili öğretmenler tarafından, siber suç veya diğer suç kavramlarıyla ilgili gerekli bilgi ve donanıma sahip olmaları genç nesilin daha bilinçli yetişmesini sağlayacaktır (Gözler ve Taşcı, 2015). Bu bakımdan bu araştırmada, eğitim fakültesindeki öğretmen adayları çalışma kapsamına alınarak bilişim suçlarına yönelik görüşleri incelenmeye çalışılmıştır.

Araştırmanın Amacı

Araştırmanın genel amacı, öğretmen adaylarının bilişim suçlarına yönelik görüşlerini incelemektir. Bu amaçla, öğrencilerin bu suçlara karşı önleyici tutum sergilemelerine yönelik görüşlerinin tespit edilmesi hedeflenmiştir. Bu amaca yönelik aşağıdaki alt amaçlar verilmiştir.

- Öğretmen adaylarının cinsiyeti ile internette mağdur olma veya saldırıya uğrama durumu arasında anlamlı fark var mıdır?
- Öğretmen adaylarının internet kullanma yılları ile internette mağdur olma veya saldırıya uğrama durumu arasında anlamlı fark var mıdır?

- Öğretmen adaylarının internete bağlanma ile internette mağdur olma veya saldırya uğrama durumu arasında anlamlı fark var mıdır?
- Öğretmen adaylarının, bilişim suçlarına yönelik görüşleri nasıldır?
- Öğretmen adaylarının bilişim kavramları ve suçlarına yönelik görüşleri ile cinsiyetleri arasında anlamlı fark var mıdır?
- Öğretmen adaylarının bilişim kavramları ve suçlarına yönelik görüşleri ile sınıf düzeyleri arasında anlamlı fark var mıdır?
- Öğretmen adaylarının bilişim kavramları ve suçlarına yönelik görüşleri ile internet kullanım yılları arasında anlamlı fark var mıdır?
- Öğretmen adaylarının bilişim kavramları ve suçlarına yönelik görüşleri ile mağdur olma veya saldırya uğrama durumu arasında anlamlı fark var mıdır?

Araştırmanın Önemi

Teknolojinin hızla gelişmesi insanoğlunun yaşamının her alanında teknolojiye kolaylıkla ulaşabilmesine neden olmuştur. Buna bağlı olarak bilişim suçları toplumların bilgi eksiklerinden veya deneyimlerinden yararlanarak mağdur edilmiştir.

Eğitim kurumları, bilişim güvenliği konusunda günümüzde önemli bir yere sahiptir. Eğitim fakültelerinde yürütülen öğretmen yetiştirme programlarında bilişim derslerinin yer alması göz önünde tutulduğunda bilişim güvenliği konusu ile ilgili olarak öğretmen adaylarının görüşlerinin belirlenmesi son derece önemlidir. Onların bilişim suçuna yönelik görüşleri ve bu suçların kendilerince algılanması gelecekte yetiştirilmesi beklenen öğrencilerin bilişim suçu konularında yeterli bilgi düzeyine ulaşmaları ve bu suçlara karşı daha önleyici bir tutum sergileyebileceklerdir. Bu özelliği ile araştırmanın alan yazına katkısı olacağı ve ileri araştırmalara yol göstereceği düşünülmektedir.

Araştırmanın Kapsam ve Sınırlılıkları

Bu alt bölümde, ele alınana araştırma ile ilgili elde edilen verilerle yapılan genellemelere ilişkin sınırlılıklar şöyledir:

1. Kuzey Kıbrıs Türk Cumhuriyeti'nde bulunan özel bir üniversitenin eğitim fakültesinde öğrenim gören öğretmen adayları ile sınırlıdır.
2. Çalışma 2018/2019 Eğitim-Öğretim yılı bahar yarıyılı ile sınırlıdır.

Tanımlar

Bilişim Suçu: Genel olarak elektronik ortamların kullanılarak iletişim teknolojileri araçları aracılığıyla gerek bilgisayar, tablet, cep telefonu veya pos makinası gibi araçların kullanılmasıyla mevcut internet alt yapısının kullanılarak bireylerin hakkının ihlal edilmesi veya kişilerin bu ortamlarda taciz edilmesiyle işlenen her türlü suç olarak tanımlanabilir.

Siber zorbalık: Günümüzde gelişen bilgi ve iletişim teknolojileri aracılığıyla çeşitli yöntemler kullanılarak gerek teknik, gerekse maddi yönden ya da her türlü zarar verme davranışlarının tümü olarak tanımlanabilir.

KAVRAMSAL ÇERÇEVE VE İLGİLİ ARAŞTIRMALAR

Bilişim suçları

Teknolojik gelişmeler insan hayatında çığır açıcı yeniliklere imza atarken kötü amaçlı kullanımları da beraberinde getirmiştir. Bilgisayar ve internet teknolojisi gün geçtikçe ilerlese de, bazı bireyler ya da örgütlü gruplar tarafından suç unsuru oluşturan, kendileri için menfaat sağlamak amacıyla kötü amaçlı kullanımların önüne geçememektedir. Suça teşebbüste bilgisayar ve internetin kullanılması bilgisayar suçları, internet suçları ve de genel olarak bilişim suçları gibi yeni kavramları hayatımıza sokmuştur (Sönmez, 2018).

Bilişim kavramı, mevcut bilginin aktarılması, uygun bir şekilde organizasyonu, bilginin korunması, tekrardan elde edilerek yeniden değerlendirilerek dağıtımının yapılmasında gerekli olan kuram ve yöntemleri içermektedir. Başka bir anlamda bilişim kavramı; bilginin kaynağından alınması ve kullanıcıya aktarılması ve genel sistem bilimi ve/veya sibernetik olarak bilinirken, otomasyon sayesinde kişinin çalıştığı alanda, doğru yer ve zamanda uygun olarak kullanılan teknolojileri de temelde ele alan bilgi sistemleri olarak bilinen etkinliklerdir (Aydın, 1992). Diğer bir anlamda kısaca söylemek gerekirse bu bilim ve/veya teknoloji dalı, bir veri işlem - bilgi işlem süreci şeklinde açıklanabilir.

Bilişim sistemi olarak bilinen sistemler günlük hayatta her alanda kullanıldığı bilinmekle beraber, bilişim teknolojisi her geçen gün daha ileri gitmektedir. Bilişim sistemleri denildiğinde akla yalnızca bir bilgisayar sistemi değil, akla yazılımlar, banka kartı, cep telefonu, internette para transferi, elektronik imza, e-devlet uygulamaları, web ortamına atılmış veriler vb. gibi gelişmiş teknolojik araç gereç ve sistemler gelmektedir (Yaycı, 2007).

Bilişim suçları için birden fazla kavram söylenmiş olsa da genel olarak kabul görmüş bir tanım bulunmamaktadır. Gelişen teknolojiyle beraber bilisim suçlarının da işlenme şekillerinin degişmesi tanımı daha da güçleştirmektedir.

Bilgisayar sistemlerinin yaygın bir şekilde kullanılması ile bilişim suçları da aynı şekilde paralel olarak ortaya çıkmıştır. Bilişim suçları günümüzde o kadar artmıştır ki, bundan dolayı ceza hukuku ve yasaların düzenlenmesi gereksiniminin

doğması esasta internetin icadı ve yaygın olarak bireyler tarafından kullanılmasıyla başlamıştır (Dülger, 2015).

Riskli kullanım nedeniyle bilişim teknolojileriyle birlikte bilişim suçları da doğmuştur. Bilişim suçu denildiğinde, bilişim alanında yapılmış olan yenilikler ile birlikte ceza hukukuna girmiş bir kavram olarak karşımıza çıkmaktadır. İlk başlarda günlük hayatta karşılaşılan suç türlerinin bilgisayar sistemleri ortamlarında da işlenmesi olarak görmüş olan bu suç çeşidi, zaman içinde teknolojide yaşanan gelişmelerle, daha önce karşılaşılmayan yeni suç çeşitlerini de ortaya çıkarmış oldu. Bilişim suçu denildiğinde veya uluslararası alandaki adlarını söylemek gerekirse "siber suç", "elektronik suç", "dijital suç" ve büyük oranda "bilgisayar suçu" ve "bilişim suçu" ifadelerinin daha çok kullanılmaktadır (Barret, 1997).

Türk ceza hukuku içerisinde yer alan bilişim suçu mevcut elektronik kayıtlara yasadışı bir şekilde erişime açılması ve/veya mevcut bu elektronik kayıtların yasadışı bir şekilde değiştirilme teşebbüsü, silinmesi ve/veya bu türdeki kayıtların ele geçirilmesi veya bu konuda hazırlık yapılması olarak tanımlanmıştır (Aydın, 1992). En çok kabul alan diğer bir tanımı ise 1993 yılında Avrupa Ekonomik Topluluğu Uzmanlar Komisyonu toplantısında ifadelendirilmiş tanımdır. Yapılmış olan bu tanıma göre bilgisayar suçu, bilgilerin otomatik bir şekilde işleme alan ve/veya verilerin bir noktadan diğer bir noktaya taşınmasında görev yapan bir sistem ile, yasa dışı bir şekilde, ahlak dışı bir yapılmış bir hareketle veya her hangi bir yetki kullanmadan gerçekleştirilmiş olan her türlü davranış biçimi şeklinde ifade edilebilir (Dülger, 2015).

Dikkatli bir şekilde bilişim suçlarının içeriği incelendiğinde, oldukça kapsamlı ve karmaşık olduğu görülebilir. Bu suç türleri; iletişim teknolojilerinin kullanılmasıyla bireylere, toplum geneline ve devlete yönelik, kanun dışı yasaklanmış faaliyetlerin gerçekleştirilmesi biçiminde belirtilmiştir. Bilişim alanında yaşanan gelişmeler, internete bağlanabilen mobil araçların, en çok da akıllı telefonların, bilişimin aktif olarak kullanıldığı tüm alanlarda yaygın biçimde kullanılmasıyla, internet üzerindeki kontrol ve güvenlik açıklarından dolayı sanal dünya üzerinde suç işlenmesinin önü de açılmış oldu (Bahar, 2018).

Perry (1986) bilişim suçlarını bilginin, programların, servislerin veya haberleşme ağlarının çökmesi, bu sistemlerin hırsızlığı, kanun dışı kullanımı,

değişikliğe uğratılması veya kopyalanması olarak ifade ederken, Parker (1989) ise bu suçun oluşması halinde bu suçu işleyene menfaat sağlaması ya da mağdur olana bir şeyler kaybettiren, kasıtlı davranışlar olarak ifade etmiştir. Özaydın (2010) ise bilgisayarın bireysel menfaat uğruna kullanılması biçiminde ifade edilmiştir.

Öyle ki yaşadığımız yüzyılda, çocukluktan itibaren bireyler kendilerini toplumdan soyutladıkları zaman diğer bireyler ile iletişim kurmada problemler yaşayabilmektedirler. Bunun nedeni akıllı telefon, tablet, bilgisayar, internet ve diğer bilişim teknolojilerinin imkanlarını kullanan kişiler kendi menfaatleri doğrultusunda, diğerlerinin haklarına gasp ederek, bu durumun sanki de etik kurallar çerçevesinde yaptıklarını sanmalarıdır (Özaydın, 2010). Her geçen gün internet ve bilişim sistemlerinde yaşanan gelişmeler bireyler arasında sanal olarak mesafe oluşturmuştur. Bundan dolayı da internette yapılmış olan etik veya yasal olmayan bir davranış sonucunda etkilenmiş olan bireyi anlamaya çalışmak giderek zorlaşmış ve etik anlamda duyarlılık da böylece yok olmuştur. Bunun yanında bireyler kendi menfaatlerini diğerlerinin kaygılarının da önünde tutarak, sosyal medyada diğerlerini rahatsız ederek, kanun dışı yolları kullanarak müzik, video, oyun, yazılımlar vb. indirmektedirler (Torun, 2007).

Bilişim Suçlarının Çeşitleri

Bilişim suçu denildiğinde, bilişim ortamında işlendiği bilinen, geleneksel suç olarak görülmeyen, bilgisayar sistemleri ve internetteki suçlar olarak ya da bilişim sistemleri kullanılarak veya bilişim sistemlerinden yararlanılmak suretiyle işlenmekte olan bilişim suçları klasik suçlar biçiminde ikiye ayrılır (Türkiyede İnternet, 2019).

Avrupa Ekonomik Topluluğu bilişim suçunu mevcut bilgiyi otomatik olarak kanuni olmadan, ahlak veya yetki dışı otomatik olarak işleme konması davranışı olarak ifade etmiş ve beş maddede ele almıştır. Bunlardan birincisi bilgisayardaki bir kaynağa veya bir verinin kaynağına yasa dışı bir şekilde ulaşılarak naklinin sağlanması için bilerek bilgisayar üzerindeki verilere erişim sağlayarak bu verilerin bozulması, silinmesi veya tamamen ortadan yok edilmesidir. İkinci olarak, bir menfaat ya da sahtekarlık yapmak amacıyla bilerek ve isteyerek bilgisayar üzerindeki verilere ve/veya programlara girmek, bozmak, silmek, yok etmektir. Bunlardan üçüncüsü ise bilgisayar sisteminin çalışmasını engellemek amacıyla

bilerek ve isteyerek bilgisayar üzerinde bulunan verilere veya programlara girmek, bozmak, silmek, yok etmektir. Dördüncü olarak, ticari olarak yarar sağlamak için bir bilgisayar programına sahip kişinin haklarını yasal olmayan yollardan zarara uğratmak gelmektedir. Bunlardan beşincisi ise, bilgisayar sisteminden sorumlu kişinin izni olmadan mevcut güvenlik tedbirlerini aşarak sisteme kasıtlı bir şekilde müdahale etmektir (Özel, 2001 ve Dolu, 2011).

Birleşmiş Milletler Uyuşturucu ve Suç Ofisi de uluslararası alanda bir siber suç veya siber saldırı tanımının olmadığına vurgu yapmaktadır (United Nations Office On Drugs and Crime). Suçlar tipik olarak belirli kategoriler etrafında toplandığını belirtmektedir. Bunlar, bilgisayar üzerideki verilerin ve sistemlerin gizliliği, bütünlüğü ve kullanılabilirliğine yönelik karşı suçlar, ikincisi ise bilgisayarla ilgili suçlar, bunlardan üçüncüsü içerikle ilgili suçlar, son olarak ise telif hakkı ve ilgili hakların ihlaliyle ilgili suçlar gelmektedir.

Genel olarak, siber suç, siber bağımlı suçlara, siber özellikli suçlara ve belirli bir suç türü olarak çevrimiçi çocuk cinsel sömürüsü ve kötüye kullanılması olarak tanımlanabilir. Siber-bağımlı suç, bir BİT altyapısı gerektirir ve genellikle kötü amaçlı yazılımların oluşturulması, yayılması ve dağıtılması, fidye yazılımı, kritik ulusal altyapıya yapılan saldırılar (örneğin bir web sitesinin organize bir suç grubu tarafından siber olarak ele alınması) sonucunda alınması olarak tanımlanır. Genellikle web sitesini verilerle aşırı yükleyerek çevrimdışı saldırı düzenlenmektedir (bir DDOS saldırısı).

Siber özellikli suç, çevrimdışı dünyada meydana gelebilecek ancak aynı zamanda BİT tarafından da kolaylaştırılabilen suçtur. Bu genellikle çevrimiçi sahtekarlıkları, çevrimiçi uyuşturucu alımlarını ve çevrimiçi kara para aklamayı içerir. Çocuk Cinsel Sömürü ve İstismar, açık internet, karanlık ağ forumları ve gittikçe artan bir şekilde "seksüel" olarak bilinen haraç yoluyla yaratılan görüntülerin sömürülmesidir (UNODC, 2019).

Bilişim Suçu Türleri

Bilişim suçlarını hedeflerine ve tekniklerine göre çok farklı çeşitlere ayrılabilir. Buna göre bilişim suçlarını ilk olarak bilgisayar sistemleri veya servislerine bir yetki olmadan erişimin sağlanması olarak ifade edilebilir. Diğer

türlerden bazıları ise bilgisayar sabotajı, bilgisayar aracılığıyla dolandırıcılık, bilgisayar aracılığıyla sahtecilik, bir bilgisayar yazılımının ilgili kişiden izin olmadan kullanımı, bireylere ait verilerin art niyetle kullanımı, sahte kimlik yaratma veya başkasının kimliğine bürünüp o kişinin taklidini yapma, kanun dışı yayınlar, ticari sırların yasadışı olarak çalınması, teror faaliyetleri, çocuk pornografisi, hacking ve diğer suçlar (organ, fuhuş, tehdit, uyuşturucu, vb.) olarak karşımıza çıkmaktadır (Bilgi Teknolojileri ve İletişim Kurumu, 2019).

Bilişim suçlarına yönelik olarak daha genel ve içerleyici bir tanımınn yapılmamış olmasının zorluğu ve bu konulardaki çekinceler olmasına rağmen bilişim suçu, "verilere karşı ve/veya veri işlemle bağlantısı olan sistemlere karşı, bilişim sistemleri aracılığıyla işlenen suçlar" şeklinde tanımlanabilir (Dülger, 2004).

Kimlik Hırsızlığı

Kimlik hırsızlığı hedeflenen kurbanın kişisel bilgilerini çalmak için düzenlenmiş bir süreçtir. Bu suç için genellikle elektronik posta kullanılır. En sık rastlanılan kimlik hırsızlığı olaylarında, fail kurbanların bilgilerinin bulunduğu kurumun (banka, kredi kurumu vb.) web sitesine çok benzeyen bir web sayfası hazırlar. Daha sonra fail kurbanlara bu kurumda bulunan hesaplarının doğrulanmaya ya da yenilenmeye ihtiyacının olduğunu belirten mailler atar. Kurbanlar, bu mailde bağlantı olarak verilen failin hazırladığı sahte web sayfasına bilgilerini doğrulamak için girerler. Bu sayfada, failin bilmek istediği bilgileri doldururlar ve doldurma işlemi bittikten sonra onay verdiklerinde tüm kişisel bilgileri failin eline geçer. Böylelikle fail, bu bilgilerle kurumun gerçek web sitesine girerek kurbanların hesaplarıyla dilediğini yapabilir. Kimlik hırsızlığı suçları genellikle belirlenmesi çok zor suçlardır. Bunun ilk nedeni, kurbanın böyle bir hırsızlıkla karşılaştığının farkında olmayışıdır. Çalınan hesaplarla yapılan işlemlerden kurban bir iki hafta sonra haberdar olmaktadır. Bu süre sonrasında, kurban internet üzerinden bilgi doğrulama yapmasıyla, başına gelen olay arasında bir bağ kuramamaktadır. Diğer bir neden ise, bu konuda uzmanlaşmış failler, kendi bilgilerini çok iyi sakladığından onları yakalamak hemen hemen imkânsızdır. Üçüncü neden, kurulan bu sahte sitelerin yabancı sunucular üzerinde kurulmuş olmasıdır. Yabancı sunucu üzerindeki bu sahte sitelerin izini sürmek ise site kapatıldıktan sonra imkânsızdır (Easttom, 2011).

Kimlik hırsızlığı için gönderilen elektronik postalar, direkt olarak mağdurlardan kişisel bilgilerini doldurmalarını gerektiren bir form içerebilir. Bazı kimlik hırsızlığı için gönderilen elektronik postalar ise kurbanların tıpkı banka telefonlarında olduğu gibi menülerin olduğu sahte bir telefon numarasını aramasını talep edebilir. Ayrıca fail tarafından gönderilen bu elektronik postalar açıldığında mağdurun bilgisayarına bir yazılım yükler ve mağdur bankasının gerçek web sayfasına girip bilgilerini girdiğinde o yazılım bu bilgileri kaydedip faile yollar (Lininger ve Vines, 2004).

Günümüzde kimlik hırsızlığı için her gün milyonlarca internet kullanıcısına bu sahte mailler gelmektedir ancak eskisine oranla kullanıcılar bilinçli olduğu için bu tuzaklara düşen mağdur sayısı azalmıştır.

Bilgisayar Korsanlığı (Hacking)

Bilgisayar korsanlığı yapan kişiler literatürde "hacker" olarak anılmaktadır. Amerikan Hükümeti bilgisayar güvenlik danışmanlarının sistemini kırarak kötü de olsa üne kavuşmuş Kevin Mitnick bir hackerdır. Aynı zamanda, Linux işletim sistemini geliştiren Linus Torvalds da bir hackerdır. İkisi de yazılım geliştirmektedir ancak birinin geliştirdiği yazılım kötü amaçlıyken diğeri pozitif amaçlıdır. Bu noktada, bu iki örneği ele aldığımızda hackerı yaşamak için kazancını bilgisayar üzerinden kazanan/çalan kimse olarak tanımlayabiliriz (Jordan, 2008).

Hacktivizm

Hacktivizm internet üzerinde grupların propaganda yaptığı popüler politik eylem olarak adlandırılabilir. Hacktivizm bilgisayar korsanlığı ile politik eylemin birleşmesi olarak da tanımlanabilir. Hacktivizm, aktivizmin elektronik ortama girmiş halidir (Jordan ve Taylor, 2004). Diğer bir deyişle, "hacktivizm, hacklemenin henüz olgunlaşmamış siyasal ajandası ve küreselleşmenin etkilerine artan bir oranda hassas hale gelen ve entelektüel bir bağlamda ortaya çıkan durum üzerine inşa edilen bir faaliyettir.". Hacktivizm eylemcilerine hacktivist denir (Taylor, 2014).

Hacktivizmin doğuşu 1999'da EDT adlı bir grubun yaptığı sanal oturma eylemine dayanır. Bu eylem Meksika Cumhurbaşkanlığı, Beyaz Saray ve Pentagon'a karşı yapılmış bir eylemdir. Grup, oturma eylemi sırasında seçmiş oldukları bu üç

hedefin bilgisayarlarına saldırıda bulunmuştur. Kullandıkları saldırı biçimi, hedef web sitelerine aynı anda farklı sunuculardan milyonlarca girişin yapıldığını algılatarak aşırı yüklemeye neden olup söz konusu sitelerin çökmesini sağlamaktadır. Hacktivistlerin çoğu teknik anlamda donanımlıdır. Hacktivistlere göre haktivizm elektronik biçimde sisteme karşı bir başkaldırı, isyandır. Hacktivistler yalnızca interneti kullananlar, interneti yanlış kullananlar ve interneti kötüye kullananlar olarak üç gruba ayrılabilir. Hacktivistler, web sayfalarında ilgili oldukları politik ya da sosyal konuyla ilgili bilgi paylaşımı, plandıkları aktivitelerin duyurulması, insanların onlara katılması için formların bulundurulması ya da maddi destek almak için hesap numaralarının yayınlanması gibi veriler bulundurur (Baldi, Gelbstein, Kurbalija, 2003).

Hacktivistlerin en dikkat çekici eylemlerinden biri Dünya Ticaret Örgütü'ne (WTO) karşı yaptıkları aktivitedir. Örgütün önceki organizasyon adıyla (GATT) alınan web sitesi (http://www.gatt.org), örgütün adı değişince kullanımdan çıktı ve yeni isimle (WTO) başka bir web sitesi (http://www.wto.org) alındı. Boşa çıkan eski adresle ilgili yetkililer herhangi bir önlem almayınca, bu adres hacktivistler tarafından ele geçirildi ve site içinde Dünya Ticaret Örgütü karşıtı eylemlere yer verildi. Hacktivistler bu şekilde sahte web siteleri oluşturdukları gibi, propaganda için var olan gerçek web sitelerin içeriğiyle de oynamaktadırlar. Hacktivistler, web sitelerin bulunduğu sunuculara erişim sağlayarak, istedikleri gibi hedeflenen web sitenin içeriğini değiştirip, silebilmektedirler (Baldi, Gelbstein ve Kurbalija, 2003).

Sanal Taciz

Son birkaç yılda taciz, gerçek hayatta insanların sıkça maruz kaldığı bir olgu haline gelmiştir. En çok karşılaşılan türleri ise cinsel taciz ve adam öldürme olarak kayıtlara geçmektedir. Sanal taciz ise daha farklı bir tanıma sahiptir. İnterneti kullanarak kişi ya da kişileri korkutmak, tehdit etmek ya da küçük düşürmek sanal taciz olarak tanımlanabilir. Bu bağlamda, günümüzde en çok rastlanılan sanal taciz, tehdit elektronik postaları yollanmasıdır. Tehdit söz konusu olduğunda ise ciddi ölüm tehditleri ile kızgınlıkla yazılmış herhangi bir tehdit mesajı arasında bir farkın olduğu unutulmamalıdır. Neyin sanal taciz olduğu neyin olmadığını anlamak için dört faktörü ele almak gerekir. İlk faktör güvenilirliktir. Eğer bir kullanıcı onun kişisel bilgilerini (adres, fotoğraf, iş yeri vb.) bildiğini gösteren birinden bir tehdit alıyorsa,

bu tehdidi ciddiye almalıdır. İkinci faktör ise sıklıktır. Eğer kullanıcı sık sık aynı kişiden tehditkâr mesajlar alıyorsa, yine ortada ciddi bir durum var demektir. Üçüncü faktör olarak belilirlilik ele alınabilir. Eğer tacizci, kullanıcıya kesin bir şekilde yer ve zaman vererek zarar vereceği tehdidini veriyorsa bu noktada mağdur hukuki işlem başlatmalıdır. Son faktör olarak yoğunluk ele alınmaktadır. Burada önemli olan kullanılan üslub ve tehdidin yoğunluğudur. Eğer üslub son derece ciddi ve tehdit detaylı bir şekilde söylendiyse, mağdur bu mesajı dikkate almalıdır (Easttom, 2011).

Sanal tacizciler sürekli tehdit mesajları göndermenin yanısıra, hedefledikleri kişilere iftira atarak da korku yayabilmektedirler. Hedef kişi hakkında sanal ortamda asılsız suçlamalar yaparak o kişilerin irtibarını yok etmeye çalışabilirler. Hedef kişilerin akraba ve yakın çevresindekilere ait elektronik posta hesaplarını öğrenek, kişi hakkında asılsız söylemlerde bulunabilirler. Ayrıca, başka tacizcileri de hedef kişiyi taciz etmeleri için organize edebilmektedirler. Bu sayede kurban çok kısa sürede binlerce tehdit mesajıyla başa çıkmak durumunda kalmaktadır. Sanal tacizcilerin bir diğer kozu ise kurban yerine mal ya da hizmet sipariş etmeleridir. Çoğu sanal tacizci kurbanları için porno dergi üyeliği başlatmakta ya da kurbanlarını küçük düşürmek için onlar adına alınmış seks oyuncaklarını iş yerlerine yollatmaktadır (Bocij, 2004).

Dolandırıcılık

İnternette dolandırıcılık, daha çok açık arttırma ve çek/para tahsilatı dolandırıcılığı olarak iki şekilde yapılmaktadır. Online açık arttırma dolandırıcılığında failler maddi kazanç elde etmek için açık arttırmaya hile karıştırmaktadırlar. Satıcı kimliğinde olan failler, alınan malın gönderiminde kargo şirketi kaynaklı hata olduğunu göstererek, açık arttırma sitesinde sunduğu maldan daha az ederi olan farklı bir malı kurbana göndererek, gönderiyi çok geç yaparak ya da satış esnasında satılan malla ilgili eksik/yanlış bilgi vererek dolandırıcılık yapmaktadırlar. Çek/para tahsilatı dolandırıcılığında ise bu kez kurban bir mal satmaktadır ve alıcı olan fail malı elden teslim almak istediğini söyler. Kurbana malın fiyatından daha fazla bir rakam yazdığı sahte çeki ya da sahte bütün parayı verir. Kurban, fiyatın daha düşük olduğunu söylediğindeyse, kurbandan hatası için özür dileyerek paraüstü talep eder. Kurban paranın ya da çekin sahte olduğunu çok sonra anlar (Easttom, 2011).

İnternette dolandırıcılığın bir diğer şekli ise işe alma dolandırıcılığıdır. Fail bilinen bir şirketin işvereni rolüne girerek, iş arayanlara onların bilgilerini isteyen mailler atarak hedeflenen kişilerin gerekli bilgilerini ele geçirir. Kimlik hırsızlığına da giren bu dolandırma yöntemiyle, kişilere maddi ve manevi zarar verilebilir (Miller, 2012).

Bilgi Korsanlığı

İnternet üzerinde yayınlanan fikrî hakların hırsızlığı sıkça karşılaşılan bir bilişim suçudur. İnternetin keşfinden bu yana, korsan programlar satın alınmakta, takas edilmekte ya da yayılmaktadır. Ayrıca aynı durumdan filmler ve müzikler de payını almaktadır. Yayılan fikrî hak ister bir program olsun ya da ister film ya da müzik, bunları internette yayan failin hiçbiri üzerinde yasal bir hakkı yoktur. Bu kişi, iyi niyetle bu tarz bir paylaşımı arkadaşları için yapsa dahi yasal olarak suç işlemektedir. Bu gibi davalar genellikle yayılan bilginin kaldırılmasını ve yayan faile para cezası kesilmesi ile sonuçlanmaktadır (Easttom, 2011).

Dünya çapında film ve müzik korsan yayıncılığı hak sahiplerine yılda yaklaşık bir milyar dolara yaklaşan maddi kayıplar yaşatmaktaktadır. Türkiye dahil olmak üzere birçok ülkede bunun önüne geçebilmek için yeterli yasaların olmaması, gün geçtikçe internetin bu yönde kullanımının artması ve bunun uluslararası düzeyde yapılıyor olması telif hakkı sahiplerine büyük darbe indirmektedir. Bilgi korsanlığı yazılım açısından ele alındığında yazılım şirketlerinin yıllık satışlarının her yıl ciddi miktarda düştüğü görülmektedir. Artık neredeyse tüm bilgisayar kullanıcıları satın almadan bir programı bedava indirerek kullanmaktadır. Kullanıcılar ister bilerek, ister bilmeyerek bedava bir programı indirip kullanıyor olmaları bir bilişim suçudur ve yasal yaptırımları vardır (US President's Council on Integrity and Efficiency Prevention Cmtte, ve United States of America, 1986).

Atılan Bilginin Çalınması Yoluyla İşlenen Suçlar

Bireyler ve şirketler farkında olmadan ellerindeki kendilerine ya da çalışanlarına ait bilgilerin bulunduğu basılı ya da CD vb. içinde bulunan kaynakları ellerinden çıkarırlar. Bu da kimlik hırsızlarına davetiye çıkarabilir. Bu tarz bilgilerin bulunduğu kaynaklar tekrar okunamayacak ya da kullanılamayacak bir şekilde çöpe atılmadığı sürece her zaman tehlike oluşturabilecek potansiyelleri vardır. Örneğin, 2004 yılında Dallas'ta Amerikan ordusundaki personele ait bilgilerin bulunduğu

kağıtlar bir çöplükte bir gazeteci tarafından bulunmuştur. Niyeti kötü olan bir kimse tarafından bulunduğunda kimlikleri ele geçirilen kişiler bu kişi tarafından bir çok mağduriyete uğratılabilirlerdi (Easttom, 2011).

Casus Yazılımlar

Casus yazılımların tek amacı hedeflenen bilgisayardaki bilgileri ele geçirmektir. Casus yazılımlar, bilgisayar sahibinin bilgisi dışında, hedef bilgisayara kurulur. Bu yazılımlar, bilgisayarda kullanılan herhangi bir kullanıcı adı ya da şifreyi ele geçirebildiği gibi, klavye üzerinde yazılan bütün bilgileri kaydederek, failin mail adresine yollar. Daha gelişmiş casus yazılımlar ise klavye etkinliklerinin dışında, bilgisayar masaüstünün belli aralıklarla görüntülerini fotoğraf gibi çeker ve hatta bazıları video olarak kaydeder. Böylede kurbanın yaptığı her hareket fail tarafından izlenmiş olur (Easttom, 2011).

Birçok internet kullanıcısı casus yazılımları bilmemektedir. Dolayısıyla casus yazılım mağduru bir çok kullanıcı vardır. Casus yazılımlar, kullanıcının her hareketini bir başkasına iletmekle kalmaz, aynı zamanda kullanıcının bilgisayarını da olumsuz yönde etkiler. Bu yazılımlar, bilgisayar performansını yavaşlatır, programların çalışmasına engel olur, sistemi çökertebilir ve bu şekilde bilgisayara zarar verebilir. Bu yazılımlar, hedef bilgisayara bir kişi tarafından direkt kurulabileceği gibi, bazen de hedef bilgisayar kullanıcısının internetten indirdiği bir programın içinde gelip, hedef bilgisayara yerleşebilir. Casus yazılımlarla ele geçirilen bilgilerle failler kimlik hırsızlığından, dolandırıcılığa her türlü suçu işleyebilmektedirler (Marcum ve Higgins, 2019).

Terörizm, sivil halkı korkutmak ya da küçük düşürmek amacı taşıyan herhangi bir resmi tanınırlığı olmayan, asilerden oluşan grupların politik mesaj verme kaygısıyla şiddet eylemleri sergilemesidir. Genellikle sivil vatandaşlar hedef alınsa da askeri kurumlar da bu tip saldırılara maruz kalmaktadır.63 Teknolojinin gelişmesiyle terör saldırılarının şekli de değişmiş ve teknolojiyi kullanan saldırılar planlanmıştır. Askerî, hükümet ve özel kuruluşların gitgide internete odaklı servislere daha çok bağımlı olmaları terör saldırılarını sanal ortama taşımıştır. Operasyondan lojistik birimlerine kadar askerîyenin tüm birimleri internetle yönetilmektedir. Aynı şekilde devlet kurumları ulusal güvenlik bilgilerini ve çok önemli kişisel kayıtları bilgisayarlarda saklamaktadır. Özel kurumlar da ağlar aracılığıyla bilgi alışverişi

yapmakta ve para transferleri gerçekleştirmektedir. Ağlara olan bu bağımlılık, ulusa tehdit oluşturan terörist grupların hedefi haline gelmiştir. Bilgisayar ve bilgisayar ağlarına yapılan ve amacı bir ulusun işleyişine zarar vermek olan planlı saldırılar, siber terörizmin oluşturduğu siber savaşlara neden olmaktadır (Potterfield, 2011)
İnternetin sağladığı hizmetlerin nasıl kötüye kullanılacağı kamuya açık bir şekilde internette yer almasından dolayı teröristlerin bu bilgiyi kullanmaları kaçınılmazdır. Teröristlerin internet tabanlı saldırılar düzenlemelerinin başlıca nedenleri şu şekilde sıralanabilir:

i. Saldırılar internette olduğu sürece dünyanın her yerinden herhangi bir zamanda gerçekleştirilebilir.
ii. Gerçek zamanlı saldırılara karşılık sanal saldırılar daha hızlıdır. Terörist kısa bir süre içinde hedef bilgisayara ulaşıp, bağlantısını aksatabilir, bilgisayarı işlevsiz kılabilir, bilgileri çalabilir.
iii. Teröristin izinin bulunması genellikle çok zordur. Çünkü bu tarz saldırılar ya bilinmeyen bir servis sağlayıcı üzerinden yapılmaktadır ya da çok iyi kamufle edilir.
iv. İnternet kullanımı ucuzdur. Çok hızlı olmayan bir bağlantı hızı bile terörist saldırıları için yeterlidir. İnternete erişimin bedeli az olsa da, internet vasıtasıyla yapılan terör saldırılarının bedeli büyük olmaktadır (The Cybercrime and The European Union, 2019).

Şüphesiz, sanal terörizm büyük zararlar vermek ve sivil vatandaşları mağdur etmek açısından teröristlerin elinde büyük bir silahtır. Yapılan bir araştırmada ABD hükümeti bilgisayarlarında 2008 yılı itibariyle, 18,050 adet güvenlik açığı olduğu tespit edilmiştir. Buna istinaden 2009 yılında Beyaz Saray'ın internet sayfasının da aralarında bulunduğu on dört hükümete bağlı internet sayfası saldırıya uğramıştır (Ching, 2010).

Sanal terörizm dahilinde olan saldırılar üç başlıkta ele alınabilir:

i. *Büyük Ölçekli Saldırılar*

Bu gibi saldırılarda bilgisayara gönderilen casus yazılımlar, bilgisayarın kontrolünü teröriste geçirir. Teröristler bu durumda, o bilgisayarın yönetimini 3.

Kişilere satarak maddi kazanç elde edebileceği gibi, kendi eylemleri için o bilgisayarın sistemini bozabilirler.

ii. *Hack Amaçlı Saldırılar*

Bu saldırılarda amaç bilgi çalmaktır. Genel olarak teröristler hükümetlerin elindeki gizli bilgileri (askerî bilgiler, finansal kayıtlar vb.) edinmek amacıyla bu yolu seçerler.

iii. *Fiziksel Hasar Veren Saldırılar*

Genellikle bir sisteme saldırıldığında o sistem zarar görür. Ancak bazı durumlarda, o sistemin düzgün çalışmasını sağladığı diğer sistemler de bu saldırıdan zarar görüp maddi ve fiziksel boyutta hasar alabilir. Örneğin, elektrik dağılımını kontrol eden bir sisteme saldırı gerçekleşmesi ve bunun sonucunda elektrik santralinin bozulması (The Cybercrime and The European Union, 2019).

Teröristler sanal ortamda modern toplum için önemli olan ve internet ya da başka bir iletişim ağına bağlı olan herhangi bir sisteme saldırıda bulunabilir (Sieber, 1986). Bu sebeple, yetkililer bilgisayar güvenlik önlemlerini geliştirme yoluna gitmeli ve güvenlik açıklarını kapatmak için yeni programlar üretmelidir.

Sanal Flört ve Evlilik Dolandırıcılığı

Sanal ortamda kullanıcılara flört ve evlilik için partner bulmayı vaad eden internet siteleri günümüzde büyük bir sektördür. Dünya üzerinde birçok insan bu gibi sitelere üye olup kendilerine uygun eş adayı bulmaya çalışmaktadır. İyi niyetli kullanıcıların abone olduğu gibi kötü niyetli kullanıcılar da bu sayfalara abone olmaktadır. Sanal flört ve evlilik dolandırıcılığı, failin mevzubahis sitelere üye olup eş arıyor gibi görünüp, aslında tanışacağı kişiden maddi çıkar sağlama amacı gütmesiyle meydana gelmektedir. Faillerin bu siteler aracılığıyla tanıştıkları kurbandan para isterken kullandıkları dört temel bahane vardır:

i. Tanıştıkları kişiye onunla gerçek hayatta tanışmak isterler ancak seyahat paralarının olmadığını söylerler.
ii. Maddi problemleri olduğunu söyleyerek yardım isterler.
iii. Hastalık ya da kaza geçirdiklerini söyleyerek yardım isterler.

iv. Vize almak için paraya ihtiyaçları olduğunu söyleyerek yardım isterler (Millhorn, 2007).

Failler, genellikle bu sitelerde kendilerine ait olmayan ancak kusursuz görünen fotoğrafları kendileriymiş gibi yayınlarlar. Bu şekilde birçok kullanıcının ilgisini çekebilir, aynı anda birden fazla kişiyi kandırabilirler. Kendileriyle ilgili diğer bilgileri de (eğitim, meslek, yabancı dil bilgisi, maaş, mal varlığı vb.) olduğundan fazla göstererek güvenilir bir profil çizip, birçok kullanıcıyı tuzaklarına düşürme potansiyeline sahiptirler (Conway, 2010).

Sanal Fuhuş

Fuhuş, bir kişinin başka bir kişiye kendini para karşılığında cinsel ilişki amaçlı belli bir süreliğine satması olarak tanımlanabilir. Birçok ülkede illegal olarak geçmektedir. İnternet üzerinde fuhuş çok yeni bir kavramdır. Bu amaçla açılmış olan internet sayfaları açık bir şekilde para karşılığında seks hizmeti sunulduğunu yazmazlar. Bunun yerine, eskort ya da tam servis gibi kelimeler kullanırlar. Yaşları 18 ile 42 arasında olan fahişelik yapan kadınlar, internet üzerinden anlaşmalar yapmayı, sokaklarda olmaktan daha kolay, güvenli ve kârlı bir iş olarak tanımlamaktadır. Bu kadınlar bu amaçlarla açılmış internet sayfalarına kendileri ile bilgileri (vücut ölçüleri, özellikleri, yaşları, telefon numaraları, yaptıkları cinsel aktiviteleri) ve fiyatlarını yazarak müşteri beklemektedir. Yalnızca bu amaçlı açılmış internet sayfalarını değil, öğrencilerin ev arkadaşı aradıkları internet sayfaları ya da ikinci el araba satan internet sayfalarını da bu iş için kullanıp, müşteri elde etmeye çalışmaktadırlar (Milhorn, 2007).

Yapılan araştırmalar bu işi yapan kadınların genellikle tek başlarına çalıştığını ortaya çıkarmıştır. Ancak bunun yanısıra sanal genel evler de vardır. İnternette fenomen olan üyelik gerektiren “Second Life” adlı sanal gerçek zamanlı oyunda da (abone olmak için yasal yaş 18’dir, ancak bunun kontrolü sağlıklı bir şekilde yapılamamaktadır.) sanal fuhuş yerini almıştır. Sanal fuhuş önüne geçilmesi zor olan bilişim suçlarındandır (Ludlow ve Wallace, 2007).

Çocuk Pornografisi

Çocuk pornografisi, çocuk bedeninin cinsel amaç güden bir şekilde fotoğraflanması ya da videoya kaydedilmesi ve bu görüntülerin üretilip, dağıtılması olarak tanımlanmaktadır. Bilişim suçu olarak çocuk pornografisi, bu görsellerin internet üzerinde üretilmesi ve dağıtımıyla gerçekleşmesidir. Ne yazık ki bilgisayar ve internet teknolojisi çocuk pornocular için büyük önem teşkil etmektedir. Bunun en belirgin örneği, çocuk istismarının canlı olarak yayınlandığı internet sohbet odalarıdır. Amerika'da böyle görüntülere yer veren bir sohbet odası tespit edilerek, görüntüler arasındaki çocukların en küçüğünün bir yaşında olması Amerikan basınında uzun süre yer almıştır (Milhorn, 2007).

İnternet anonim bir araç olduğu için çocuk pornografisi materyallerine sanal ortamda kolaylıkla ulaşmak mümkündür. Bu görselleri üretenler, kendileri gibi diğer üreticilerle o video ve fotoğrafları paylaşmayıp, üretici olmayan çocuk pornografisi bağımlılarıyla da bu görselleri bedava paylaşmaktadırlar (Quayle ve Taylor, 2003).

Sanal Haraç

Sanal haraç, failin karşısındaki insanı internet üzerinden malına ya da canına zarar vereceğini söyleyerek tehdit etmesi sonucu, o kişiden para, eşya ya da seks talep etmesi, bir nevi haraç istemesi olarak tanımlanmaktadır. Sanal haraççılar en çok para talep etse de son zamanlarda cinsel yönden haraç talep etmeye de başlamışlardır. Özellikle genç kızların, fotoğraflarını facebook adreslerinden ele geçirip resim düzenleme programlarıyla başka çıplak vücut fotoğraflarına kurbanların kafalarını montajlayarak, o fotoğrafları onları internette yayınlamakla tehdit eden haraççılar, kızların kendileriyle telefon ya da internet üzerinden seks yapmalarını talep etmektedirler (Milhorn, 2007).

Sanal haraççıların tehditleri genellikle mağdurla ilgili herhangi bir gizli bilginin ele geçirilmesiyle başlar. Bu ele geçirme, bilgisayar korsanlığı yoluyla olabileceği gibi günlük yaşantı esnasında da mağdur hiç farketmeden gerçekleşebilir (Tipton ve Krause, 2007).

Bilişim Suçlarının Tarihçesi

Bilgisayar sistemlerinin ve bilişim teknolojilerinin yoğun bir biçimde kullanılmasıyla beraber bilişim suçları gibi bir suç türü ortaya çıkmıştır. İnternetin tüm ülkelerde yaygınlaşması ile beraber bilişim suçlarında belirgin sayı artışı görülmüştür. Bilgisayar teknolojisi kolay takip edilmeyen, gayet hızlı ve insan hayatında kolaylık sağlayan, özel ve kamu kurumlarında yeni bir çağ açan, ticaret ve iş hacminde genişlemeler sağlayarak önemli farklılıklar yaratmıştır. Böylece kötü amaçlı internet kullanımları ortaya çıkmış, teknolojinin sağlamış olduğu kolaylığı kullanarak haksız kazanç elde etmek isteyen bireylerden ötürü bu yeni alana suç kavramı girmiş oldu. Suç unsurunun gelişen teknolojinin içinde barınıyor olması, bilgisayar sistemleri ve teknolojiyi kullanan kimseler için güvensiz bir ortam olarak anılmaktadır (Sönmez, 2018).

Dünyada ilk işlenen bilişim suçu, 1966 yılı itibarıyle 23 yaşında olan bir bilgisayar programcısı ve banka çalışanı olan Minneapolis, başkasının mevduat hesabında bulunan para miktarı değerinde değişiklik yapmak suretiyle işlendiği söylenmektedir (Parker, 1968). Bilişim suçlarındaki ilk hukuki düzenlemelerle ilgili olarak yaşanan gelişmeler aşağıda verilen paragrafta belirtilmiştir (Kruse II ve Heiser, 2002; Shrivastava, Sharma ve Dwivedi, 2012; Gökçearslan, 2016).

Dijital hukuk ve onun tarihi gelişimininden bahsetmek gerekirse 1978 yılındaki Florida eyaletinde bulunan bilgisayar sistemlerinde bulunan verilerin yetkisiz bir şekilde değiştirilip silinmiş olması, 1980 yıllarında bilgisayar suçlarının çözümü eski kanunlarla yapılmakta ve özel herhangi bir kanun bulunmamaktaydı. 1983 yılında bilgisayar suçlarıyla ilgili olarak kanun çerçevesinde düzenleme yapmış olan ilk ülkelerden biri Kanada'dır. 1984 yılında Amerika'da bilgisayar ile alakalı dolandırıcılık ve kötüye kullanma açısından kanuni düzenlemeler yapılmıştır. 1992 yılında Collier ve Spaul "Bilgisayar suçu ile ilgili bir hukuki yöntem" isminde bir araştırma da yapmıştır. 2002 yılında dijital veriler ile alakalı olarak bilimsel çalışma grubu olarak bilinen SWGDE "Bilgisayar hukuku ile ilgili en iyi pratikler" isminde bir araştırmaya imza atmıştır. 2005 yılında ise yapılmış test ve kalibrasyon laboratuvarının ihtiyacı için ISO standartı geliştirilmiştir. 2005 yılından günümüz itibarı ile bilgisayar suçları ve türleri farklı boyutlar açısından tartışma konusu edilmiştir.

Bilişim suçları dahilinde mağdurlara gerçekten ciddi anlamda zararlar veren türlerden örnek vermek gerekirse, daha sonraları kendinden çok sözettirip tüm internet dünyasında tanınmış bir kimse olan "Condor" kod adlı Kevin Mitnick isimli genç kişi, 1981'de Pasifik Bell anahtarlama istasyonunun verilerini çalmakla suçlandığı belirtilmektedir. Mitnick 1982 yılında, Kuzey Amerika Hava Savunma Komutanlığı bilgisayarlarına girmiştir. Bunun yanında, Kaliforniya'daki tüm telefon anahtarlama merkezlerine erişim sağlayarak, Manhattan'da bulunan üç tane merkezi telefon şirketinin bir anlık kontrolünü ele geçirdiği literatürde yer almaktadır. 1988'de 25 yaşında olan Mitnick, MCI ve Digital Equipment şirketlerinde çalışan güvenlik çalışanlarına ait elektronik postaları ele geçirdiği de bilinmektedir. Bunun üzerine Digital Equipmant, Mitnick'i bilgisayar işlemlerinde yaptığı değişiklikler nedeniyle 4 milyon Amerikan Doları zarar vermiş oldu ve 1 milyon Amerikan Dolar değerinde bir yazılım çaldığı için suçlanmış ve yargılanarak bir yıl hapse mahkûm edildi. Yine 1993 yılında Mitnick, California Motorlu Araçlar Departmanı'nın veri tabanlarından sürücü belgelerini çalmakla suçlanmıştır. 1994 yılının birinci günü ise Mitnick, San Diego Supercomputer Center'deki Tsutomu Shimomura'ya ait sisteme giriş sağlamıştır. Bu olaydan sonra Shimomura, Mitnick'in tutuklanmış olduğu 1995 yılına gelene kadar internet üzerinden Mitnick'i takip etmiştir. Sonuç olarak Mitnick, yargılanarak suçlu bulunmuş, yaklaşık 5 yıl hüküm giydikten sonra, 21 Ocak 2000 tarihinde federal cezaevinden çıkmıştır (Özdilek, 2002; Littman, 1996).

Kuzey Kıbrıs Türk Cumhuriyetinde, Türkiye ve Dünyada Bilişim Suçları ve Hukuki Esaslar

Ülkeler için bilgi toplumuna geçiş önemli olmakla beraber bu süreç ile bilişim teknolojilerinin kullanılmasıyla yaşamın vazgeçilmez bir parçası haline gelmiştir. Bu süreç içerisinde, topluluklarda bilişim teknolojileri daha çok kullanılmakta ve enegelenemz bir şekilde daha fazla bilişim suçuyla karşı karşıya kalınmaktadır. KKTC'de yaşanan teknolojik gelişmeler ve bilgi toplumu olma yolunda yaşanan gelişmeler ile diğer ülkeler gibi benzer bir süreçten geçtiği söylenebilir. Bundan dolayı, siber suçlar ile mücadele etmek amacıyla Bilişim Teknolojileri ve Haberleşme Kurumu'nca (BTHK) 2018'de "Bilişim Suçları Yasa Tasarısı" hazırlanma süreci içine girilmiştir. Bu yasayla, bilişim sistemlerindeki ağların ve

verilerin gizliliği, doğruluğu ve ulaşılabilirliği, zarar verici faaliyetlerin durduurlması hedeflenmiştir. Ağ ve verilerin kötü amaçlı kullanımı ve bilişim suçlarının engellenmesi, içerik sağlayıcı, yer sağlayıcı, erişim sağlayıcı ve toplu kullanım sağlayıcıların yükümlülük ve sorumluluklarının düzenlenmesi de bu yasayla kontrol altına alınmya çalışılmıştır. Tüm bu faaliyetler kapsamında suç oluşturan eylemler ve cezai niteliklerinin belirlenmesi, söz konusu suçlar ile etkili biçimde mücadele edilmesine ve suçların takip edilmesine ilişkin esas ve usuller bu yasa tasarısı ile düzenlenmiştir (BTHK, 2019).

KKTC'de, henüz daha bir bilişim yasası yürürülükte değildir. Taslak olarak hazırlanan Bilişim Yasa Tasarısı, geçen yıllar süresinde duyulmuş olan ihtiyaca ve sürdürülmüş olan araştırmalar da gözetildiğinde yasalaştırılmadan bekletilmektedir. Kuzey Kıbrıs'ta, yürürlükte olan herhangi bir bilişim yasasının bulunmaması; iletişim çağında dijital ortamların ve sosyal medyanın yayagın olarak kullanıldığı bir dönemde, önemli problemlere yol açtığı belirtilmektedir. Bilişim ortamında işlenmiş olan suçlar, "kanunsuz suç ve ceza olmaz" easasıyla cezasız kalabilmekte; suçlulara cezai yaptırımların uygulanmasında zorluklar ile karşılaşılmaktadır (Dolunay ve Sağsan, 2019).

Bilişim çevreleri ve ortamlarında yaşanmış olan bu gelişmelere yönelik kanunkoyucular, 1990 yılının başında, hem uygulama alanında kendini hissettiren ihtiyaçları karşılamak amacıyla hem de Türkiye'nin üye olduğu farklı uluslararası kuruluşların tavsiye kararlarına uymak amacı ile bazı düzenlemeler yapmışlardır. Bu anlamda bilişim suçları kapsamında ilk düzenleme TCK'ya 1991 yılı itibarıyle girmiş ve 3756 sayılı Kanun iile 765 sayılı TCK'nın ikinci kitabına birkaç bilişim suçunu öngören "Bilişim Alanında Suçlar" başlıklı 11. bap eklenmiştir. Bilişim suçları dahilinde, bazı ülkelerde ayrı bir kanun düzenlemesi veya mevcut ceza kanunlarının içerisine bu türdeki suçlara yönelik yeni bölümlerin eklenmesi sağlanmıştır. Fakat, bunun tersine ayrı bölümlerde ve/veya yeni kanun düzenleme ihtiyacı olmaksızın mevcut kanunların yanlarına eklemeler yaparak var olan ihtiyacın karşılanmasına çalışan bazı ülkeler de vardır. Bunun gibi yasa tasarılarına ayrı ayrı düzenleme yapmış olan ülkelerden bazıları, Şili, Danimarka, Fransa, Yunanistan, İngiltere, İtalya, Japonya, Kanada, Avusturya, İsveç ve ABD olarak gösterilebilmektedir (Akbulut, 2000).

ABD'de bilişim suçlarından zanlıların elde ettiği kazanç yıllık 3 milyar dolar olarak kayıtlara geçmiştir. Stanford Araştırma Enstitüsü'nün verilerine göre, ABD'deki bilgisayar dolandırıcılığına uğrayan bir şirket 425 bin dolar, bir banka 132 bin dolar ve kamuoyu tarafından bilinen bir kişi 220 bin dolar zarara uğramıştır. FBI'ın tahminleri yalnızca on binde bir kişinin bilişim suçları bağlamında yakalanıp hapis cezası aldığı yönündedir. (Bu rakam 1984 yılında 22 kişide 1 kişidir.) ABD bilişim suçları yıl bazında %500 artmaktadır ve bu oran gün geçtikçe kendini aşmaktadır (Clutterbuck, 1992).

Amerika'da bilişim suçlarının geçmişi 1960'lı yıllara kadar uzanmaktadır. İnternetin ve bilgisayarın anavatanı olan Amerika Birleşik Devletleri'nde gerek federal, gerekse eyalet düzeyinde bilişim suçları konusunda bir çok yasa çıkartılmıştır. ABD'de bugün için farklı bilişim suçu biçimlerini düzenleyen bazı federal yasalar kabul edildiği bilimektedir. Ancak bunlar içinde en önemli olarak Federal Temel Yasa'nın 18. bölümü 1030. Madde gelmektedir. Bu yasa genel olarak, korunmakta olan bir bilgisayar sistemine yetkisiz ve izinsiz bir şekilde erişmeyi yasaklayan özelliktedir. Yasa metninde belirtildiği gibi, kamu ve özel sektörün sahip olduğu tüm bilgisayar sistemlerinin yanında, bireysel bir bilgisayar da bu korumadan tam anlamda yararlanabilmektedir. Amerika'da bilişim suçları ve siber terörizmin sonlanması için uğraşan birçok kurum ve kuruluşun sahip olduğu özel birim ve bölümler vardır. Bu birimlerden bazıları ise; FBI "National Infrastructure Protection Center", "Information Technology Association of America", "Trap and Trace Center Authority" ile "Carnegie Mellon's Emergency Response Team" (CERT) ve bazı üniversitelerin bünyelerinde kurulmuş olan bazı bölümler bunlar için önem arz edenlerden bazılarıdır (Emniyet Genel Müdürlüğü, 1999).

Yeni teknolojilerin kullanılmasıyla işlenen suçların Fransa iççin maliyeti 1998 yılı için 14 milyar Frang seviyesinde olmakla beraber, 1999 yılın için ise bu konularda polis ve ve güvenlik ile ilgilenen kurumlara 3815 olay bildirilmiştir. Bu olayların 2450 tanesi internet ve bilişim sistemlerinin kullanılmasıyla işlenen suçlar olduğu görülmüştür. Diğer kalan 1336 tanesiyse telekomünikasyon sistemleri ile alakalı olanlardır. Fransız Danıştay'ı tarafından 1998'de yayınlanan internet konsu ile ilgili raporda, var olan mevzuat, bilgisayar üzerinden işlenen suçlar için de olacak şekilde kapsamı genişletilerek yeterli olması beklenmiştir. 1999 yılının 17 Mart tarihinde şifreleme sistemi ile ilgili mevzuat incelenerek değişiklikler yapıldı.

Bununla birlikte 2000 yılının Şubat ayında elektronik imzaların hukuki bir değerinin olmasına yönelik bir kanunun yasalaşması sağlanmıştır (Emniyet Genel Müdürlüğü, 1999).

"Bilgisayarın Kötüye Kullanılması Kanunu" (Computer Misuse Act) olarak bilinen kanun ile İngiltere'de bilişim suçları 29.08.1990'da yürürlüğe girmek suretiyle belli bir düzenleme altına girmiştir. Yapılmış olan bu kanun 3 bölümden ve 18 kısım olarak planlanmıştır. Böylece bu kanunla yetkisiz bir şekilde bilgisayar sistemlerine erşim sağlanmasının ve/veya değişiklik yapılmasıyla veya benzeri müdahale yapılarak bunun önlenmesi de amaçlanmıştır (Yazıcıoğlu, 1997). Bu suç türlerinden birincisi, yetkisiz bir kişinin bilişim ile ilgili cihazlara veri erişimi sağlaması ve programlara girmesi, bunlardan ikinciyse, diğer bir başka suçun işlenmesine olanak sağlamak ve bu durumu kolaylaştırarak yetkisiz bir şekilde bilişim cihazlarına girilmesi, son olarak bunlardan üçüncüsü, bilgisayar sistemleri, veriler ve programların yetkisiz kimseler tarafından yasa dışı bir şekilde değiştirilmesidir (Akıncı, Alıç ve Er (2004). 1964 yılında yapılan "Müstehcen Yayınlar Kanunu" ve 1984 yılında Telekomünikasyon Kanunu'nda yapılan değişiklikler ile sanal dünyada pornografi ile birlikte çocuk pornografisi konularında farklı düzenlemeler yapılmıştır (Dülger, 2004b). 1978 yılında Çocukların Korunması Kanunu'nda yer almakta olan "fotoğraf" tanımı, 1994 yılında yapılan Ceza Adaleti ve Kamu Düzeni Kanunu çerçevesinde internet üzerindeki resimlerin de kapsanacak biçimde değiştirilerek, internette bulunan çocuk pornosu ile ilgili resimlerin montajlanmasıyla yapılmış şekillerinin bulundurulması suç olarak kabul edilmektedir (Mahmutoğlu, 2002). İtalya'da Bilişim suçları konusunda kanunlarda yapılan düzenlemeler 23 Aralık 1993 yılında 547 sayılı kanunla yapılmış oldu.

Bilişim Etiği

Bilişim teknolojilerindeki gelişmeler birçok olumlu özellikle insanların hayatında yer etse de bilişim teknolojilerinin en yaygın kullanıldığı toplumlarda "bilgisayar etiği", "bilişim etiği", "teknolojide etik" gibi kavramlar gündeme gelmiştir. Teknolojinin birey ve toplum üzerine etkilerini kapsayan bu kavramlar bir sorun olarak toplum yaşamını etkileyen bir seviyeye ulaşmıştır. Bu sorunlarla birlikte bilişim etiği kavramı tartışmalarla gündemde kalmaya devam etmektedir (Dedeoğlu,

2006). Son zamanlarda İnternet araçlarının yaygın kullanımı "İnternet etiği" kavramını da gündeme getirmiştir.

Etik ve ahlak kimi zaman birbirinin yerine kullanılsa da tam anlamıyla aynı anlamı taşımamaktadır. Etik "etos" kelimesinden türemiştir. Ahlak kelimesinin kökü arapça "hulk" ya da Latince "mos" tur. İki dilde de bu kavram, alışkanlık, töre, karakter, huy, mizaç anlamına gelmektedir (Gündoğan, 2010).

Bilişim etiği, bilgisayar ve İnternet etiğini kapsayan bilişim alanında hizmet sunan ve hizmet alanlarının davranışlarıyla ilgili etiğe yönelik bir alt alandır. Bilişim etiği, bilgisayar ve İnternet kullanımı, bilişim sistemi ve ağ yönetimi, hukuki ve yönetsel yönde etik kuralları kapsamaktadır (Tanrıkulu ve ark., 2007). Bilişim etiği, bilişim teknolojileri kullanıcılarının ve bu kullanıma aracılık yapan kuruluşların bu teknolojileri kullanırken uyması gereken kurallara yönelik normlar olarak tanımlanmaktadır. Bu normların belirlenmesinin nedeni, bilişim teknolojilerini kullanan paydaşların ortamı daha güvenli kullanabilmeleri ve çıkacak sorunların en aza indirilmesidir. Toplumlar birbirinden farklı etik davranışlar belirlese de uluslararası boyutta ortak paydada buluşulması gerekmektedir. İnternet'in bir merkezi olmadığı, ortamda herkesin eşit olduğu düşünülürse ortak kullanımdaki kullanıcıların etik davranışları benimsemesi gerekliliği tartışılmaz bir konudur. Bu noktada paydaşlardan biri olan İnternet servis sağlayıcılarının da sorumlulukları vardır (Gökçearslan, 2016).

Hızla gelişmekte olan bilgisyar ve iletişim teknolojileriyle beraber bilişim etiği de gündeme çok sık gelmiştir (Örs, 2010). Bilişimi hedef alan bilişim etiği bu konudaki teknolojilerin etik kullanımını tanımlayarak norm ve kodlardan içerisinde barındırmaktadır. Kullanılan bu norm ve kodlar sayesinde kişiler en az zarar görerek ve en çok yarar sağlayarak bireylerin güvenliğini sağlamaktadır (Sevindik, 2011). Bilişim etiği sayesinde bireyler evrensel kişilere özgü değerler sayesinde bilinenden çok fazla problemler ve tehlikelerle yüzleşebilmektedir. Hukuksal açıdan doğruyla yanlışı birbirinden ayırcak şekilde anlatmaya çalışan bu durumların hangisinin doğru veya hangisinin yanlış olduğu konusundaki kurallar maalesef belirlenememektedir (Uysal, 2006). Bundan dolayı; bilişim etiğiyle ilgili olarak telif hakkı ihlali, hackerlik, lisanssız yazılım kullanımı, izinsiz dosyaların kopyalanması veya paylaşılması, mahremiyet içieren konular da dahil olmak üzere fazlaca

tartışılmaktadır (Johnson, 2000). Bu nedenlerden ötürü bireylerin genellikle etik davranışlarda bulunma isteğiyle hareket etmesi son derece önemlidir (Uysal, 2006).

Siber Zorbalık ve Siber Mağduriyet

Diğer kimseleri incitiecek derecede rahatsız ederek kötü davranışlar içinde olmak tarih boyunca tüm ülkelerde rastlanılan sorun olmuştur. Başkalarına saldırmak olarak da isimlendirilen bu türdeki davranış biçimleri günümüz dünyasında çok kez görülmektedir. Saldırgan davranış biçimlerinden biri olarak zorbalık söylenebilir (Gökler, 2009).

Zorbalık terimi (bullying) ilk başlarda İngiltere'de 1800 ve bu yılı içeren günlerde sonucu ölüm olan bir olayın ardından işin zorbalık olduğu söylense de, o günlerde zorbalık gibi kötü bir davranışın normal davranılar olarak benimsenmesinden dolayı bu sorun üzerinde pek de durulmamıştır (Allanson, Lester, ve Notar, 2015).

Saldırganlık gibi bir davranışın bir alt türlerinden olan zorbalık, diğer türleri de gözetildiğide, yapılan çalışmalarda farklı bir biçimde sınıflandırıldığ gözlemlenmiştir. Bu sınıflandırmalara bakıldığında ağırlıklı bir biçimde zorbalık davranışının doğrudan ve/veya dolaylı olarak yapılması konusu sürekli irdelenmektedir (Olweus, 1993; Slonje ve Smith, 2008; Gökler, 2009). Doğrudan hedefe yönelik yapılmış olan zorbalıklarda vurulması ve incitilmesi benzeri fiziksel tepkiler ile tehdit edilmesi, hakaret ve/veya alay edilmesi benzeri davranışları ve sözel tepkileri içermektedir. Dolaylı yönden yapılmış olan zorbalık türleri ise sosyal ilişkilerde reddetmek benzeri anlaşılması diğerine göre daha da güç olan davranışların tümüdür (Slonje ve Smith, 2008).

Duygusal taciz ya da yıldırma internet üzerinden de yapılabilmektedir. Bu durum manevi şiddet, zorbalık, siber zorbalık, akran zorbalığı ya da mobbing olarak adlandırılabilir ve internet üzerinden yapıldığında bilişim suçu olarak kabul edilebilir. Literatürdeki tanımla iş yeri terörü olarak bilinen mobbing iş yeri ile sınırlandırmak da günümüz şartlarında yetersiz kalmaktadır. "Mobbing bir ve/veya çok fazla birey tarafından, bir veya birden fazla bireye, düzenli bir şekilde, kasti bir şekilde düşmanca ve ahlağa uymayan bir yaklaşım tipiyle, düzenli bir şekilde, çok değişik nedenleri olabilen, bireyi pasifize etmek amcıyla, bireyin özgüvenine

uygulanan psikolojik ve daha ötesi fiziksel saldırgan davranışlar olarak belirtilmektedi". Diğer bir deyişle, siber zorbalık (cyberbullying) elektronik-temelli iletişim araçları kullanarak bir birey veya grup tarafından kendi kendinin güvenini sağlayamayan kurbana yönelik saldırgan, bilrek yapılan ve süreklilik arz edecek şekilde kullanımı olarak tanımlanmaktadır (Smith, Mandavi, Carvalho, Fisher, Russel ve Tippett, 2008).

Son zamanlarda teknolojiyle yaşanmakta olan gelişmelerle birlikte zorbalık ile ilgili türlere bir yenisi daha eklenmiş oldu. Siber zorbalık olarak bilinen son çıkan bu tür, gelişen teknolojiyle üretilen araçların, özellikle de akıllı telefon ve bilgisayar sistemlerinin kullanılmasıyla ortaya çıktığı ifade edilmektedir (Ayas, 2014; Slonje ve Smith, 2008). Teknolojinin de gelişmemesiyle birlikte literatürde yavaş yavaş yer almaya başlayan siber zorbalık terimi ilk olarak Kanadalı araştırmacı Bill Belsey (2004) tarafından kullanılmıştır (Dikmen ve Tuncer, 2017). Zorbalıkta bir yeni tür olarak literatürde daha fazla 'siber zorbalık' (cyberbullying) olarak ifade ediliyor olsa da diğer araştırmacılarca 'sanal zorbalık', 'elektronik zorbalık' ve 'internet zorbalığı' benzeri kavramların da kullanıldığını görmekteyiz (Yetim, 2015).

Siber zorbalık için değişik tanımlar varıdr. Patchin ve Hinduja (2008) siber zorbalığı, elektronik metinlerin kullanılmasıyla bilerek ve isteyerek tekrarlayacak şekilde yapılmış olan zarar veren davranışlar olarak karşımıza çıktığını ifade etmişlerdir. Li (2007) ise siber zorbalık için, 'internet ve iletişim teknolojilerinin (e-posta, anlık mesaajlaşma, kişlere ait web sitesi gibi) bir kiş veya grup tarafınca tekrarlayacak biçimde başkalarını aşağılama ve küçük düşürme amacı ile kullanımı' biçimde açıklamıştır. Bauman ve Newman (2013) tarafından yapılan siber zorbalık tanımı ise "iletişim araçlarının kullanımıyla bir başkasına sosyal statü açısından ve itibarına zarar verecek biçimde kasıtlı bir şekilde zarar vermek" biçiinde ifade edilmiştir. Willard (2007) siber zorbalık için "internet ve dijital teknolojilerin kullanılmasıyla diğer kişilere zararlı metin, resim veya video gibi bir tür sosyal saldırganlık yollarının gönderilmesi olarak belirtmiştir. Siber zorbalık için bir diğer tanım ise, bir kişi veya kişilerin iletişim araçlarını kullanarak kendi güvenliğini sağlamada güçlük çekmekte olan birine yönelik kötü bir aömaçla ve sıklıkla tekrar edecek şekilde kullanması olarak ifade edilmiştir (Calvete, Orue, Estévez, Villardón, ve Padilla, 2010). Belsey (2004) için siber zorbalık, diğer kişilere zarar verme

eğilimiyle kişi ve/veya grupların bilgi ve iletişim teknolojilerinin tekrar edecek bir biçimde kullanılması olarak belirtilmiştir.

Bilişim Suçları ve Çocuklar

Ahlakî boyutu ele aldığımızda gençler ve çocuklar tarafından çokça kullanılan anında mesajlaşma programları ve chat yazılımları incelenebilir. Bu gibi programlarda karşısındakini tanıma şansı elde edemeyen çocuk ya da gençler ahlakî sınırları ihlal edebilecek şekilde yönlendirilebilirler. Bu gibi programlar internette teşhirciliğin yayılmasını sağlamıştır. Karşı taraftan pornografik içerik sunulan çocuk ya da gençler birçok yönden olumsuz olarak etkilenmektedir. Yapılan bir çalışma bu gibi yazılımlar üzerinden pornografik içerikle tanışan genç ve çocukların, tanışmayanlara oranla daha erken cinsellikle tanıştıklarını göstermektedir. Evlilik dışı olarak gösterilen bu pornografik içerikler, gençlerin evliliğe bakış açısını değiştirmekte ve evlilik yaşantısını onların gözünde değersizleştirmektedir. Bu tarz pornografik içerikler yalnızca gencin ya da çocuğun konuştuğu karşı taraf tarafından sağlanmamaktadır. Bazı mesajlaşma ve chat yazılımları, ara yüzleri pornografik reklamlar içermektedir. Bu pornografik reklamlar zaman zaman şiddet içeren görseller de içermektedir. Bu tarz içerikler çocuk ve gençler de büyük travmalara yol açmakla birlikte yetişkinleri de negatif yönden etkilemektedir. Şiddet içeren bu görseller, yetişkin kadın ve erkekleri, kadın-erkek ilişkileri açısından duygusuzlaştırmaktadır. Bireyler fark etmeseler de, karşı cinse karşı bu görseller yüzünden sado-mazoşist ve vahşi duygular geliştirebilmektedir. Bu tarz psikolojik sorunlar, bireylerin özel hayatlarında ciddi sorunlara yol açabilir. Ayrıca bu görseller, bireylerde hayatlarının merkezine cinselliği koymaları gerektirdiği duygusu uyandırabilir (Thornburgh ve Lin, 2002).

Bilişim suçları kapsamında hakkında adli işlem başlatılan suçlu profilleri incelendiğinde, özellikle 18 yaş altında çocuk olarak tanımlanan ve hukuktaki tabiriyle suça sürüklenen çocukların da mevcut olduğu belirlenmiştir (Ereş, 2009). Suç davranışı, öğrenilen bir davranış olup, suçu işleyenlerin henüz çocuk olarak isimlendirilen yaşta olması, yetişkinlere nazaran daha savunmasız olmaları, suçların anlam ve önemini yeterince kavrayamamaları toplumdaki ana problemler arasındadır (Kahya, 2015). Uyuşturucu, cinsellik, şiddet, kumar vb. birçok unsur internette bulunmaktadır (Yalçın ve Gürbüz, 2015). Yetişkinler, suçları bildikleri için suçun

anlamını kavrayabiliyorken, çocukların için aynı durumu söylemek oldukça zordur. Çocuklar, suç ile ilgili çok bir şey bilmedikleri için hem mağduriyet yaşarlar, hem de kimi zaman suç işlenmesine sebebiyet vererek mağduriyet yaşanmasına sebep olurlar.

Büyük şehirlerde yaşayan geçler ve çocuklar farklı kültürden gelen guruplarla karşılaşmakta ve sosyal medya etkisi altına girmektedir. Anne babanın çoğunlukla çalışması nedeniyle çocuklar üzerinde denetimi yetersiz kalmaktadır. Bu durum da çocuklar aile içerisinde meydana gelebilecek çatışmalara maruz kalabilirler. Büyük metropollerde boş vakitlerini değerlendirmek isteyecekleri yerlerin, kırsal kesimlerde ise farklı faaliyetlerin yetersiz oluşu, çocuk ve gençleri yeni ve farklı arayışlara, en fazla olarak da İnternete ittiği görülmüştür. Sanal değil de gerçek dünyadaki gibi sanal ortamlarda çocuklar ve gençler için bazı riskler vardır. Çocuklar İnternette olduğu zaman en fazla tanımadıkları farklı bireylere güvenmekte, kendine ait bilgileri paylaşmak suretiyle akran istismarı ile karşılaşabilmekte, cinsel istismar ve çocuk pornografisi benzeri önemli risklerle karşılaşabilmektedirler (Alikaşifoğlu, 2012). ABD'de yapılmış olan bir diğer çalışmada küçük çocukların %75'i ebeveynleri ve/veya sahıslarına ait bilgileri herhangi bir şekilde endişe bile duymadan ve gönüllü bir biçimde tanımadıkları kişilere paylaşabilmekte ve kendilerine ait olan bu bilgiler için sanki de bir şey verileceğini sanarak kandırılmaktadırlar (Çevik, 2012).

Küçük yaştaki çocukların İnterneti yoğun bir şekilde kullandığı bir dönemde yaşamaktayız. İnternete herhangi bir şekilde erişim sağlayan çocuklar, İnterneti hayatlarının naçizane bir parçası veya vazgeçilmez bir öğe biçimde algılamaktadırlar (Ersoy ve Ersoy, 2008). Bundan 15 sene önce Prensky (2001), 1980'li yıllar ve sonrasında doğan, teknolojinin merkezinde büyümüş olan bu nesli dijital yerli olarak adlandırmıştır. Bu Dijital yerliler olarak adlandırılan nesil bile şimdi büyümüş ve birer yetişkin olmuşlardır. 2000'li yıllardan sonra doğan ve tamamen akıllı telefon ve olabildiğince mikro (mobil) teknolojiler ile büyümeye başlayan yeni jenerasyon ise kimi çalışmalarda Z Kuşağı olarak adlandırılmıştır (Çubukcu ve Bayzan, 2013). Bu konuda yapılan çalışmalarda net bir zaman söylemek mümkün olmamakla birlikte bazı çalışmalarda 90'lı yıllarda doğan jenerasyonu da Z kuşağına dâhil etmektedir (Geck, 2007).

Zaman algısı değişse de bu yenil nesil çocukları teknolojik yönden kısaca şöyle izah edebiliriz: Teknoloji onlar için ulaşılması gereken bir araç değil her daim yanlarında bulunması gereken bir ihtiyaçtır. Özellikle İnternet teknolojilerinin getirmiş olduğu fırsatlardan dolayı bilgiye çabuk bir şekilde erişme ve özümseme ihtiyacı duyarlar. Analitik düşünürler. Sosyal mecralar ile arkadaşları ile hızlı bir şekilde iletişim kurup kararlar alırlar. Oyun, eğlence, bilgi edinme ve gündelik hayatlarının diğer önemli bileşenlerinin çoğu onlar için bilgisayar ve İnternettedir. Bu maddeleri diğer toplumsal ve sosyal yönlerden ele alarak çoğaltmak mümkündür. Burada önemli olan nokta ise teknoloji ve özellikle İnternet ile birlikte çok farklı bir nesil ile karşı karşıya kaldığımızdır. İnternet kullanımı çocuklar arasında hızla artmaktadır. Çocuklar İnternet'i daha küçük yaşlarda kullanmaya başlamakta, farklı iletişim araçları kullanarak çevrimiçi ortamda daha fazla zaman geçirmektedir. İnternet onların eğitimi, yaratıcılıkları ve kendilerini ifade etmeleri bakımından önemli bir kanal olabilmektedir. Bununla birlikte, bu durum çocukların yetişkinlere göre daha savunmasız oldukları bir risk ortamını da beraberinde getirmektedir. (Güler, Bayzan ve Güneş, 2019).

Türk basınında bilişim suçları konusunda yer alan haberlerde faillerin daha çok çocuk kullanıcıları hedef aldığı, onları kandırarak cinsel yönden istismar ettiği görülmektedir. Bunun yanı sıra ikinci olarak kimlik hırsızlığının sıkça yaşandığı görülmektedir. Failler özellikle zengin olduğu bilinen kişilerin bilgilerini ele geçirip banka hesaplarına ulaşmaktadır. Amatör olarak işlenen bu suçların failleri bilgisayar ip adreslerinden yakalanarak gerekli yargılamaya tabii tutulmaktadır. Fakat çoğu zaman bu yaptırımlar mağdurların psikolojik yönden rahatlamasını sağlamamaktadır. Bu gibi bilişim sistemleri yoluyla işlenen suçların kurbanı olan başta çocuk kullanıcılar olmak üzere yetişkinler de maddi manevi zarara uğramaktadırlar. Bu noktada, bilişim suçlarına ve internet ortamından gelecek saldırılara karşı kullanıcıların bilinçlenmesi, kendilerini ve çocuklarını korumaya yönelik önlemler almaları konusunda bilgilendirici her türlü yayının yapılması devlet tarafından atılması gereken en önemli adımlardan biri olmalıdır. Bu gibi önlemler de en az kanunlar kadar bu suçların azalmasında etkili olabilir (Sönmez, 2018).

Öğretmen Adayları ve Bilişim Güvenliği

İnternete daha çok gençlerin rağbet gösterdiği düşünülse de ileri yaştaki bireylerin de gün geçtikçe internet kullanımının içinde yer almaya başladığı gözlemlenmektedir. Kuşkusuz bunun nedeni internetin insanlığa sağladığı eğlence, bilgiye kolayca ulaşım, vakit doldurma, iletişim, evden kolayca alışveriş ve internet üzerinden para kazanma gibi faydalarıdır. Buzdağının görünen yüzü olan bu faydaların insan hayatındaki olumlu etkisi yadsınamaz. Gün geçtikçe zorlaşan hayat şartları karşısında çoğu insan için en ekonomik yollu kaçış yolu olarak benimsenen internet kullanımı dünyada ve ülkemizde gittikçe artmaktadır. İnsanlar bireyselliklerinin konforunda güvenli olarak tanımlayabilecekleri bir ortamda internete girerek en ucuz ve en kolay şekilde istedikleri gibi vakit geçirebilmektedirler. Peki, kendilerini güvende hisseden bir internet kullanıcısı, gerçekten güvenli bir ortamda mıdır? Olması gereken yanıt "evet" olsa da, ne yazık ki sanal âlem yediden yetmişe tüm kullanıcılar için tehlikelerle dolu bir dünyadır (Sönmez, 2018).

Artan bilişim güvenliği tehditleri, Uluslararası Eğitimde Teknoloji Topluluğu standartları, kamu kurum ve özel sektörde verilerin çok önemli olduğu dikkate alındığında öğretmen adaylarının bilişim güvenliği bilgileri son derece önemlidir. Ayrıca, olası bir bilişim suçundan bireyin kendisini ne şekilde koruması gerektiği konularında bilgilendirme ve yönlendirilmeye gereksinim duymaktadır. Yaşadığımız yüzyılda bilgi ve iletişim teknolojilerinin açık bir ifadesi biçiminde açıklanan bilgisayar ve akıllı telefonlar çoğu kişinin gayet rahat bir şekilde ulaşabileceği araçlar olmuş ve bilişim suçunun oluşmasını daha kolay hale getirmiştir. Bu nedenden dolayı bilişim suçlarından dolayı mağdur olabilecek olası bireylerin çoğalmasına neden olabilir. Böylece, bilişim suçları ve türlerinin yeni nesiller tarafından bilinmesi çok önemlidir. Fakat güvenlikten sorumlu kurumların bilişim suçlarını önleme ve bu olayları açığa çıkarma faaliyetlerinin yeterli olamayacağı bilinmekle beraber, toplumun geneli düşünüldüğünde bu suçların oynamış olduğu önemli roller sebebiyle eğitimde liderlik özelliği bulunan öğretmenlerin bilişim suçları ve diğer yakından ilgili bu kavramları yeterince bilmesi halinde, bilişim suçları konularında genç nesilleri yeterli bilinç düzeyine çıkarmalarına yönelik yeni ve önem arz eden sorumlulukların değerli öğretmenlere yüklenmesi gerekmektedir (Gözler ve Taşçı, 2015).

Bilişim suçlarının önüne geçilmesi ve bu konularda yeterince farkındalık oluşturulması diğer gruplara nazaran öncelikli grup olarak bilinen öğretmen adayları ve sonrasında öğretmenlerin olduğu söylenebilir. Öğretmen adaylarının bu konuda farkındalıklarının belirlenmesi ve arttırılmasına yönelik öneriler gelecekte onların yetiştireceği öğrencilere de etki edecektir (Topal, Geçer, Akkaya, Güzel ve Of, 2018)

Bilişim Güvenliği Farkındalığı

Bilişim teknolojilerinin kullanımın artmasıyla her alanda üretilen bilgi miktarında hızlı bir artış olmaktadır. Bilgi toplumunda hayatımızdaki pek çok işlemin kolaylaşmasıyla birlikte bilgi güvenliği konusuna yönelik farklı boyutlarda riskler ve beraberinde tehditler oluşmaktadır. Kullanıcıların oluşan bu risk ve tehditleri farkında olmamasında dolayı en fazla maddi olarak zarara uğramaları ve/veya kayıtlı olan kendilerine ait bilgilerinin değişikliğe uğratılması, silinmesi veya kendilerine ait bilgilerin izin alınmadan erişim sağlanması benzeri istenmeyen bazı istenmeyen durumlarla karşı karşıya kalabilmektedir. Bu teknolojiler vasıtasıyla işlenen suçlar kişilere, kişilerin mülkiyet hakkına, devlete veya özeldeki kurumlara, bu kurumların teknik sistemlerini çökertmek için de işlenmektedir (Pati, 2019). Bilgisayarlar ve internet aracılığıyla bu teknolojilerin kullanılmasıyla gerçekleştirilebilen suç şekline bilişim suçu denmektedir (Maheshwari, Hyman ve Agrawal, 2011) .

İlgili Araştırmalar

Türkiye'deki eğitim fakülteleri içerisinde öğrenimini görmekte olan öğrenciler ile yapılan çalışmada, bilişim güvenliği farkındalık düzeylerinin incelenmiş ve araştırma sonucunda, birçok öğrenci bilişim güvenliğinin ne olduğu ve bu konudaki farkındalıklarının bulunduğu anlaşılmıştır. İnternet kullanımıyla ilgili süre konusunda, bilişim güvenliği maddelerinden elde edilen veriler neticesinde internete erişim sağlayan katılımcı grubunun ortalama ve ortalamanın üstünde öğrencilerin en fazla korsan yazılım kullanıyor oldukları anlaşılmıştır. Bilişim teknolojileri ile ilgili araç gereç ve yazılımlardan maksimum yararlanmanın etik kullanım açısından bir ilerlemeye neden olmadığı da görülmüştür. Elde edilen sonuca göre bilhassa ilerde verilmesi planlanan eğitimlerle daha fzla deneyime sahip kullanıcı grubuna etik ve yasal kullanım ile ilgili olarak öncelik verilmesi gerekmektedir (Akgün ve Topal, 2015).

Öğretmen adayları ile yapılan bir başka araştırmada, Bilgisayar ve Öğretim Teknolojileri Eğitimi (BÖTE) bölümünde öğrenim gören öğretmen adaylarının bilişim güvenliği bilgilerinin ne düzeyde olduğu ortaya konulmaya çalışılmıştır. BÖTE'de öğrenim gören öğretmen adaylarının bilişim güvenliği bilgi düzeylerinin düşük olduğubu araştırmanın yine sonucudur. Bunun yannda, BÖTE öğretmen adaylarının bilişim güvenliği konusundaki bilgi düzeylerinin cinsiyet ve öğrenim gördüğü üniversite açısından farklılaştığı da görülmüşken; yaşa, sınıf, kaç yıldır bilgisayar sahibi olma, günlük bilgisayar kullanım süresi, günlük internet kullanım süresi ve bilişim güvenliği konusunda bir ders ve/veya kurs alma durumu açısından anlamlı farklılık olmadığı da bu araştırma sonucunda anlaşılmıştır. Genel olarak bu araştırma soncunda, BÖTE bölümü için geliştirilen öğretim programında bilişim güvenliği ilgili bir dersin yer almasında büyük faydalar olacağından bu dersin öğretim programına eklenmesi sonucu ortaya konmuştur (Gökmen ve Akgün, 2015).

Yapılan bir diğer araştırmada, öğretmenlerin yetiştirildiği bölümlerin arasında bulunan Sınıf Öğretmenliği Anabilim dalında bulunan öğretmen adayları aslında sınıf öğretmeni olacak olan adayların bilişim suçları konularındaki görüşleri, ayrıca bu suçların kendilerince ne kadar algılandığı belirlenmeye çalışılmıştır. Çalışma grubunda sınıf öğretmenlerinin, eğitimde anaokuldan sonra ilk basamakta yer alıyor oluşu, çocukların eğitim çağının ilk yıllarında öğretmenler çocuklar için rol model olmakta, gençlere önemli mesajlar vermektedirler. Yapılmış olan araştırmanın çalışma grubunu, 2013–2014 öğretim yılında Erciyes Üniversitesi'nin ilköğretim bölümündeki sınıf öğretmenliği anabilim dalında öğrenim görmekte olan 205 öğretmen adayı oluşturmuştur. Bu çalışma sonucuyla, öğrencilerin bilişim suçlarına yönelik bilinç düzeyleri ve bu suçlara yönelik önleyici tutum sergileme düzeylerinin son derece düşük olduğu, bilişim suçları konularında güvenlik ile ilgili kurumlarca bilgilendirilme gereksinimi olduğu belirlenmiştir (Gözler ve Taşçı, 2015).

Geçmiş yıllarda çoğu zaman kağıt üzerine baskı şekilindeki materyaller ile öğretim yapan öğretmenler, şimdilerde ise bilgi ve iletişim teknolojilerini kullanarak bilgiyi dijital ortamlar kullanarak hazırlamakta ve saklamaktadırlar. Eğitim öğretim faliyetlerinde teknolojiyi yoğun olarak her zaman kullanmaları istenen öğretmenlere ait dijital verilerin güvenliği önem arz etmektedir. Dijital veri güvenliği farkındalıklarının araştırıldığı bir başka çalışmada MEB'e bağlı Balıkesir ilinde 29

farklı okulda görev yapan toplam 870 öğretmenden elde edilen veriler toplanması için dijital veri güvenliği farkındalık ölçeği (DVGFÖ) kullanılmıştır. Elde edilen bulgular ışığında, öğretmenlerin oldukça yüksek dijital veri güvenliği farkındalıklarına sahip oldukları anlaşılmıştır. Sahip olmuş oldukları bu farkındalık düzeyinin cinsiyet, günlük bilgisayar kullanımı süresi, günlük İnternet kullanımı süresi ve farklı teknolojilere sahip olma durumuna bağlı olarka değiştiği görülmüş; fakat branş, öğrenim kademesi, öğrenim durumu ve mesleki kıdem açısından değişmediği de belirlenmiştir. (Yılmaz, Şahin ve Akbulut, 2016).

Bir diğer araştırmada, nitel araştırma yöntemi olarak olgu bilim deseni kullanılarak eğitim fakültesinde okumakta olan öğretmen adaylarının bilişim suçları ile ilgili deneyimleri ve bilişim güvenliği dersi kapsamında yer alması gerekli konulara ilişkin görüşlerinin tespit edilmiştir. Bu araştırmada çalışma grubu olarak, öğretmenlik programlarında öğrenim gören öğretmen adayları şeçilmiştir. Araştırma bulgularına göre; az da olsa bazı öğretmen adaylarının bilişim suçu işlemiş oldukları ya da bilişim suçlarınna maruz kalmış oldukları, bilişim suçu konularında bilgi düzeylerinin yeterli olmadığı ve bir bilişim suçu ile karşı karşıya kaldıklarında ne yapacaklarını bilmedikleri anlaşılmıştır. Bunun yanında, öğretmen adaylarının çoğunun bilişim güvenliğinin ne olduğu veya kapsamı konularında yetersiz bilgi birikimine sahip oldukları belirlenmiştir. Bu araştırma sonucunda bilişim teknolojilerinin güvenli bir şekilde kullanılması ve kişisel bilgilerinin güvenliğinin sağlanması gibi birçok konuda öğretmen adaylarının eğitime ihtiyaçları olduğu analaşılmıştır (Gökmen ve Akgün, 2016).

Lise öğrencilerinin internet kullanımına ilişkin öz yeterliklerine ilişkin algıların belirlenmesi amacıyla yapılan çalışmada, örneklem olarak KKTC sınırları içerisinde bulunan 30 lisede okuyan 880 lise öğrencisi alınmıştır. Araştırmaya katılanların “Sosyal Ağ (sosyal medya) Güvenliği” konusundaki öz yeterliklerinin ilk boyutu incelenmiştir. Anketlere yapılan açıklamaya göre, “Sosyal Ağ (sosyal medya) Güvenliği”; “Kötü Amaçlı Yazılım” ve “Web Güvenliği ve Sosyal Mühendislik” olan araştırmanın ikinci ve üçüncü boyutlarında katılımcıların yeterliliği orta düzeydedir. Araştırmanın son aşamasında “Bilgisayar Güvenliği” ile ilgili öğrenciler yeterli düzeyde olduğu tespit edildi. Sonuç olarak, öğrencilerin düzenli olarak kullandıkları Sosyal Ağlarda yeterli güvenceye sahip oldukları, oysa Web Güvenliği ve Sosyal mühendislik alanında orta düzeyde yeterliğe sahip oldukları görülmüştür.

Bu sonucun temel nedeni, öğrencilerin interneti tam bilinçli ve doğru kullanmamaları, dolayısıyla öğrencilerin bu konularda eğitim almadıklarıdır (Erçağ, ve Karabulut, 2017).

Malezya yarımadasının kuzey bölgesinde bulunan üniversite öncesi bir kurumda öğrencilerin siber güvenlik farkındalık seviyelerini araştırılmıştır. Bu araştırmanın yürütülmesi için zemin hazırlayan iki faktör vardır. Birincisi, ağır bilgisayar kullanıcıları olarak öğrencilere yönelik tehditler var ve ikincisi, öğrencilerin çalışmalarını yakında tamamlamaları üzerine gelecekteki işçi gücü olacağından, öğrencilerin siber güvenlik bilincini kazanmaları gerekiyor. Ankete toplam 318 öğrenci katılmıştır. Araştırma bulguları, öğrencilerin farkındalığının ortalama düzeyde olduğunu ve erkek ve kız öğrenciler arasında siber güvenlik farkındalığı düzeyinde bir fark olmadığını göstermektedir. Çalışma ayrıca, saatlerce bilgisayar kullanımının öğrencilerin siber güvenlik farkındalığı düzeyine katkıda bulunmadığını ortaya koymaktadır. İlginç bir şekilde, bu araştırma ayrıca, farklı kurslardan öğrenciler arasında farklı siber güvenlik farkındalığı seviyelerinin bulunduğunu ve daha iyi bilgi işlem becerisine sahip öğrencilerin daha iyi siber güvenlik farkındalığı seviyelerine sahip olduğunu bulunmuştur (Subramaniam, 2017).

Siber eğitim müfredatının, büyüyen siber teknolojileri dikkate alması ve bu teknolojilerin hangi yönlerinin dördüncü sanayi devrimi ile uyumlu hale getirilmesi gerektiği çok önemlidir. Yazılan kitap bölümünde, Güney Afrika'daki mevcut siber güvenlik eğitimi seviyesinin kapsamlı bir analizi sunulmuştur. Ayrıca, ülkedeki siber güvenlik eğitiminin mevcut eğilimlerini izlemenin yanı sıra, herhangi bir bilgi açığı dahil olmak üzere yaşanmakta olan zorluklar da incelenmiştir. Bölüm sonunda, bölüm, herhangi bir siber güvenlik tehdidini azaltabilecek gelişmiş siber güvenlik yanıtları elde etmek için ülkedeki siber güvenlik eğitiminin güçlendirilmesinde göz önünde bulundurulması için öneriler verilmiştir (Kariuki, 2018).

Özellikle bilgi ve iletişim teknolojilerindeki gelişmeler suç işlemeyi kolaylaştırmış ve bilişim suçları olarak adlandırılan kavram ortaya çıkmıştır. Bilişim suçlarının önlenmesi ve bu konuda farkındalığın arttırılmasında öncelikle ele alınması gereken gruplardan biri öğretmen adayları ve dolayısıyla öğretmenlerdir. Yapılan bir diğer çalışmada Kocaeli Üniversitesi'nde öğrenim gören öğretmen

adaylarının bilişim suçlarına yönelik bilgi düzeylerini belirlemek ve çeşitli değişkenlerle ilişkilendirilmesi amaçlanmıştır. Araştırma sonuçlarına göre öğretmen adaylarının bilişim suçları konuları ile ilgili bilgi düzeylerinin yeterli düzeyde olmadığı görülmüştür. Cinsiyete, ortalama günlük bilgisayar kullanma sürelerine göre bazı konularda anlamlı farklılıklar olduğu gözlenmiştir. Öğretmen adayları için kapsamı iyi belirlenmiş bilişim suçları konularıyla ilgili bir eğitim verilmesi önerilmektedir (Topal, Geçer, Akkaya, Güzel ve Mustafa, 2019) .

Üniversite öğrencilerinin problemli internet kullanım düzeyinin siber zorbalık ve siber mağduriyet düzeylerini yordama gücünü belirlemek; cinsiyet, sınıf düzeyi, anne ve babanın eğitim düzeyi ve ailenin gelir düzeyine göre öğrencilerin siber zorbalık düzeyi ve siber mağduriyet düzeyinde bir değişim olup olmadığı incelenmiştir. Araştırma bulguları gözetildiğinde, siber zorbalık ve siber mağduriyetin üniversite öğrencileri arasında yaygın bir problem olduğunu ortaya koymuştur. Öğrencilerin siber zorbalık ve siber mağduriyet düzeyleri cinsiyet ve ailenin gelir düzeyine göre anlamlı düzeyde farklılık gösterirken sınıf düzeyi ve babanın eğitim düzeyine göre anlamlı düzeyde farklılık göstermemektedir. Annenin eğitim düzeyine göre ise siber zorbalık düzeyleri anlamlı düzeyde farklılık gösterirken siber mağduriyet düzeyleri göstermemektedir. Buna ek olarak, problemli internet kullanımının alt ölçekleri olan sosyal fayda ve internetin olumsuz sonuçları siber zorbalık ve siber mağduriyeti yordarken diğer alt ölçek olan aşırı kullanım yordamamaktadır. Bulgular, ilgili alanyazın temelinde tartışılmış ve bazı öneriler sunulmuştur (Gönültaş, 2019).

YÖNTEM

Bu bölümde araştırma modeli, çalışma gurubu, veri toplama araçları, verilerin toplanması ve analizlerinde kullanılan teknikler ele alınacaktır.

Araştırma Modeli

Nicel araştırma yaklaşımı çerçevesinde yürütülen bu araştırmada tarama modelinden yararlanılmıştır. Tarama modeli, geçmişte ya da halen var olan bir durumu var olduğu şekliyle betimlemeyi amaçlayan araştırma yaklaşımlarıdır (Büyüköztürk, Çakmak, Akgün, Karadeniz ve Demirel, 2017).

Çalışma Grubu

Araştırmanın çalışma grubunu 2018-2019 eğitim-öğretim yılında Yakın Doğu Üniversitesi Atatürk Eğitim Fakültesi'nde bilişim teknolojileri dersi alan 282 öğretmen adayı oluşturmaktadır.

Çalışma Grubunun Demografik Özellikleri

Çalışma grubunun demografik özelliklerine ilişkin bazı bulgular tablo 3.1'de verilmiştir.

Tablo 3.1

Çalışma grubunun demografik özellikleri

Cinsiyet	**N**	**%**
Kız	182	64,5
Erkek	100	35,5
Yaş	282	21,5
Sınıf Düzeyi		
1.Sınıf	58	20.6
2.Sınıf	114	40.4
3.Sınıf	46	16.3
4.Sınıf	64	22.7
Toplam	282	100,0

.Tablo 3.1 incelendiği zaman "çalışma gurubunun demografik özellikleri" durumuna öğretmen adaylarının 282 ifadesinden (182)'si kız ve (100)'ünü erkek öğretmen adayları oluşturmaktadır. Yaş aralığı ise (21.5) yaş olarak saptanmıştır. Sınıf düzeyleri durumuna ise 282 öğretmen adayı (58), 1. Sınıf, (114)'ü 2. Sınıf , (46)'sı 3.sınıf, (64)'ü 4.sınıf olarak ifade etmiştir.

Araştırmanın Çalışma Grubunu Oluşturan Öğretmen Adaylarının İnternet ile İlgili Kişisel Bilgilerine Göre Frekans ve Yüzdeleri

Bu bölümde araştırma kapsamına alınan öğretmen adaylarının internet ile ilgili kişisel bilgilerine yer verilmiştir.

Tablo 3.2

Öğretmen adaylarının internete bağlanma yerlerine göre dağılımları

İnternete Bağlanma Yeri	**N**	**%**
İnternete Bağlanmıyorum	10	3,5
Evden	216	76,6
İnternet Kafeden	32	11,3
Cep Telefonundan	226	80,1
Okulda BT sınıfından	38	13,5
Diğer	8	2,8

Tablo 3.2 incelendiği zaman "öğretmen adaylarının internete bağlanma yerlerine göre dağılımları" durumuna öğretmen adaylarının 282 ifadesinden (10)'u internete bağlanmıyorum, (216)'sı evden, (32)'si internet kafeden, (226)'sı cep telefonundan, (38)'i okulda BT sınıfından ve (8)'i diğer ifadelerini kullanmıştır.

Tablo 3.3

Öğretmen adaylarının kaç yıldan beri internet kullandıklarına yönelik dağılımları

Yıl	N	%
0-1yıl	10	3.5
1-2yıl	12	4.3
2-3yıl	80	28.4
3 yıl ve üzerinde	180	63.8

Tablo 3.3 incelendiği zaman "öğretmen adaylarının kaç yıldan beri internet kullandıklarına yönelik dağılımları" durumuna öğretmen adaylarının toplam 282 ifadesinden (10)'u 0-1 yıl, (12)'si 1-2 yıl, (80)'i 2-3 yıl ve (180)'i 3 yıl ve üzerinde kullandıkları tespit edilmiştir.

Tablo 3.4

Öğretmen adaylarının internete bağlanma amaçlarına göre dağılımları

İnternete Bağlanma Amacı	N	%
Oyun oynama	138	48.9
Video izleme	226	80.1
Arkadaşlarla Sohbet	242	85.8
Hayatla İlgili Paylaşımda bulunmak	140	49.6
Ödev Yapmak	224	79.4
Araştırma Yapmak	210	74.5
Diğer	10	3.5

Tablo 3.4 incelediği zaman "öğretmen adaylarının internete bağlanma amaçlarına göre dağılımları" durumuna öğretmen adaylarının toplam 282 ifadesinden (118)' i oyun oynama, (226)'sı video izleme, (242)'si arkadaşlarla sohbet etme, (140)'ı hayatla ilgili paylaşımda bulunmak, (224)'ü ödev yapmak, (210)'u araştırma yapmak ve (10)'u ise diğer amaçlarla internete bağlanmaktadır.

Tablo 3.5

Öğretmen adaylarının hangi sıklıkla internete girdiklerine yönelik dağılımları

Sıklık	**N**	**%**
0-1saat	18	6.4
1-2saat	28	9.9
2-3saat	150	53.2
3 saat ve üzeri	86	30.5

Tablo 3.5 incelendiği zaman "öğretmen adaylarının hangi sıklıkla internete girdikleri" sorusuna öğretmen adaylarının toplam 282 ifadesinden (18)'i 0-1 saat, (28)'i 1-2 saat, (150)'si 2-3 saat ve (86)'sı 3 saat ve üzeri ifadelerini kullanmıştır.

Tablo 3.6

Öğretmen adaylarının internette ailesinin kredi kartı ile alış veriş yapma durumlarına göre dağılımları

Ailesinin kredi kartı ile alış veriş yapma durumu	**N**	**%**
Evet	102	36.2
Hayır	180	63.8

Tablo 3.6 incelendiği zaman " öğretmen adaylarının internette ailesinin kredi kartı ile alış veriş yapma" durumları sorusuna öğretmen adaylarının toplam 282 ifadesinden (102)'si evet ve (180)'i ise hayır ifadesini kullanmıştır.

Tablo 3.7

Öğretmen adaylarının internette mağdur olma veya saldırıya uğrama durumlarına göre dağılımları

Mağdur olma veya saldırya Uğrama Durumu	**N**	**%**
Evet	74	26.2
Hayır	208	73.8

Tablo 3.7 incelendiği zaman, "öğretmen adaylarının internette mağdur olma, saldırıya uğrama" durumları sorusuna öğretmen adaylarının toplam 282 ifadesinden (74)'ü evet ifadesini kullanmış ve (208)'i ise hayır ifadesini kullanmıştır.

Tablo 3.8

Öğretmen adaylarının internette hangisine maruz kaldıklarına göre dağılımları

Maruz Kalınan Durum	**N**	**%**
Elektronik posta yoluyla	40	14.2
Yazılı mesaj yolu ile	76	27.0
Resimli mesaj yolu ile	54	19.1
Anında karşılıklı mesaj ile	48	17.0
Sosyal iletişim ağları ile	78	27.7
Sohbet odaları ile	38	13.5
Sanal ortamdaki oyunlar esnasında	56	19.9
Diğer	4	1.4

Tablo 3.8 incelendiği zaman "öğretmen adaylarının internette hangisine maruz kaldıklarına göre dağılımları" durumuna öğretmen adaylarının toplam 282 ifadesinden (40)'ı elektronik posta yoluyla, (76)'sı yazılı mesaj yolu ile, (54)'ü resimli mesaj yolu ile, (48)'i anında karşılıklı mesaj yolu ile, (78)'i sosyal iletişim

ağları ile, (38)'i sohbet odaları ile, (56)'sı sanal ortamdaki oyumlar esnasında ve (4)'ü diğer ifadelerini kullanmışlardır.

Veri Toplama Aracı

Araştırmada veri toplama araçları olarak, kişisel bilgi formu, geçerliği ve güvenirliği Gözler ve Taşçı (2015) tarafından sağlanıp geliştirilen "Bilişim Kavramları ve Suçlarına Yönelik Öğrenci Görüş Ölçeği" kullanılmıştır.

Kişisel Bilgi Formu

Kişisel bilgi formu araştırmacılar tarafından geliştirilmiştir. Bu form içinde 8 madde bulunmaktadır; Cinsiyet, yaş, bölüm ve sınıf düzeyi ile ilgili maddelerden oluşmaktadır.

Bilişim Kavramları ve Suçlarına Yönelik Öğrenci Görüş Ölçeği

Araştırma kapsamına alınan öğretmen adaylarının bilişim kavramları ve suçlarına yönelik görüşlerinin saptanması amacıyla Gözler ve Taşçı (2015) tarafından 2015 yılında geliştirilen Bilişim Kavramları ve Suçlarına Yönelik Öğrenci Görüş Ölçeği (BKSYÖGÖ) kullanılmıştır.

BKSYÖGÖ beşli derecelendirme kullanılarak geliştirilmiş 16 maddeden oluşmaktadır. Ölçeğe verilen yanıtlar "Hiç katılmıyorum=1", "Katılmıyorum=2", "Kısmen katılıyorum=3", "Katılıyorum=4" ve "Tamamen katılıyorum=5" olacak şekilde puanlanmıştır. Ölçekten alınacak olan yüksek puan, bilişim kavramları ve suçlarına yönelik öğretmen adaylarının görüşlerinin olumlu olduğunu ifade edilmektedir (Gözler ve Taşçı, 2015). Aşağıda Tablo 3.3.1'de ölçeğin sonuçlarının yorumlarında kullanılan puan sınırları verilmiştir.

Tablo 3.3.1

Ölçeğin sonuçlarının yorumlarında kullanılan puan sınırları

Puan Sınırları	
1–1,80	Hiç Katılmıyorum
1,81–2,60	Katılmıyorum”
2,61–3,40	Kısmen Katılıyorum
3,41–4,20	Katılıyorum
4,21–5.00	Tamamen Katılıyorum

Yapılan geçerlik-güvenirlik çalışması sonucunda Cronbach alfa güvenirlik katsayısı; ölçeğin geneli için 0,84 ve KMO değeri ise .76’dır.

Araştırmacılar tarafından hesaplanan Cronbach alfa güvenirlik katsayısı ölçeğin geneli için 0,74’dir. Bu sonuçlar doğrultusunda bilişim kavramları ve suçlarına yönelik öğretmen adaylarının görüşlerinin saptanmasında geçerli ve güvenilir bir ölçme aracı olduğu görülmüştür.

Verilerin Toplanması

Araştırmanın gerçekleştirilebilmesi için YDÜ Eğitim Bilimleri Enstitüsünden gerekli etik izin alındıktan sonra, Atatürk Eğitim Fakültesinde bulunan yöneticilerden de izin alınarak öğretmen adaylarından araştırıma için gönüllü olanlara uygulanmıştır. Öğretmen adaylarının müsait oldukları gün ve saatlerde ölçek ve kişisel bilgi formu öyle uygulanmıştır. Böylece, ölçek ve kişisel bilgi formu 10-15 dakikalık süre sonunda toplanmıştır.

Verilerin Analizi

Araştırma verilerinin elde edilmesinden sonra çözümlenmesi için Statistical Package for Social Sciences SPSS 24.0 istatistik yazılım programı kullanılmıştır. Yapılmış olan tüm istatistiklerde anlamlılık düzeyi değeri .05 olarak alınmıştır.

Verilerin homojenlik olarak dağılıp dağılmadığının tespiti için SPSS ile ön çalışma yapılmıştır. Bağımlı değişkenlerin alt gruplardaki dağılımlarının normal

olmaması yapılmış olan Kolmogorow-Smirnov testi sonucunda anlaşılmıştır ($p<0,05$). Her iki ölçek maddelerinin açıklamaları için ortalama ve standart sapma değerleri hesaplanmıştır.

Araştırmada ortalama puanlar arasındaki farkların anlamlılığın test edilmesi için, değişkenin iki alt grubu olması durumunda parametrik olmayan testlerden bağımsız örneklemler için Mann-Whitney U testi ve çapraz tablolar için Ki-kare testleri kullanılmıştır. Kruskal Wallis H testi, ilişkisiz ikiden daha fazla örneklem ortalaması arasındaki farkın anlamlı bir şekilde farklı olup olmadığını belirlemek için uygulanmıştır (Büyüköztürk ve diğ., 2017).

BULGULAR VE YORUMLAR

Araştırmanın bu bölümünde genel ve alt amaçlar göz önünde bulundurularak elde edilen veriler ile, frekans (N), yüzdelik (%), aritmetik ortalama ($\overline{X}$), standart sapma (SS), bağımsız örneklemler için Mann-Whitney U testi ve Kruskal Wallis H testi kullanılarak oluşturulan tablolara ait bulgu ve yorumlara yer verilmiştir.

Bu bölümde, araştırmanın amacı ve alt amaçları doğrultusunda elde edilen bulgular yer almaktadır.

Tablo 4.1.

Öğretmen adaylarının cinsiyeti açısından internette mağdur olma veya saldırya uğrama durumuna yönelik ki -kare (X^2) testi analizi

Cinsiyet		Mağdur olma veya saldırya Uğrama Durumu			Kay Kare (Ki kare) (X2)	Sig. Anlamlılık (p)
		Evet	Hayır	Toplam		
Kız	N	46	136	182	**0.248a**	**.672**
	%	25.3%	74.7%	100.0%		
Erkek	N	28	72	100		
	%	28.0%	72.0%	100.0%		
Toplam	N	74	208	282	**p > 0,05**	
	%	26.2%	73.8%	100.0%		

Tablo 4.1'de araştırmaya dahil edilen öğretmen adaylarının cinsiyeti açısından internette mağdur olma veya saldırya uğrama durumları benzerlik göstermektedir. Yapılan Ki-kare testi sonucunda istatiksel anlamda anlamlı bir fark bulunmadığı için (p>0,05) öğretmen adaylarının cinsiyeti açısından internette mağdur olma veya saldırya uğrama durumu üzerinde bir etkisi olmadığı görülmüştür.

Tablo 4.2.

Öğretmen adaylarının interneti kullanma yılları açısından internette mağdur olma veya saldırya uğrama durumuna yönelik ki -kare (X^2) testi analizi

Kaç Yıldır İnternet Kullanıyor		Mağdur olma veya saldırya Uğrama Durumu			Kay Kare (Ki kare) (X2)	Sig. Anlamlılık (p)
		Evet	Hayır	Toplam		
0-1yıl	N	6	4	10		
	%	60.0%	40.0%	100.0%		
1-2yıl	N	8	4	12		
	%	66.7%	33.3%	100.0%		
2-3yıl	N	16	64	80	**17.930a**	**.001**
	%	20.0%	80.0%	100.0%		
diğer	N	44	136	180		
	%	24.4%	75.6%	100.0%		
Toplam	N	74	208	282		
	%	26.2%	73.8%	100.0%	**p < 0,01**	

Tablo 4.2'de araştırmaya dahil edilen öğretmen adaylarının interneti kullanma yılları açısından internette mağdur olma veya saldırya uğrama durumlarında anlamlı farklılıkların olduğu görülmüştür. Yapılan Ki-kare testi sonucunda istatiksel anlamda anlamlı bir fark bulunduğu için ($p<0,05$) öğretmen adaylarının internet kullanım yılları açısından internette mağdur olma veya saldırya uğrama durumu üzerinde bir etkisi olduğu görülmşütür. İnterneti daha uzun yıllar kullanan kişilerin mağdur olma ve saldırya uğrama durumlarında daha çok artış görüldüğü gözlemlenmektedir.

Tablo 4.3

Öğretmen adaylarının internete bağlanma ile mağdur olma veya saldırya uğrama durumuna yönelik ki -kare (X^2) testi analizi

İnternete Bağlanmıyorum		Mağdur olma veya saldırya Uğrama Durumu			Kay Kare (Ki kare) (X2)	Sig. Anlamlılık (p)
		Evet	Hayır	Toplam		
Evet	N	6	4	10	**5.752a**	**.026**
	%	60.0%	40.0%	100.0%		
Hayır	N	70	202	272		
	%	25.7%	74.3%	100.0%		
Toplam	N	76	206	282	**p < 0,05**	
	%	27.0%	73.0%	100.0%		

Tablo 4.3'de araştırmaya dahil edilen öğretmen adaylarının internete bağlanma ile mağdur olma veya saldırya uğrama durumları arasında anlamlı farklılıklar görülmüştür. Yapılan Ki-kare testi sonucunda istatiksel anlamda anlamlı bir fark bulunduğu için ($p<0,05$) öğretmen adaylarının internete bağlanma açısından mağdur olma veya saldırya uğrama durumu üzerinde bir etkisi olduğu görülmüştür.

Öğretmen Adaylarının Bilişim Kavramları ve Suçlarına Yönelik Görüşleri

Öğretmen adaylarının bilişim kavramları ve suçlarına yönelik görüşlerine ilişkin ortalama ve standart sapma değerleri Tablo 13'de verilmiştir.

Tablo 4.4

Öğretmen adaylarının bilişim kavramları ve suçlarına yönelik görüşleri

Maddeler	$\bar{X}$	**SS**
Mail adresimin ya da benzeri sayfalarının şifresinin kırılması durumunda ne yapacağımı bilirim.	3.41	1.307
Lisans eğitimimizde aldığımız bilgisayar derslerinde bilişim suçlarına yönelik bilgiler verilmelidir.	3.86	1.200
Mail adreslerimin şifrelerini samimi arkadaşlarım bilir.	2.07	1.347
İnternet dolandırıcılığı hakkında yeterli bilgiye sahip değilim.	2.73	1.233
Mail ya da kendime ait kişisel kullanım sayfalarımın başkalarının eline geçmesi beni çok üzer.	3.90	1.297
Bana gelen virüslü maili fark edebilirim.	3.16	1.254
Tanımadığım kişileri mail adresime ve kişisel sayfalarıma eklemem.	3.60	1.283
Kredi kartımla internetten rahatlıkla alışveriş yaparım.	3.31	1.319
Bilgisayarım virüslere karşı korunaklıdır.	3.64	1.151
Basın ve medya internet suçları	3.17	1.146
Herhangi bir bilişim suçuna şahit olduğumda ne yapacağımı bilirim.	3.26	1.166
Bilişim suçlarına verilen cezaların ağır olması gerekmektedir.	3.64	1.087
Bilişim suçlarına yönelik bilgilendirmenin ilköğretimden itibaren başlaması gerekmektedir.	3.90	1.092
Bilişim suçları gözde büyütülecek düzeyde tehlikeli değildir.	2.26	1.277
Bilişim suçlarına yönelik, öğrencilere konferanslar veya seminerler düzenlenmelidir.	3-.97	1.128
Bilişim suçlarını işleyebilen insanlar çok zeki insanlardır.	2.98	1.268
Genel Ortalama	3.30	.552

Tablo 4.4'de öğretmen adaylarının bilişim kavramları ve suçlarına yönelik görüşlerine ilişkin ortalama ve standart sapma değerlerine göre değerlendirildiğinde, "Mail adresimin ya da benzeri sayfalarının şifresinin kırılması durumunda ne yapacağımı bilirim" ($\bar{X} = 3.41, SS = 1.307$), "Lisans eğitimimizde aldığımız bilgisayar derslerinde bilişim suçlarına yönelik bilgiler verilmelidir" ($\bar{X} = 3.86, SS = 1.200$), "Mail ya da kendime ait kişisel kullanım sayfalarımın başkalarının eline geçmesi beni çok üzer" ($\bar{X} = 3.90, SS = 1.297$), "Tanımadığım kişileri mail adresime ve kişisel sayfalarıma eklemem" ($\bar{X} = 3.60, SS = 1.283$), "Bilişim suçlarına verilen cezaların ağır olması gerekmektedir" ($\bar{X} = 3.64, SS =$

1.087), "Bilişim suçlarına yönelik bilgilendirmenin ilköğretimden itibaren başlaması gerekmektedir" ($\bar{X} = 3.90,\ SS = 1.092$), "Bilişim suçlarına yönelik, öğrencilere konferanslar veya seminerler düzenlenmelidir" ($\bar{X} = 3.97, SS = 1.128$) ve "Bilgisayarım virüslere karşı korunaklıdır" ($\bar{X} = 3.64, SS = 1.151$) maddeleri için öğretmen adayları katılıyorum yanıtı vermişlerdir.

Ayrıca, "İnternet dolandırıcılığı hakkında yeterli bilgiye sahip değilim ($\bar{X} = 2.73, SS = 1.233$), "Bilişim suçlarını işleyebilen insanlar çok zeki insanlardır" ($\bar{X} = 2.98, SS = 1.268$), "Bana gelen virüslü maili fark edebilirim" ($\bar{X} = 3.16, SS = 1.254$), "Kredi kartımla internetten rahatlıkla alışveriş yaparım" ($\bar{X} = 3.31, SS = 1.319$), "Basın ve medya internet suçları" ($\bar{X} = 3.17, SS = 1.146$), "Herhangi bir bilişim suçuna şahit olduğumda ne yapacağımı bilirim" ($\bar{X} = 3.26, SS = 1.166$) maddeleri için öğretmen adayları kararsızım yanıtı vermişlerdir.

Tüm bunların yanında "Bilişim suçları gözde büyütülecek düzeyde tehlikeli değildir" ($\bar{X} = 2.26, SS = 1.277$) ve "Mail adreslerimin şifrelerini samimi arkadaşlarım bilir" ($\bar{X} = 2.07, SS = 1.347$) maddeleri için öğretmen adayları katılmıyorum yanıtı vermişlerdir.

Öğretmen adaylarının bilişim kavramları ve suçlarına yönelik görüşleri genel olarak incelendiğinde ise ($\bar{X}$=3,30, SS=,552) kararsızım diyerek bu konuda bilgi sahibi olma konusunda emin olmadıklarını belirtmişlerdir.

Öğretmen adaylarının bilişim kavramları ve suçlarına yönelik görüşlerinin cinsiyet açısından değerlendirilmesi

Öğretmen adaylarının bilişim kavramları ve suçlarına yönelik görüşleri cinsiyete göre Tablo 14'de yapılan Mann-Whitney U testi ile karşılaştırılmıştır.

Tablo 4.5.

Öğretmen adaylarının bilişim kavramları ve suçlarına yönelik görüşlerinin cinsiyete göre karşılaştırılması

	Cinsiyet	N	Sıra Ortalaması	Sıra Toplamı	U	Z	p
Bilişim kavramları ve suçlarına yönelik görüşler	Kız	182	135.01	24571.00	7918,0	-1,806	.071
	Erkek	100	153.32	15332.00			

Öğretmen adaylarının bilişim kavramları ve suçlarına yönelik görüşlerinin cinsiyete göre karşılaştırılmasına yönelik Tablo 4.5'de yapılan Mann-Whitney U testi sonucunda anlamlı bir fark bulunmamıştır (p>.05). Buna göre, kız ve erkek Öğretmen adaylarının bilişim kavramları ve suçlarına yönelik görüşleri aynı düzeydedir.

Öğretmen adaylarının bilişim kavramları ve suçlarına yönelik görüşlerinin sınıf düzeyine göre karşılaştırılması

Öğretmen adaylarının bilişim kavramları ve suçlarına yönelik görüşleri sınıf düzeyine göre Tablo 15'de yapılan Kruskal Wallis H testi ile karşılaştırılmıştır.

Tablo 4.6.

Öğretmen adaylarının bilişim kavramları ve suçlarına yönelik görüşlerinin sınıf düzeyine göre karşılaştırılması

	Sınıf Düzeyi	N	Sıra Ortalaması	Sd	X^2	p
Bilişim kavramları ve suçlarına yönelik görüşler	1. Sınıf	58	150.64	2	6,587	,087
	2. Sınıf	114	127.69			
	3. Sınıf	46	141.50			
	4. Sınıf	64	157.81			

Tablo 4.6'da öğretmen adaylarının bilişim kavramları ve suçlarına yönelik görüşlerinin sınıf düzeyine göre incelenmesi amacıyla yapılan Kruskal Wallis H testi

sonucunda, görev yapılan sınıf düzeyi değişkenine göre, öğretmen adaylarının bilişim kavramları ve suçlarına yönelik görüşleri [X^2=6,587, p>0.05] ile ilgili olarak anlamlı bir fark olmadığı tesbit edilmiştir.

Öğretmen adaylarının bilişim kavramları ve suçlarına yönelik görüşlerinin kaç yıldan beri internet kullandıklarına göre karşılaştırılması

Öğretmen adaylarının bilişim kavramları ve suçlarına yönelik görüşleri kaç yıldan beri internet kullandıklarına göre Tablo 16'de yapılan Kruskal Wallis H testi ile karşılaştırılmıştır.

Tablo 4.7.

Öğretmen adaylarının bilişim kavramları ve suçlarına yönelik görüşlerinin kaç yıldan beri internet kullandıklarına göre karşılaştırılması

	İnternet kullanma yılı	N	Sıra Ortalaması	Sd	X^2	p
Bilişim kavramları ve suçlarına yönelik görüşler	0-1yıl	10	155.90	3	5,245	,155
	1-2yıl	12	90.33			
	2-3yıl	80	141.30			
	3 yıl ve üzeri	180	144.20			

Tablo 4.7'de öğretmen adaylarının bilişim kavramları ve suçlarına yönelik görüşlerinin kaç yıldan beri internet kullandıklarına göre incelenmesi amacıyla yapılan Kruskal Wallis H testi sonucunda, kaç yıldan beri internet kullandıkları değişkenine göre, öğretmen adaylarının bilişim kavramları ve suçlarına yönelik görüşleri [X^2=5,245, p>0.05] ile ilgili olarak anlamlı bir fark olmadığı tesbit edilmiştir.

Öğretmen adaylarının bilişim kavramları ve suçlarına yönelik görüşlerinin mağdur olma veya saldırya uğrama durumu açısından değerlendirilmesi

Öğretmen adaylarının bilişim kavramları ve suçlarına yönelik görüşlerinin mağdur olma veya saldırya uğrama durumuna göre Tablo 17'de yapılan Mann-Whitney U testi ile karşılaştırılmıştır.

Tablo 4.8.

Öğretmen adaylarının bilişim kavramları ve suçlarına yönelik görüşlerinin mağdur olma veya saldırya uğrama durumuna göre karşılaştırılması

	Saldırya uğrama durumu	N	Sıra Ortalaması	Sıra Toplamı	U	Z	p
Bilişim kavramları ve suçlarına yönelik görüşler	Evet	74	150.85	11163.00	7004,0	-1,150	.250
	Hayır	208	138.17	28740.00			

Öğretmen adaylarının bilişim kavramları ve suçlarına yönelik görüşlerinin mağdur olma veya saldırya uğrama durumuna göre karşılaştırılmasına yönelik Tablo 4.8'de yapılan Mann-Whitney U testi sonucunda anlamlı bir fark bulunmamıştır ($p>.05$). Buna göre, mağdur olma veya saldırya uğrama durumu farketmeksizin öğretmen adaylarının bilişim kavramları ve suçlarına yönelik görüşleri aynı düzeydedir.

SONUÇ VE ÖNERİLER

Araştırmanın bu bölümünde araştırmaya katılan öğretmen adaylarının bilişim kavramları ve suçlarına yönelik sonuçlara ve önerilere yer verilmiştir.

Sonuçlar

Çalışma kapsamında, öğretmen adaylarının görüşlerini belirlemek amacı ile tutum ölçeği uygulanmıştır. Uygulanan tutum ölçeği sonucunda öğretmen adaylarının görüşlerine aşağıda yer verilmiştir.

Araştırma kapsamındaki öğretmen adaylarının cinsiyeti açısından internette mağdur olma veya saldırya uğrama durumları benzerlik göstermektedir. Karaca (2019)'un çalışmasında erkek öğrencilerin internette daha fazla mağdur olduğu görülmüştür.

Öğretmen adaylarının İnterneti daha uzun yıllar kullanan kişilerin mağdur olma veya saldırıya uğrama durumlarında artış olduğu görülmüştür. Yapılan başka bir araştırmda ise cep telefonu ve interneti daha uzun süredir ve daha çok kullanan öğrenciler, daha çok sanal zorbalık yapma eğiliminde olduğu ve de sanal zorbalığa daha çok maruz kaldığı belirtilmiştir (Doğan Çevirgen, 2018).

Araştırmaya dahil edilen öğretmen adaylarının internete bağlanma ile mağdur olma veya saldırya uğrama durumlarında arasında anlamlı farklılıklar görülmüştür. Öğretmen adaylarının internete bağlanmayanların genelde mağdur olduğu veya saldırya uğradığı görülmüştür. Araştırma kapsamında çalışmaya katılan öğretmen adayları yaygın olarak evden ve cep telefonundan internete bağlandıkları sonucuna ulaşılmıştır. Demirli ve Arslan'ın (2018)'deki çalışması ile paralellik göstermektedir.

Öğretmen adaylarının bilişim kavramları ve suçlarına yönelik genel olarak görüşlerinin orta düzeyde olduğu görülmektedir. Kuru ve Ocak (2016)'da kamu görevlilerine yapmış oldukları çalışmada siber güvenlikle ilgili olarak kariyerleri süresince yeterli eğitim verilmesi ve üniversitelerin müfredatıyla ilgili gerekli düzenlemelerin tereddüt edilmeden gözden geçirilmesi gerektiği sonucuna ulaşılmıştır. Gökmen ve Akgün (2015)'göre sınıf düzeyi farketmeksizin öğretmen adaylarının bilişim kavramları ve suçlarına yönelik görüşleri çalışma ile benzerlik göstermektedir. Gökmen ve Akgün (2016)'da yapmış oldukları çalışmada ise eğitim fakültesinde öğrenim gören öğretmen adaylarının bilişim suçu işledikleri, bilişim

suçuna maruz kaldıkları, bilişim suçu konusunda bilgilerinin olmadığı ve bir bilişim suçuyla karşılaştıklarında ne yapabileceklerini bilmediklerini tespit etmişlerdir.

Araştırmaya katılan kız ve erkek Öğretmen adaylarının bilişim kavramları ve suçlarına yönelik görüşleri aynı düzeydedir. Başka bir araştırmada ise, erkeklerin bilişim güvenliği konusundaki bilgilerinin kadınlara nazaran daha fazla olduğu belirtilmiştir (Gökmen ve Akgün, 2015).

Öğretmen adaylarının bilişim kavramları ve suçlarına yönelik görüşlerinin sınıf düzeyine göre incelendiğinde, farklı sınıf düzeyindeki öğretmen adaylarının bilişim kavramları ve suçlarına yönelik görüşlerinin aynı olduğu görülmüştür. Kamali'nin (2015) üniversite öğrencileri ile olan çalışmasında da benzer olarak siber mağdur olan öğrencilerin bu durumu sınıfa göre anlamlı bir farklılık göstermemiştir. Öğretmen adaylarının bilişim kavramları ve suçlarına yönelik görüşlerinin kaç yıldan beri internet kullandıklarına göre incelendiğinde, internet kullanım yılı fark etmeksizin öğretmen adaylarının bilişim kavramları ve suçlarına yönelik görüşlerinin aynı olduğu görülmüştür. Benzer şekilde yapılan başka bir araştırmada da geçen yıl zarfında tecrübe artsa da kişiler saldırıya uğrayabileceği belirtilmiştir (Karacı, Akyüz ve Bilgici, 2017).

Öğretmen adaylarının bilişim kavramları ve suçlarına yönelik görüşlerinin mağdur olma veya saldırya uğrama durumuna göre incelendiğinde, mağdur olma veya saldırya uğrama durumu farketmeksizin öğretmen adaylarının bilişim kavramları ve suçlarına yönelik görüşleri aynı düzeyde olduğu görülmüştür. Aslan (2019)'un yapmış olduğu araştırma sonucuna göre de, öğrencilerin siber farkındalık durumlarının İnternette saldırıya uğrama durumu ile anlamlı bir farklılık göstermediği görülmüştür.

Öneriler

Bu bölümde araştırmada elde edilen sonuçlar doğrultusunda öneriler sunulmuştur. Daha uzun yıllar internet kullanan kişiler daha çok mağdur olma veya saldırıya uğrama durumu yaşamıştır. Kullanım süreleri de gözetildiğinde siber zorba davranışlara maruz kalmamaları için kendilerine bu konuda eğitimler verilebilir.

Öğretmen adaylarının bilişim kavramları ve suçlarına yönelik genel olarak kararsızım diyerek bu konuda bilgi sahibi olma konusunda emin olmadıklarını

belirtmişlerdir. Üniversite eğitim programlarına bilişim kavramları ve suçlarına yönelik seçmeli dersler konabilir. Araştırmaya katılan öğretmen adayları yaygın olarak evden ve cep telefonundan internete girmektedirler. Öğretmen adaylarının okulda veya eğitim amaçlı internet kullanımlarının niçin fazla olmadığı araştırılabilir.

Öğretmen adaylarının çoğunluğu arkadaşlarla sohbet, video izlemek ve ödev-araştırma yapmak amacıyla internete bağlanmak istemektedirler. Önceliklerin neden eğitim olmadığı araştırılabilir. Öğretmen adaylarının internete bağlanmayanların genelde mağdur olduğu veya saldırıya uğradığı görülmüştür. Bu durumda daha önce internete bağlananların şimdi bağlanmadığı görülmüştür. Bunun nedenlerini açığa çıkaran aratırmalar yapılması gerekmektedir.

KAYNAKÇA

Akgün, Ö. ve Topal, M. (2015). Eğitim Fakültesi Son Sınıf Öğrencilerinin Bilişim Güvenliği Farkındalıkları: Sakarya Üniversitesi Eğitim Fakültesi Örneği. *Sakarya University Journal Of Education, 5*(2), 98-121.

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

Alikaşifoğlu, M. (2012). İnternet Kullanımı Ve Çocuk Ve Ergen Sağlığı Türk Pediatri Kurumu Tbmm Sunusu, 22 Eylül 2019 Tarihinde Https://Www.Tbmm.Gov.Tr Adresinden Alındı.

Allanson, P. B., Lester, R. R., ve Notar, C. E. (2015). A History Of Bullying. *International Journal Of Education And Social Science, 2*(12), 31-36.

Aslan, S. (2019). *Bilişim Teknolojileri Alanındaki Meslek Lisesi Öğrencilerinin Siber Güvenliğe Yönelik Bilgi Düzeylerinin Belirlenmesi* (Yüksek Lisans Tezi, Necmettin Erbakan Üniversitesi Eğitim Bilimleri Enstitüsü).

Ayas, T. (2014). Prediction Cyber Bullying With Respect To Depression, Anxiety and Gender Variables. *Online Journal Of Technology Addiction ve Cyberbullying*(1), 1-17.

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

Aydın, M. (2019). *Siber Zorbalıkla Karşılaşan Gençlerin Benlik Saygısı ve Stresle Baş Etme Yöntemlerinin İncelenmesi* (Yüksek Lisans Tezi, Maltepe Üniversitesi, Sosyal Bilimler Enstitüsü).

Bahar, A. (2018). Bilişim Suçları, İletişim ve Sosyal Medya. *İstanbul Aydın Üniversitesi Dergisi*, *10*(3), 1-36.

Baldi, S., Gelbstein, E. ve Kurbalija, J. (2003). *Hacktivism, cyber-terrorism and cyberwar: The activities of the uncivil society in cyberspace*. Diplo Foundation.

Balkı, E. ve Saban, A. (2009). Öğretmenlerin Bilişim Teknolojilerine İlişkin Algıları Ve Uygulamaları: Özel Esentepe İlköğretim Okulu Örneği. *İlköğretim Online, 8*(3).

Barrett, N. (1997). Digitalcrime: Policing The Cybernation. Koganpage.

Bauman, S. ve Newman, M. L. (2013). Testing Assumptions About Cyberbullying: Perceived Distress Associated With Acts Of Conventional And Cyber Bullying. *Psychology Of Violence, 3(*1), 27–38.

Belsey, B. (2004). Cyberbullying. Şubat 1, 2019 Tarihinde Http://Www.Cyberbullying.Ca/ Adresinden Alındı

Akbulut, B. B. (2000). "Bilişim Suçları", *Selçuk Üniversitesi Hukuk Fakültesi Dergisi*, 2000/1-2, S. 553.

Bilgi Teknolojileri ve İletişim Kurumu (2019). Bilişim Hukuku ve Bilişim Suçu. Https://İnternet.Btk.Gov.Tr/Bilisim-Hukuku-Ve-Bilisim-Sucu

Bocij, P. (2004). *Cyberstalking: Harassment in the Internet age and how to protect your family*. Greenwood Publishing Group.

Braga, A. A. (2005). Hot Spots Policing And Crime Prevention: A Systematic Review Of Randomized Controlled Trials. *Journal Of Experimental Criminology*, *1*(3): 317-342.

Bthk. (2019). Yasa Ve Düzenlemeler, Çalışılan Yasalar, Bilişim Suçları Yasa Tasarısı. Http://Www.Bthk.Org/Documents/Yasa-Duzenleme/Bilisimtasari.Pdf Adresinden 12/4/2019 Tarihinde Erişildi.

Calvete, E., Orue, I., Estévez, A., Villardón, L., ve Padilla, P. (2010). Cyberbullying İn Adolescents: Modalities And Aggressors' Profile. *Computers İn Human Behavior, 26*(5), 1128–1135.

Çevik, H. H. (2012). Bilişim, Teknoloji ve Çocuk: Sosyal Sorunlar ve Çözüm Önerileri, Polis Akademisi, Tbmm Sunusu, 22 Nisan 2016 Tarihinde Https://Www.Tbmm.Gov.Tr Adresinden Alındı.

Ching, J. (2010). *Cyberterrorism*. The Rosen Publishing Group, Inc.

Clutterbuck, R. (2013). *Terrorism, Drugs ve Crime in Europe after 1992*. Routledge., Toutledge, London, 1992;

Çubukcu, A., ve Bayzan, Ş. (2013). Türkiye'de dijital vatandaşlık algısı ve bu algıyı internetin bilinçli, güvenli ve etkin kullanımı ile artırma yöntemleri. *Middle Eastern ve African Journal of Educational Research, 5*, 148-174.

Doğan Çevirgen, B. (2018). *Geleneksel Akran Zorbalığı, Sanal Zorbalık Ve Ebeveyn İzlemesinin Bazı Değişkenler Açısından İncelenmesi*. Yüksek Lisans Tezi, Malatya: İnönü Üniversitesi Eğitim Bilimleri Enstitüsü.

Parker, D. B. (1989). Computer Crime: Criminal Justice Resource Manual .Justice, Washington.

Dedeoğlu, G. (2006). *Bilişim toplumu ve etik sorunlar*. İstanbul: Alfa Aktüel.

Demirli, C., ve Arslan, G. (2018). Ergenlerin İnternet Bağımlılığı Düzeylerinin İncelenmesi. *Istanbul Ticaret Üniversitesi Sosyal Bilimler Dergisi*, *17*(33), 49-64.

Dikmen, M., ve Tuncer, M. (2017). Akademisyenlerin siber zorbalığa yönelik algıları ve mücadele etme yöntemleri. *Dicle Üniversitesi Ziya Gökalp Eğitim Fakültesi Dergisi*, (31), 675-686.

Dolunay, A. ve Sağsan, M. (2019). Kişilik Haklarını İhlal Eden Siber Suçlar: Kktc Örneği. *Journal Of History Culture And Art Research, 8*(2), 433-449. Doi:Http://Dx.Doi.Org/10.7596/Taksad.V8i2.1949

Dülger, M. V. (2015). *Bilişim suçları ve internet iletişim hukuku*. Seçkin Yayıncılık.

Dülger, M. V. (2004) '' *Bilişim Suçları''* Seçkin Yayınevi, Ankara, 2004.

Dülger, M. V. (2004b) "Avrupa Konseyi ve Avrupa Birliği Düzenlemelerinde Çocuk Pornografisinin İnternet Aracılığıyla Yayılmasına Karşı Yapılan Düzenlemeler '' İbd, Cilt 78, Sayı 2004/4.

Emniyet Genel Müdürlüğü. (1999). Bilişim Suçları Ve Bilgi Güvenliği Kurulu Çalışma Raporu. Ankara.

Erçağ, E., ve Karabulut, M. (2017). Perceptions On Self-Efficacy Of Students Studying At Secondary Education İn The Trnc On Internet Security. *Revista De Educación A Distancia,* (54).

Ereş, F. (2009). Toplumsal bir sorun: suçlu çocuklar ve ailenin önemi. *Aile ve Toplum Eğitim, Kültür ve Araştırma Dergisi, Yıl11, Cilt5*, (17), 88-96.

Ersoy, A. F., ve Ersoy, A. (2008). İnternet ve çocuk hakları eğitimi. *Web: http://ietc2008. home. anadolu. edu. tr/adresinden*, *12*.

Geck, C. (2007). The generation Z connection: Teaching information literacy to the newest net generation. *Toward a 21st-century school library media program*, *235*, 2007.

Gibb, Z. G., ve Devereux, P. G. (2014). Who does that anyway? Predictors and personality correlates of cyberbullying in college. *Computers in Human Behavior*, *38*, 8-16.

Gökçearslan, Ş. (2016). Bilişim suçları ve etik. *Pegem Atıf İndeksi*, 127-148.

Gökler, R. (2009). Okullarda akran zorbalığı. *Uluslararası İnsan Bilimleri Dergisi*, *6*(2), 511-537.

Gökmen, Ö. F., ve Akgün, Ö. E. (2015). Bilgisayar ve Öğretim Teknolojileri Eğitimi Öğretmen Adaylarının Bilişim Güvenliği Bilgilerinin Çeşitli Değişkenlere Göre İncelenmesi. *Çukurova Üniversitesi Eğitim Fakültesi Dergisi, 44*(1), 61-84.

Gökmen, Ö. F., ve Akgün, Ö. E. (2016). Öğretmen Adaylarının Bilişim Suçlarına Yönelik Deneyimleri ve Bilişim Güvenliği Ders İçeriğine Yönelik Görüşleri/Teacher Candidates' Experiences Of Cyber Crime and Their Views For The Information Security Course Content. *Mustafa Kemal Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, 1*3(33), 178-193.

Gönültaş, M. (2019). *Üniversite Öğrencilerinin Siber Zorbalık ve Siber Mağduriyet Düzeylerinin Problemli İnternet Kullanım Düzeyleri Ve Demografik Değişkenlere Göre İncelenmesi*. Yüksek Lisans Tezi, Ege Üniversitesi, Sosyal Bilimler Enstitüsü, İzmir.

Gözler, A. ve Taşçı, U. (2015). Sınıf Öğretmenliği Bölüm Öğrencilerinin Bilişim Suçları. *Bilişim Teknolojileri Dergisi, 8*(3), 147.

Güler, N., Bayzan, Ş. ve Güneş, A.(2019). İnternette Çocuklara Yönelik Riskler ve Ailelerin Bilinçlendirme Faaliyetlerindeki Rolü. Erişim Tarihi: 10/10/2019, Https://Www.Guvenliweb.Org.Tr/Dosya/Fwdhr.Pdf

Gunay, O., Ozturk, A., Arslantas, E. E., ve Sevinc, N. (2018). Internet addiction and depression levels in Erciyes University students. *Dusunen Adam The Journal of Psychiatry and Neurological Sciences, 31*, 79-88.

Gündoğan, A. O. (2010). *Felsefeye Giriş.* İstanbul: Dem Yayınları.

Güneş, A. (2015). *Sosyal Ağ Kullanımı ve Güvenlik Algısı:* Temel Öğretim Öğrencileri Üzerine Bir Araştırma, Polis Akademisi Güvenlik Bilimleri Enstitüsü Güvenlik Stratejileri Ve Yönetimi Anabilim Dalı Doktora Tezi, Ankara.

Hürriyet, (2019). Dolandırılan Dekan. Erişim Tarihi: 12/04/2019. İnternet: Http://Arama.Hurriyet.Com.Tr/Arsivnews.Aspx ?İd=4818411

Jordan, T. (2008). *Hacking: Digital media and technological determinism*. Polity.

Jordan, T., ve Taylor, P. (2004). *Hacktivism and cyberwars: Rebels with a cause?*. Routledge.

Kahya, Y. (2015). Suç Teorileri Işığında Tü Rkiye'de Kaçakçılık Olgusu: Toplumsal Nedenleri, Boyutları ve Algısı. *Anadolu Üniversitesi Sosyal Bilimler Dergisi, 15*(3):159-178.

Kamali, A. (2015). Assessing cyberbullying in higher education. *Information Systems Education Journal, 13*(6), 43–53.

Karaca, H. (2019). *Ortaokul Öğrencilerinde Siber Zorbalık ve Mağduriyetle, İnternet Bağımlılığı, Aile İşlevleri ve Ebeveynlerin İnternet Kullanımı Arasındaki İlişkinin İncelenmesi.* Yüksek Lisans Tezi, Yakın Doğu Üniversitesi Sosyal Bilimler Enstitüsü.

Karacı, A., Akyüz, H. İ. ve Bilgici, G. (2017). Üniversite Öğrencilerinin Siber Güvenlik Davranışlarının İncelenmesi1. *Kastamonu Eğitim Dergisi, 25*(6), 2079-2094.

Kariuki, P. (2018). Cyber Security Education in the Fourth Industrial Revolution: The Case of South Africa. In *Handbook of Research on Information and Cyber Security in the Fourth Industrial Revolution* (pp. 517-530). IGI Global.

Koçak, H., ve Dandin, A. N. (2017). Toplumsal Ve Yönetsel Alanda Bilişim Teknolojilerinin Kriminal Etkileri. *Afyon Kocatepe Üniversitesi Sosyal Bilimler Dergisi*, *19*(1), 137-152.

Kokkinos, C. M., Baltzidis, E. ve Xynogala, D. (2016). Prevalence and Personality Correlates Of Facebook Bullying Among University Undergraduates. *Computers İn Human Behavior, 55,* 840–850. Doi:10.1016/J.Chb.2015.10.017.

Kruse Iı, W. G., ve Heiser, J. G. (2002) Computer Forensics: Incident Response Essentials. Addison-Wesley.

Kuru, H., ve Ocak, M. (2016). Determination of cyber security awareness of public employees and consciousness-rising suggestions. *Journal of Learning and Teaching in Digital Age*, *1*(2), 57-65.

Li, Q. (2007). Bullying İn The New Playground: Research İnto Cyberbullying And Cyber Victimisation. *Australasian Journal Of Educational Technology, 23*(4), 435-454.

Lindsay, M. ve Krysik, J. (2012). Online Harassment Among College Students. *Information, Communication ve Society, 15*(5), 703–719. Doi:10.1080/1369118x.2012.674959

Littman, J. (1996). The Fugitive Game: Online With Kevin Mitnick: The Inside Story Of The Great Cyberchase. Atlantic/Little, Brown.

Ludlow, P., ve Wallace, M. (2007). *The Second Life Herald: The virtual tabloid that witnessed the dawn of the metaverse*. MIT press.

MacDonald, C. D., ve Roberts-Pittman, B. (2010). Cyberbullying among college students: Prevalence and demographic differences. *Procedia-Social and Behavioral Sciences*, *9*, 2003-2009.

Maheshwari, H., Hyman, H. S., ve Agrawal, M. (2011). A Comparison of Cyber-Crime Definitions in India and the United States. In *Cyber Security, Cyber Crime and Cyber Forensics: Applications and Perspectives* (pp. 33-45). IGI Global.

Mahmutoğlu, F. S. (2002) "*Bankacılık Suçları Bağlamında Çıkar Amaçlı Suç Örgütü",* Avrupa Birliğine Uyum Süreci Bağlamında Organize Suçlulukla Mücadele, Panel, 5 Ekim 2001, Bildiriler ve Tartışmalar, Yönetici Kayıhan İçel, İstanbul.

Marcum, C. D., ve Higgins, G. E. (2019). Cybercrime. In *Handbook on Crime and Deviance* (pp. 459-475). Springer, Cham.

Miller, R. L. (2012). *Business Law Today, Standard: Text ve Summarized Cases*. Cengage Learning.

Millhorn, J. (1999). *Student's Companion to the World Wide Web: Social Sciences and Humanities Resources*. Scarecrow Press.

Dolu, O. (2010). *Suç teorileri: Teori, araştırma ve uygulamada kriminoloji*. Seçkin.

Gredler, G. R. (2003). Olweus, D.(1993). Bullying at school: What we know and what we can do. Malden, MA: Blackwell Publishing, 140 pp., $25.00. *Psychology in the Schools*, *40*(6), 699-700.

Ozansoy, K., Altınay, Z., ve Altınay, F. (2018). Developing Strategies to Prevent "Cyber-Bullying". *Eurasia Journal of Mathematics, Science and Technology Education*, *14*(5), 1925-1929.

Örs, F. (2010). Küresel Medya Ortamında Yaşanan Etik Sorunlar Ve Uluslararsı Düzenlemeler. *Journal Of Yasar University*, 20(5), 3443-3452.

Özaydın, B. (2010). Teknoloji kültürü ve etik, Süleyman Demirel Üniversitesi. *Fen Bilimleri Enstitüsü, basılmamış yüksek lisans tezi, Isparta*.

Özel, C. (2001). Bilişim Suçları İle İletişim Faaliyetleri Yönünden Türk Ceza Kanunu Tasarısı. *ĐBD, Yıl, 2*.

Parker, D. B. (1968). Rules Of Ethics İn İnformation Processing. *Communications Of The Acm, 11*(3), 198-201.

Patchin, J. W., ve Hinduja, S. (2008). Cyberbullying: An Exploratory Analysis Of Factors Related To Offending And Victimization. *Deviant Behavior, 29*(2), 129-156.

Porterfield, J. (2011). *Careers as a Cyberterrorism Expert*. The Rosen Publishing Group, Inc.

Prensky, M. (2001). Digital natives, digital immigrants. *On the horizon*, *9*(5).

Quayle, E., ve Taylor, M. (2003). Child pornography and the Internet: Perpetuating a cycle of abuse. *Deviant Behavior*, *23*(4), 331-361.

Perry, R. L. (1986). Computer Crime. New York: Franklin Watts.

Raskauskas, J. And Stoltz, A. D. (2007). Involvement İn Traditional And Electronic Bullying Among Adolescents. *Developmental Psychology, 43*(3), 564–575. Doi:10.1037/00121649.43.3.564

Ratcliffe, J. H. (2004). The Hotspot Matrix: A Framework For The Spatio- Temporal Targeting Of Crime Reduction. *Police Practice And Research, 5*(1): 5-23.

Sevindik, T. (2011). Bilişim ve Etik Ders Notları. Http://Www.Yarbis.Yildiz.Edu.Tr/Web/Userannouncementsfiles/Dosya2f 00c8b17de37 3c9f729e1440b895329.Pdf Adresinden Alındı

Shrivastava, G., Sharma, K., ve Dwivedi, A. (2012). Forensic Computing Models: Technical Overview. *Computer Science ve Information Technology, 5,* 207-216. Doı : 10.5121/Csit.2012.2222

Sieber, U. (1986). *The international handbook on computer crime: computer-related economic crime and the infringements of privacy*. John Wiley ve Sons, Inc..

Slonje, R., ve Smith, P. K. (2008). Cyberbullying: Another Main Type Of Bullying? *Scandinavian Journal Of Psychology, 49*(2), 147–154.

Smith, P., Mandavi, J., Carvalho, M., Fisher, S., Russell, S. ve Tippett, N. (2008). Cyberbullying: Its Nature And İmpact İn Secondary School Pupils. *The Journal Of Child Psychology And Psychiatry. 49*, 376-385.

Sönmez, Y. (2018). *Günümüz İnternet Ortamında Bilişim Suçları Ve Türkiye'deki İnternet Haber Sitelerine Yansımaları*. Yüksek Lisans Tezi, Marmara Üniversitesi Sosyal Bilimler Enstitüsü.

Statista. (2016). Daily İnternet Usage İn Turkey. Https://Goo.Gl/Cwpfqw (Erişim Tarihi: 15.08.2017).

Subramaniam, S. R. (2017). Cyber security awareness among Malaysian pre-university students. E. *Proceeding of the 6th Global Summit on Education*, 1-14.

Tanrıkulu, C. (2007). Bilişim Teknolojilerinin Kullanılmasının Hukuksal Boyutu. *TBD Kamu-BİB Kamu Bilişim Platformu IX. Antalya*.

Taylor, P. A. (2014). "Hacktivizm" (Çev: Mustafa Ali Minarlı) (Ed: Mukadder Çakır); Yeni Medyaya Eleştirel Yaklaşımlar, Doğu Kitabevi, İstanbul.

TCK. (2014).Türk Ceza Kanunu. Erişim Tarihi : 12/4/2019. Http://Www.Mevzuat.Gov.Tr/Mevzuatmetin/1.5.5237.Doc

TDK (2019). Guncel Turkce Sozluk. Erişim Tarihi: 12 Ekim 2019, Http://Www.Tdk.Gov.Tr

The Cybercrime And The European Union, (2019). Council Of Europe Https://Rm.Coe.İnt/16802e6ffc, Erişim Tarihi: 05.10.2019

Thornburgh, D. ve Lin, H. (2002). *Youth, pornography and the Internet* (p. 388). Washington, DC: National Academy Press.

Topal, A. D., Geçer, A. K., Akkaya, O., Güzel, Y. E., ve Of, M. (2019). Öğretmen Adaylarının Bilişim Suçları İle İlgili Tutum ve Bilgi Düzeylerinin İncelenmesi. *Pamukkale Üniversitesi Eğitim Fakültesi Dergisi*, *45*(45), 159-174.

Torun, Ö. (2007). *Resmi Ortaöğretim Kurumlarında Öğrenim Gören Öğrencilerin İnternet Etiğine İlişkin Algılarının İncelenmesi.* Yüksek Lisans Tezi, Marmara Üniversitesi Eğitim Bilimler Enstitüsü, İstanbul.

Us President's Council On Integrity And Efficiency Prevention Cmtte, ve United States Of America. (1986). Computers: Crimes, Clues And Controls--A Management Guide.

Uysal, Ö. (2006). Öğretmen Adaylarının Bilgisayar Etiğine İlişkin Görüşleri. Yüksek Lisans Tezi, Anadolu Üniversitesi Eğitim Bilimleri Enstitüsü, Eskişehir.

Varol, C. ve Varol, N. (2001). Gençliğin İnternet Kullanımına Yaklaşımı Ve İnternet Kafeler. Btıe Konferansı. 3-5 Mayıs 2001. Ankara.

Whittaker, E. ve Kowalski, R. M. (2015). Cyberbullying via social media. *Journal Of School Violence*, *14*(1), 11–29. Doi:10.1080/15388220.2014.949377

Willard, N. (2007). Cyberbullying And Cyberthreats. Şubat 8, 2019 Tarihinde Http://Books.Google.Com.Tr/Books?İd=Vytdg2btnl4cvePrintsec=FrontcoverveDq=Cyberbullying+And+Cyberthreats:Responding+To+The+Challenge+Of+Online+Social+Aggression,+Threats,+And+Distress,veHl=TrveSa=XveEi=3go9u9ogn6lb7abe_4dacqveVed= 0cb4q6aewaa Adresinden Alındı

Willard, N., E. (2007). Cyberbullying And Cyberthreats: Responding To The Challenge Of Online Social Aggression, Threats And Distress. Research Press.
Http://Books.Google.İt/Books?İd=Vytdg2btnl4cvePrintsec=FrontcoverveDq=Nancy+WillardveHl=İtveEi=Bkdxtufag8jahafot9w1dgveSa=XveOi=Book_ResultveCt=ResultveResnum=1veVed=0cdeq6aewaa

Yalçın, N. ve Gürbüz, F. (2015, Şubat). Sosyal Ağlarda İşlenen Suçlar, Facebook Sosyal Ağı Örneği. Akademik Bilişim Konferansı, Eskişehir.

Yaşa, H. ve Pınarbaşı, T. E. (2018). Sosyal Medyada Bir Siber Zorbalık Örneği: Mina Başaran.

Yaycı, E. (2007). Bilişim Suçları. Gazi Üniversitesi Sosyal Bilimler Enstitüsü, Basılmamış Yüksek Lisans Tezi.

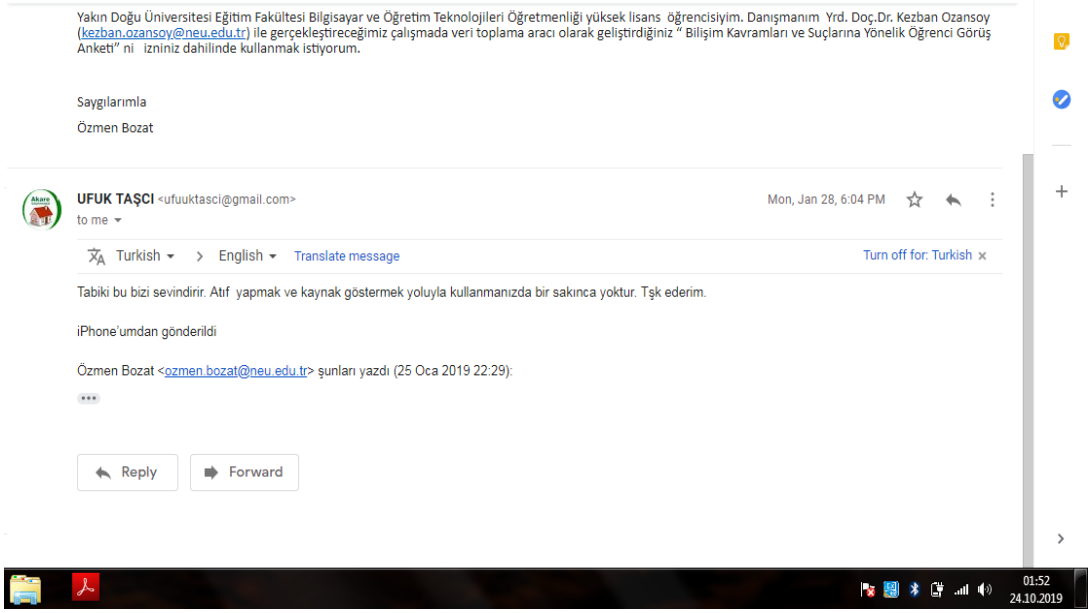
Yazıcıoğlu , R. (1997) ‘’ Bilgisayar Suçlar Kriminolojik Sosyolojik ve Hukuki Boyutları İle ‘’ Alfa Yayınevi, İstanbul, 1997.

Yetim, S. (2015). Siber zorbalık, Türkiye ve ABD karşılaştırması (ABD v. Drew dosyası). *TBB Dergisi, 120,* 325-84.

Yılmaz, E., Şahin, Y. L., ve Akbulut, Y. (2016). Öğretmenlerin Dijital Veri Güvenliği Farkındalığı. *Sakarya University Journal Of Education, 6*(2), 26-45.

EKLER

Ek – 1: Anket Kullanım İzni



Yakın Doğu Üniversitesi Eğitim Fakültesi Bilgisayar ve Öğretim Teknolojileri Öğretmenliği yüksek lisans öğrencisiyim. Danışmanım Yrd. Doç.Dr. Kezban Ozansoy (kezban.ozansoy@neu.edu.tr) ile gerçekleştireceğimiz çalışmada veri toplama aracı olarak geliştirdiğiniz " Bilişim Kavramları ve Suçlarına Yönelik Öğrenci Görüş Anketi" ni izniniz dahilinde kullanmak istiyorum.

Saygılarımla

Özmen Bozat

UFUK TAŞCI <ufuuktasci@gmail.com> Mon, Jan 28, 6:04 PM

to me

Turkish › English Translate message Turn off for: Turkish

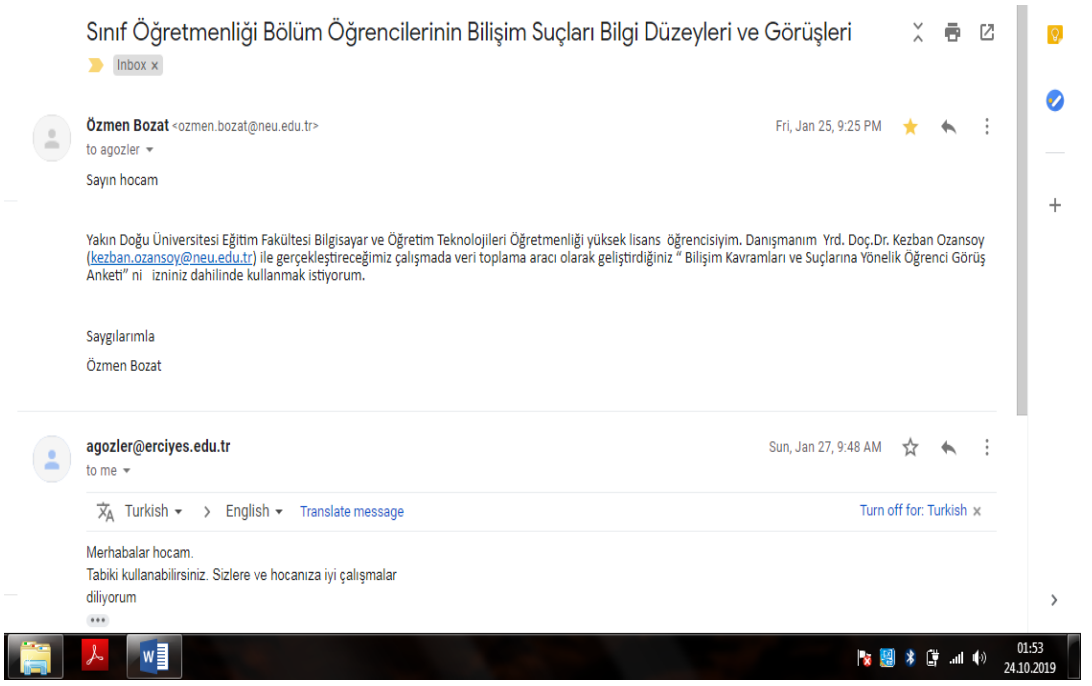
Tabiki bu bizi sevindirir. Atıf yapmak ve kaynak göstermek yoluyla kullanmanızda bir sakınca yoktur. Tşk ederim.

iPhone'umdan gönderildi

Özmen Bozat <ozmen.bozat@neu.edu.tr> şunları yazdı (25 Oca 2019 22:29):

Reply Forward

01:52 24.10.2019



Sınıf Öğretmenliği Bölüm Öğrencilerinin Bilişim Suçları Bilgi Düzeyleri ve Görüşleri

Inbox ×

Özmen Bozat <ozmen.bozat@neu.edu.tr> Fri, Jan 25, 9:25 PM

to agozler

Sayın hocam

Yakın Doğu Üniversitesi Eğitim Fakültesi Bilgisayar ve Öğretim Teknolojileri Öğretmenliği yüksek lisans öğrencisiyim. Danışmanım Yrd. Doç.Dr. Kezban Ozansoy (kezban.ozansoy@neu.edu.tr) ile gerçekleştireceğimiz çalışmada veri toplama aracı olarak geliştirdiğiniz " Bilişim Kavramları ve Suçlarına Yönelik Öğrenci Görüş Anketi" ni izniniz dahilinde kullanmak istiyorum.

Saygılarımla

Özmen Bozat

agozler@erciyes.edu.tr Sun, Jan 27, 9:48 AM

to me

Turkish › English Translate message Turn off for: Turkish

Merhabalar hocam.
Tabiki kullanabilirsiniz. Sizlere ve hocanıza iyi çalışmalar diliyorum

01:53 24.10.2019

Ek – 2: "Bilişim Kavramları ve Suçlarına Yönelik Öğrenci Görüş Ölçeği"

Bilişim Kavramları ve Suçlarına Yönelik Tutum Anketi

Sayın Gönüllü;

Yakın Doğu Üniversitesi, Eğitim Bilimleri Enstitüsü, Bilgisayar ve Öğretim Teknolojileri Eğitimi Anabilim Dalı, Yüksek Lisans Tezi kapsamında planlanmış olan yukarıda adı yazılı araştırmaya katılmak üzere davet edilmiş bulunuyorsunuz. Bu araştırmada yer almayı kabul etmeden önce, araştırmanın ne amaçla yapılmak istendiğini anlamanız ve kararınızı bu bilgilendirme çerçevesinde özgürce vermeniz gerekmektedir. Aşağıdaki bilgileri lütfen dikkatlice okuyunuz, sorularınız olursa sorunuz ve açık yanıtlar isteyiniz. Ölçek maddelerinin cevaplanması 15-20 dakikanızı alacağı öngörülmektedir.

Bilişim suçlarının günümüz dünyasında ne derece yaşandığını ve öğretmen adaylarının bu konu hakkında ne derece bilgilerinin olduğunu tespit etmek amaçlı olduğunu belirtmek isterim. Bilişim suçu kısaca şöyle tanımlanabilir. Ağ ve bilgisayar teknolojileri vasıtasıyla gerçekleştirilen ve yasalar karşısında kişilerin hakkının gasp edilmesi ya da rahatsızlık verilmesi gibi gerekçelerle resmi olarak suç niteliği taşıyan, yasalar tarafından önceden cezalarının belirlendiği suçlardır.

Bu araştırmada yer almak tümüyle sizin isteğinize bağlıdır. Araştırmada yer almayı reddedebilirsiniz ya da başladıktan sonar yarıda bırakabilirsiniz. Bu araştırmanın sonuçları bilimsel amaçlarla kullanılacaktır. Araştırmadan çekilmeniz ya da araştırmacı tarafından araştırmadan çıkarılmanız halinde, sizle ilgili veriler kullanılmayacaktır. Ancak veriler birkez anonimleştikten sonar araştırmadan çekilmeniz mümkün olamayacaktır. Sizden elde edilen tüm bilgiler gizli tutulacak, araştırma yayınlandığında da varsa kimlik bilgilerinizin gizliliği korunacaktır. Aşağıdaki soruları doldurduğunuzda çalışmayı onaylamış olursunuz.

Yukarıda yer alan araştırmaya başlamadan once gönüllülere verilmesi gereken bilgileri içeren metni okudum. Eksik kaldığını düşündüğüm konularda sorularımı araştırmacılara sordum ve doyurucu yanıtlar aldım. Yazılı ve sözlü olarak tarafıma sunulan tüm açıklamaları ayrıntılarıyla anladığım kanısındayım. Çalışmaya katılmayı isteyip istemediğim konusunda karar vermem için yeterince zaman tanındı.

Bu koşullar altında, araştırma kapsamında elde edilen şahsıma ait bilgilerin bilimsel amaçlarla kullanılmasını, gizlilik kurallarına uyulmak kaydıyla sunulmasını ve yayınlanmasını, hiçbir baskı ve zorlama altında kalmaksızın, kendi özgür irademle kabul ettiğimi beyan ederim.

Araştırmacı Bilgileri

Yrd.Doç.Dr. KezbanOzansoy Bilgisayar ve Öğretim Teknolojileri Eğitimi Bölümü Öğretim Üyesi, Yakın Doğu Üniversitesi Tel: 0542 865 17 55 E-mail: kezban.ozansoy@neu.edu.tr	ÖzmenBozat Bilgisayar ve Öğretim Teknolojileri Eğitimi Bölümü YL Öğrencisi Yakın DoğuÜniversitesi Tel: 0548 852 99 90 E-mail: ozy.ultiman@gmail.com

KİŞİSEL SORULAR

1. **Cinsiyetiniz.**
   ( )Kadın ( )Erkek
2. **Yaş:**.....
3. **Branşınız.:**.....
4. **Kaçıncı sınıfsınız:**
   ( ) 1.sınıf ( ) 2.sınıf ( ) 3.sınıf ( ) 4.sınıf
5. **İnternete nerelerden bağlanıyorsunuz? (Birden fazla seçenek işaretleyebilirsiniz.)**
   ( )Bağlanmıyorum
   ( )Evden
   ( )İnternet Kafeden
   ( )Cep Telefonuyla
   ( )Okulda BT Sınıfından
   Diğer .....
6. **Kaç yıldan beri internet kullanıyorsunuz?**
   ( )0-1 yıldır kullanıyorum
   ( )1-2 yıldır kullanıyorum
   ( )2-3 yıldır kullanıyorum
   Diğer .....
7. **İnterneti hangi amaçlarla kulanıyorsunuz? (Birden fazla seçenek işaretleyebilirsiniz.)**
   ( )Oyun oynamak
   ( )Video izlemek
   ( )Arkadaşlarıyla sohbet etmek
   ( )Hayatında ne olup bittiğini paylaşmak
   ( )Ödev yapmak
   ( )Araştırma yapmak
   Diğer .....
8. **İnternete hangi sıklıkla giriyorsunuz.**
   Günde 0-1 saat ( )
   Günde 1-2 saat ( )
   Günde 2-3 saat ( )
   Diğer .....
9. **İnternette ailemin kredi kartı ile alışveriş yaparım.**
   ( )Evet ( )Hayır
10. **İnternet ortamında sizi mağdur edecek bir olayla veya saldırıyla karşılaştınız mı?**
    ( )Evet ( )Hayır
11. **Aşağıdakilerden hangisine maruz kaldınız. (Birden fazla seçenek işaretleyebilirsiniz.)**
    ( )Elektronik posta yolu ile
    ( )Yazılı mesaj yolu ile
    ( )Resimli mesaj yolu ile
    ( )Anında karşılıklı mesaj ile
    ( )Sosyal iletişim ağları ile
    ( )Sohbet odaları ile
    ( )Sanal ortamdaki oyunlar esnasında
    Diğer.....

	Bilişim Suçlarına Yönelik Tutum Maddeleri	**Hiç Katılmıyorum**	**Katılmıyorum**	**Kısmen Katılıyorum**	**Katılıyorum**	**Tamamen Katılıyorum**
1	Mail adresimin ya da benzeri sayfalarının şifresinin kırılması durumunda ne yapacağımı bilirim.					
2	Lisans eğitimimizde aldığımız bilgisayar derslerinde bilişim suçlarına yönelik bilgiler verilmelidir.					
3	Mail adreslerimin şifrelerini samimi arkadaşlarım bilir.					
4	İnternet dolandırıcılığı hakkında yeterli bilgiye sahip değilim.					
5	Mail ya da kendime ait kişisel kullanım sayfalarımın başkalarının eline geçmesi beni çok üzer.					
6	Bana gelen virüslü maili fark edebilirim.					
7	Tanımadığım kişileri mail adresime ve kişisel sayfalarıma eklemem.					
8	Kredi kartımla internetten rahatlıkla alışveriş yaparım.					
9	Bilgisayarım virüslere karşı korunaklıdır.					
10	Basın ve medya internet suçları hakkında insanları bilgilendiriyor.					
11	Herhangi bir bilişim suçuna şahit olduğumda ne yapacağımı bilirim.					
12	Bilişim suçlarına verilen cezaların ağır olması gerekmektedir.					
13	Bilişim suçlarına yönelik bilgilendirmenin ilköğretimden itibaren başlaması gerekmektedir.					
14	Bilişim suçları gözde büyütülecek düzeyde tehlikeli değildir.					
15	Bilişim suçlarına yönelik, öğrencilere konferanslar veya seminerler düzenlenmelidir.					
16	Bilişim suçlarını işleyebilen insanlar çok zeki insanlardır.					

Ek – 3: Yakın Doğu Üniversitesi Bilimsel Araştırmalar Etik Kurul Onayı

YAKIN DOĞU ÜNİVERSİTESİ

BİLİMSEL ARAŞTIRMALAR ETİK KURULU

12.12.2019

Sayın Özmen Bozat

Bilimsel Araştırmalar Etik Kurulu'na yapmış olduğunuz YDÜ/EB/2019/314 proje numaralı ve **"Bilişim Suçlarına Yönelik Eğitim Fakültesi Öğretmen Adaylarının Tutumları"** başlıklı proje önerisi kurulumuzca değerlendirilmiş olup, etik olarak uygun bulunmuştur. Bu yazı ile birlikte, başvuru formunuzda belirttiğiniz bilgilerin dışına çıkmamak suretiyle araştırmaya başlayabilirsiniz.

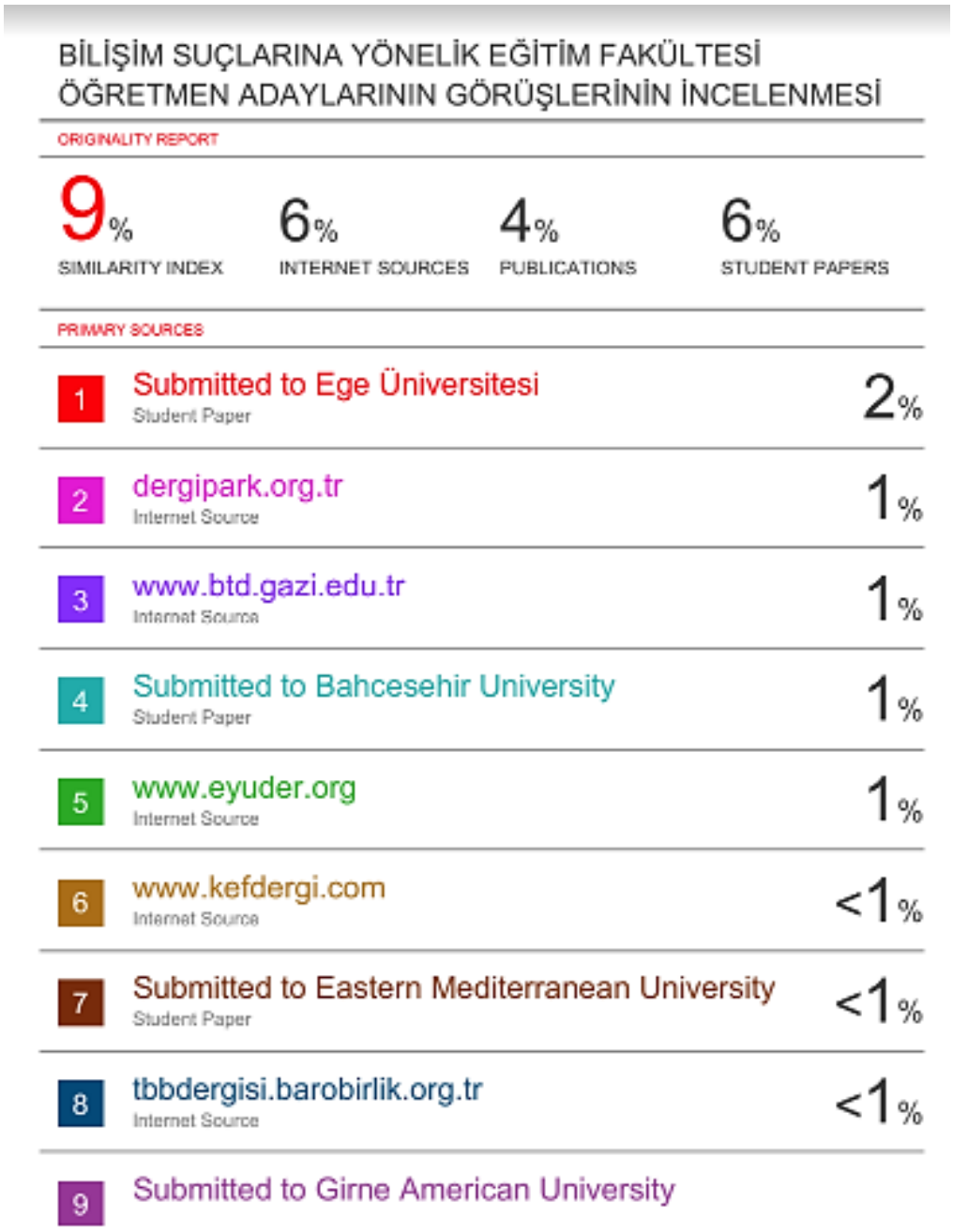
Doçent Doktor Direnç Kanol

Bilimsel Araştırmalar Etik Kurulu Raportörü

Direnç Kanol

Not: Eğer bir kuruma resmi bir kabul yazısı sunmak istiyorsanız, Yakın Doğu Üniversitesi Bilimsel Araştırmalar Etik Kurulu'na bu yazı ile başvurup, kurulun başkanının imzasını taşıyan resmi bir yazı temin edebilirsiniz.

İNTİHAL RAPORU



BİLİŞİM SUÇLARINA YÖNELİK EĞİTİM FAKÜLTESİ ÖĞRETMEN ADAYLARININ GÖRÜŞLERİNİN İNCELENMESİ

ORIGINALITY REPORT

9%	6%	4%	6%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to Ege Üniversitesi Student Paper	2%
2	dergipark.org.tr Internet Source	1%
3	www.btd.gazi.edu.tr Internet Source	1%
4	Submitted to Bahcesehir University Student Paper	1%
5	www.eyuder.org Internet Source	1%
6	www.kefdergi.com Internet Source	<1%
7	Submitted to Eastern Mediterranean University Student Paper	<1%
8	tbbdergisi.barobirlik.org.tr Internet Source	<1%
9	Submitted to Girne American University	