Sınıf Öğretmenliği Bölüm Öğrencilerinin Bilişim Suçları Bilgi Düzeyleri ve Görüşleri

Alpaslan GÖZLER[1], Ufuk TAŞCI[2]

[1]Erciyes Üniversitesi Eğitim Fakültesi İlköğretim Bölümü Kayseri, Türkiye
[2]Elmadağ Polis Meslek Yüksek Okulu Ankara, Türkiye
agozler@erciyes.edu.tr, ufuuktasci@gmail.com.tr
(Geliş/Received: 03.04.2015; Kabul/Accepted: 23.06.2015)
DOI: 10.17671/btd.11974

Özet – Bilişim suçları, günümüzde bilişim teknolojilerinin gelişimiyle ve artan oranda kullanımıyla ortaya çıkan suç türüdür. Bu suçların sadece kolluğun önleyici faaliyetleriyle önlenmeye çalışılması yeterli değildir. Toplumun ve bireylerin eğitilmesi konusunda önemli roller oynayan öğretmenlerin, bilişim suçlarının önlenmesi konusunda da etkin olması, bireyleri bilinçlendirmesi gerektiği düşünülürken, aynı zamanda öğretmenlerinde bu konuda bilinçli olmaları gerektiği düşünülmektedir. Çalışmada öğretmen yetiştiren bölümler arasında yer alan Sınıf Öğretmenliği Anabilim dalındaki öğrencilerin dolayısıyla sınıf öğretmenleri adaylarının bilişim suçları hakkındaki görüşleri ve bu suçları algılama düzeyleri ölçülmeye çalışılmıştır. Çünkü sınıf öğretmenleri, eğitimin anaokulundan sonra ilk basamağında yer almakta, bireylerin eğitim çağına atıldığı ilk yıllardaki önemli rol modelleri olmakta, bireylere verdikleri mesajlar önemli olmaktadır. Bu durum verdikleri mesajların ağırlığını arttırmaktadır. Araştırma grubunu, 2013–2014 Öğretim Yılı Güz yarıyılında Erciyes Üniversitesi İlköğretim Bölümü Sınıf Öğretmenliği Anabilim dalında eğitim gören 205 öğrenci oluşturmaktadır. Araştırma sonucunda, öğrencilerin bilişim suçları konusunda bilinç düzeylerinin ve bu suçlara karşı önleyici tutum sergileme seviyelerinin düşük olduğu, bilişim suçları konusunda güvenlik birimlerince ve diğer ilgili kurumlarca bilgilendirilmeye ihtiyaç duydukları tespit edilmiştir.

Anahtar Kelimeler *– Bilişim, Suç, Aday Öğretmenler.*

Views and Knowledge Levels of Classroom Teaching Department Students About Cyber Crımes

Abstract - Cyber crime is any crime that has emerged and increased with the development and use of today's information technologies. It is not sufficient to prevent this crime only through law enforcement efforts. On the one hand; it is thought that teachers who play key roles in educating individuals and societies should be active and raise awareness among the individuals for the prevention of Cyber crimes; on the other hand, they themselves should be well-informed about the prevention of Cyber crimes. The current study aimed at measuring opinions and perception levels of Cyber crimes of the teacher-candidates of classroom teaching department; one of the departments that train teacher-candidates. Classroom teaching follows pre-school education in the formal education process; therefore, classroom teachers become significant role models during the early years of individuals' education and give important messages to the individuals. The study group was composed of 205 students who studied at Department of Classroom Teaching Kayseri, Faculty of Education, Erciyes University during the fall semester of 2013-2014 academic year. In light of the study results; it was found out that students' consciousness levels about Cyber crimes and level of showing preventive behaviors against these crimes were low and they needed being informed by security units and other relevant institutions about Cyber crimes.

Keywords– Informatics, Crime, Candidate, Teachers.

1. GİRİŞ (INTRODUCTION)

Öğretmenlik, toplumun tüm sektörlerinde çalışan insanların meslek sahibi olmasında, eğitilmesinde, toplumsal kültür ve değerlerin insanlara aktarılmasında ve nitelikli insan gücünün yetiştirilmesinde etkili olan bir meslektir [1]. Eğitim sisteminin ilk basamağı olan ilköğretim dönemi, bireyi yaşamına hazırlamada temel

teşkil etmektedir. Bu yıllarda kazanılan bilgi ve beceriler, üst kademede kazanılacak öğrenmeler için ön koşul niteliği taşıması nedeniyle sınıf öğretmenlerinin yetiştirilmesi ayrı bir önem taşımaktadır [2].

Teknoloji, günümüzün bilgi toplumlarında, insan yaşamının temel dinamiğini oluşturmaktadır [3]. Bilişim teknolojileri, sürekli ve artan biçimde gelişmektedir. Yeni teknolojik yeniliklerin kısa süre içerisinde demode olduğu görülmektedir. Bu gelişme ve yenilikler insanları ve toplumları etkilemekte, yeniliği icat eden insanoğlunu kendi icadının peşinde koşan öznelere çevirmektedir.

Teknolojik gelişmenin en son çıkardığı suç tipi bilişim suçları olarak adlandırılmaktadır. Bilişim suçlarının mağdurları arasında toplumda eğitim seviyesi yüksek kişilerin olması oldukça dikkat çekici olup [4] bilişim suçları konusunda yeterli bilince sahibi olmayan bireylerin mağdur olma ihtimalinin oldukça yüksek olduğu söylenebilir.

Bilişim suçlarının önlenmesi ve suçları işleyenlerin soruşturulması, kolluk kuvvetleri olarak polis ve jandarma tarafından yapılmasını gerektirir. Ancak kolluk kuvvetlerinin bilişim suçlarını önleme ve aydınlatma faaliyetinin yeterli olmayacağı düşünülmekte, toplumda oynadığı önemli roller nedeniyle eğitim lideri olarak kabul edilen sınıf öğretmenleri tarafından, bilişim suçu ve diğer ilgili kavramların yeterli düzeyde bilinmesi yoluyla bilişim suçları konusunda genç nesli bilinçlendirmeye yönelik yeni ve önemli sorumluluklar yüklenmesi gerektiği düşünülmektedir.

2. BİLİŞİM SUÇLARI (CYBER CRIMES)

Bilişim kavramının bir çok tanımı bulunmasına rağmen, tanımlarda geçen ortak özellikler; bilginin aktarılması, organize edilmesi, saklanması, tekrar elde edilmesi, değerlendirilmesi ve dağıtımı için gerekli kuram ve yöntemler ile bilgiyi kaynağından alıp kullanıcıya aktaran ve genel sistem bilimi, sibernetik, otomasyon ile insanın çalışma çevrelerindeki yerinde ve zamanında kullanılan, insanoğlunun teknik, ekonomik ve toplumsal alanlardaki iletişiminde kullandığı ve bilimin dayanağı olan bilginin, özellikle elektronik makineler aracılığı ile düzenli ve ussal biçimde işlenmesi teknolojileri temel alan bilgi sistemleri, şebekeleri, işlevleri, süreçler ve etkinlikler olarak sıralanabilmektedir [5,6,7,8].

Suç, insanlarda bulunan çeşitli ihtiraslarla beraber toplum halinde yaşamanın ortaya çıkardığı türlü sosyal çelişkiler, uyumsuzluklar sonucu ortaya çıkmaktadır [9]. Son dönemde teknolojik gelişmeye dayalı olarak ortaya çıkan bilişim suçları, oldukça yeni bir suçu tipi olarak görülebilir. Türkiye'nin internete ilk defa 12 Nisan 1993 yılında bağlandığını ifade etmek gerekirse, bu alanda Türkiye'nin yeni bir teknolojiyle karşılaşmış olduğu söylenebilir [10].

Bilişim suçları; bilişim ortamında işlenebilen, klasik suçlar arasında sayılmayan, bilgisayar ve internete özgü suçlar olarak *dar anlamda* suçlar ile bilişim sistemleri kullanılarak veya bilişim sistemlerinden yararlanılarak işlenen *geniş anlamda bilişim suçları* klasik suçlar olarak ikiye ayrılmaktadır [11].

Bilişim suçları konusunda üzerinde anlaşılan bir tanım yoktur. Hekim ve Başıbüyük, bazı çalışmalarda bu suçların; *siber suç, bilgisayar suçu, elektronik suç, dijital suç veya ileri teknoloji suçları* gibi kavramlarla ifade edildiği belirtmektedir [12].

Perry bilişim suçlarını; "bilginin, programların, servislerin, ekipmanların veya haberleşme ağlarının yıkımı, hırsızlığı, yasadışı kullanımı, değiştirilmesi veya kopyalanması" [13], Parker, "işlendiği takdirde faile çıkar elde ettirecek bir şeyler kazandıran ya da kurbana kaybettiren, aynı zamanda bilgisayar kullanımı veya teknolojisi bilgisini içeren herhangi bir kasıtlı davranış" [14], Strothcamp tarafından da; "bilgisayarın kişisel çıkar elde edinimi için kullanılması" [15] şeklinde tanımlamaktadır.

Polisiye bir bakış açısıyla bilişim suçları ise, klasik suç türlerinden farklı olarak bilgi ve iletişim teknolojilerin gelişimi ile ortaya çıkmış, bilişim, sistemlerine yönelik sistemin çalışmasını engelleme, sisteme yetkisiz erişim, sistemden bilgi çalma veya silme gibi suç türleri olarak tanımlanmaktadır [16].

En geniş kabul gören tanım Avrupa Ekonomik Topluluğu Uzmanlar Komisyonu tarafından 1983 tarihinde Paris Toplantısı'nda yapılmış; *"Bilgileri otomatik isleme tabi tutan veya verilerin nakline yarayan bir sistemde gayri kanuni, gayri ahlaki veya yetki dışı gerçekleştirilen her türlü davranış"* [17] şeklinde tanımlanmıştır.

Bilişim suçlarının, Fransa'da 1801 yılında Joseph Marie Jacquard'ın dokuma tezgâhında işlemi otomatikleştirmek için ürettiği delikli kartların, sektörde çalışan işçilerin istihdamını etkileyeceği endişesiyle yine işçilerin sabotajıyla karşılaşmasıyla başladığı düşünülmektedir [18]. Fakat kayıtlara giren ilk bilişim suçu, 1966'da Minneapolis Tribüne gazetesinde yayınlanan "Bilgisayar Uzmanı Banka Hesabında Tahrifat Yapmakla Suçlanıyor" isimli makaleyle kayıtlara geçmiştir [5].

1970'li yıllarda "phreaker" adı verilen ve telefon sistemlerine girip bu yolla bedava telefon görüşmeleri yapan telefon hacker'ları ile birlikte bu suçlar kamuoyunda duyulmaya başlamıştır [19]. 1973 yılında, kayıtlara geçen en büyük bilişim suçu Los Angeles eyaletinde gerçekleşmiştir. Bu olay "Equity Funding" adındaki sigorta şirketinde 64.000 sahte müşteri kaydı yapılmasıyla gerçekleştirilen dolandırıcılık olayıdır [20].

Bilgisayar ağlarının zamanla gelişmesi, bilişim suçlarının elektronik ortamlara taşınmasına neden olmuştur.

Saldırganlar dosyaları kopyalamış, silmiş, sistemi çökertmiş ya da sistemlere zarar vermişlerdir. Amerika Birleşik Devletleri 1986 yılında çıkardığı "Federal Computer Fraud and Abuse Act" (Federal Bilgisayar Sahtekârlığı ve Kötüye Kullanma) adlı yasayı çıkartarak, bu suçla ilgili ilk yasal mücadeleyi başlatmıştır [21].

Bu yasa çıktıktan sonra tutuklanıp ceza alan ilk kişi 1988 yılında, bilgisayar güvenlik uzmanı olan Robert Tappan Morrist olmuştur. Yine aynı yılda Kevin Mitnick; bilgisayar sistemlerinden gizli bilgi ve binlerce kredi bilgisi çalmakla, California motor araçları veri tabanına girmekle ve New York ve California'nın birçok makineyi birbirine bağlayan cihazlarını uzaktan kontrol etmekle suçlanmıştır. Böylece devlet bilgisayarlarına izinsiz ve yetkisiz giren Kevin Mitnick, FBI'nın en çok arananlar listesinde yer alan ilk bilişim suçlusu olarak tarihe geçmiştir [21]. Bu suçların teknolojiyi icat eden ve kullanmaya başlayan ülkelerde başlaması oldukça dikkat çekicidir.

Yeni gelişmelerle birlikte 1999 yılından itibaren virüsler internette çok büyük zararlara neden olmaya başlamışlardır. CIH virüsü binlerce bilgisayara milyar dolarlar değerinde zararlar vermiştir. Bu zarardan önce virüslerin bu denli zararlı olabileceği düşünülmemiştir. 2000 yılında "LoveBug", "Melisa" ve 2001 yılında "Kırmızı Kod" (Code Red) çok büyük zararlara sebep olan virüs olarak bilişim suçları tarihinde yerini almıştır [22].

Bilgi ve iletişim sektörünün gelişmesinin en önemli yan etkilerinin başında, bu suçların teknolojiler kullanılarak işlenmeye başlanmış olmasıdır. Her geçen gün yeni suç işleme araç ve yöntemleri ortaya çıkarken, suç işleme yöntemine karşın önlemler bulunduğu anda, daha gelişmiş ve farklı bir suç işleme yöntemi geliştirilmektedir [16]. Bu gelişme bilişim teknolojilerinin uzmanı olmayan sıradan vatandaşı olumsuz etkilerken, bilişim suçlarının takibi ve bu teknolojilerin ülke genelinde sağlıklı şekilde dağıtımından sorumlu kamu kurumlarının politikalarını sürekli güncelleştirmeleri zorunluluğunu doğurmaktadır. Türkiye, kamu kurumlarının ve özel işletmelerin kritik öneme sahip bilişim sistemlerinin güvenliğinin sağlanması ve siber olayların etkilerinin düşük seviyede kalması, meydana gelen suçların adli ve kolluk birimlerince etkin araştırılması ve soruşturulması amacıyla çıkarılan Ulusal Siber Güvenlik Stratejisi ve Eylem Planı 2013-2014'ü hazırlayarak, ilgili kamu kuruluşlarının görevlerini belirlemiştir. Böylece ulusal bir politika yürürlülüğe konmuştur [23].

Günümüzde, Türk Ceza Kanununda (TCK) yazılı olan suç tiplerinin büyük çoğu internet üzerinden işlenmekte ve bilişim suçları kapsamına girebilmektedir [24]. Artık neredeyse internet üzerinden işlenemeyen veya internet olmadan işlenemeyecek suç kalmayacak şeklinde bir yorumda dahi bulunulabilir. Türkiye'de bilişim suçları alanında yapılan bir araştırmada, 1990 yılından 2011 yılının Temmuz ayına kadar yıl ve il bazında mahkemelere intikal eden 40 farklı suç maddesine ait 73.185 adet ceza ve hukuk davasıyla ve toplam 98.391 sanık bulunduğu bildirilmektedir [25].

İnternetin kullanımı o kadar yaygınlaşmıştır ki, Haziran 2014 verilerine göre 7 milyarı geçen dünya nüfusunun yaklaşık % 42,3'ü yani 3.035.749.340 kişi interneti kullanmaktadır. Yine Türkiye'de internet kullanımı günden güne artmakta, nüfuzun % 56'7'si yani 46.282.850 kişi internet kullanmaktadır [26]. Artık bilişim suçu işleyenler ulusal tehlikenin ötesinde uluslararası nitelikte tehdit unsuru olarak görülmektedirler. Sürekli büyüyen teknolojiyle birlikte gelişen bilişim suçu yöntemleri gittikçe daha fazla maddi ve manevi zarara neden olmaktadır.

Bilişim suçlarının diğer suçlardan; işlenme, şekil ve kaynak yönünden bazı farklılıkları bulunmaktadır. Bilişim suçlarında en büyük özellik işlenme şekli olduğu kabul edilmektedir [11]. Ayrıca siber suçları işleyenlerin çok büyük zararlar verebilmelerine rağmen, suçun sanal ortamda işlenmesi sonucu, verilen zararın gözlemlenebilmemesi nedeniyle, insanların verdikleri zarardan dolayı herhangi bir sorumluluk hissetmedikleri tespiti yapılmıştır [27]. Bilişim suçlarının işlenme şekillerini beş başlıkta toplamak mümkündür [28];

1. Bilgisayarda bulunan kaynağa veya herhangi bir değere gayri meşru şekilde ulaşarak transferini sağlamak için kasıtlı olarak bilgisayar verilerine girmek, bunları bozmak, silmek, yok etmek,

2. Bir sahtekârlık yapmak için kasıtlı olarak bilgisayar verilerine veya programlarına girmek, bunları bozmak, silmek, yok etmek,

3. Bilgisayar sistemlerinin çalışmasını engellemek için kasten bilgisayar verilerine veya programlarına girmek, bozmak, silmek, yok etmek,

4. Ticari anlamda yararlanmak için bir bilgisayar programının yasal olarak sahibinin haklarını zarara uğratmak,

5. Bilgisayar sistemi sorumlusunun izni dışında, konulmuş olan emniyet önlemlerini aşmak sureti ile sisteme kasıtlı olarak girip müdahalede bulunmaktır.

Birleşmiş Milletler ve Avrupa Birliği tarafından 11.06.1999 tarihinde hazırlanan "Bilişim Suçları" raporunda ise suç çeşitleri altı başlık altında toplanmıştır. Bunlar;

- Bilgisayar Sistemlerine ve Servislerine Yetkisiz Erişim ve Dinleme,
- Bilgisayar Sabotajı,
- Bilgisayar Yoluyla Dolandırıcılık,
- Bilgisayar Yoluyla Sahtecilik,

• Kanunla Korunmuş Yazılımın İzinsiz Kullanımı,

• Diğer Suçlar" başlığı altında Kanundışı Yayınlar, Pornografik Yayınlar (Büyük ve Çocuk Pornografisi), Hakaret ve Sövme [29].

Ülkelerin hukuksal açıdan suç olarak belirledikleri bilişim suçları genel itibariyle birbirine benzemektedir. Hemen hemen bütün ülkeler bilgisayar aracılığıyla dolandırıcılık, verilere zarar vermek, verilerde sahtekârlık, sabotaj, sisteme yetkisiz girme, zaman hırsızlığı ve verilerin ele geçirilmesi gibi bilişim faaliyetlerini suç olarak belirlemiştir [30].

1987 tarihli TCK öntasarısında bilişim suçları hakkında herhangi bir düzenleme bulunmamakta iken, 1989 tarihli TCK öntasarısını hukuk mevzuatımızda bu suçların düzenlendiği ilk metin olarak değerlendirmek mümkündür [31]. 765 sayılı TCK, 1991 tarihinde çıkarılan 3756 sayılı kanunla "Bilişim Alanında Suçlar" başlığıyla, cürüm niteliğinde olmak üzere, 525a, 525b, 525c ve 525d maddelerinde düzenlenmiştir [30]. Ceza hukukumuzda yeni ve demokratik gelişmeler olmasıyla ve toplumsal ihtiyaçların artmasıyla bu ihtiyaçları gidermek ve gelişmelere yer vermek üzere 5237 sayılı TCK, 2004 tarihinde TBMM tarafından kabul edilmiştir. Bu kanun 12 Ekim 2004 tarihli 25611 sayılı Resmi Gazete'de yayınlanmıştır [32].

Yeni TCK'nın 243, 244, 246 ve 246'ncı maddelerinde düzenlenen bilişim suçları; bilişim sistemine girme ve orada kalma, sistemi engelleme, bozma, verileri yok etme veya değiştirme, banka ve kredi kartlarına ilişkin suçlar şeklinde düzenlenmiştir. Bu suçlar şikâyete bağlı suçlar değildir. Savcılar bu suçun işlendiğini öğrendiğinde görevleri gereği araştırıp, sorumlular için dava açmak durumundadırlar [33].

3. YÖNTEM (METHOD)

Araştırmada betimsel tarama modeli kullanılmıştır. Araştırmanın çalışma grubunu, 2013–2014 Öğretim Yılı Güz yarıyılında Erciyes Üniversitesi İlköğretim Bölümü Sınıf Öğretmenliği Anabilim dalındaki 205 öğrenci oluşturmaktadır. Çalışma grubu söz konusu bölümdeki tüm sınıfları içermektedir. Veri toplama aracı olarak araştırmacılar tarafından geliştirilen 16 maddelik Likert tipi "Bilişim Kavramları ve Suçlarına Yönelik Öğrenci Görüş Anketi" kullanılmıştır. Ölçeğin Cronbach Alpha iç tutarlılık katsayısı 0,84, KMO değeri ise .76'dır.

Veri toplama aracında:

- 1–1,80 arası değerler "Hiç Katılmıyorum",
- 1,81–2,60 aralıkları "Katılmıyorum",
- 2,61–3,40 arası "Kısmen Katılıyorum",
- 3,41–4,20 arası "Katılıyorum",
- 4,21–5.00 arası "Tamamen Katılıyorum" seçeneğine karşılık gelmektedir.

Veri toplama aracının dağıtılmasından sonra 196 anket geri dönmüş ve 3 anket hatalı doldurulması nedeniyle iptal edilmiştir. 193 anketten elde edilen veriler çözümlemeye dâhil edilmiştir. Verilerin çözümünde bilgisayar destekli analiz yazılımı SPSS-16 kullanılmıştır. Verilerin çözümlenmesinde; f, %, aritmetik ortalama, t testi, analizi testi kullanılmış, anlamlılık düzeyi .05 olarak belirlenmiştir. Bulgular sonucunda gruplar arasında anlamlı farklılıklar bulunmamıştır.

4. BULGULAR VE YORUMLAR (RESULTS AND COMMENTS)

Bu bölümde araştırmadan elde edilen bulgular ve yorumlar alt başlıklar halinde sunulmaya çalışılmıştır.

4.1. Demografik, Bilgisayar ve İnternet Kullanma Özelliklerine İlişkin Bulgular ve Yorumlar (Results And Comments Regarding Demographics, Using Computer and İnternet)

Bu bölümde, araştırmaya katılan öğrencilerin demografik özelliklerine ilişkin bulgular; bilgisayar ve internet kullanma durumları, bilgisayar ve internet konusunda herhangi bir kursa katılıp katılmama durumları ve bilgisayar ve interneti kullanım amaçlarıyla ilgili veriler çözümlenmiş ve tablolar haline getirilerek yorumlanmıştır.

Tablo- 1. Cinsiyet ve Öğrenim Gördükleri Sınıf Düzeyine Göre Bulgular
(Results According To The Gender And Education Studying The Class Level)

Değişkenler		***Frekans***	***%***
Cinsiyet	***Erkek***	***64***	***33***
	Kız	***129***	***67***
Sınıf	***1***	***46***	***24***
	2	***49***	***25***
	3	***51***	***26***
	4	***47***	***25***
Toplam		***193***	***100***

Tablo-1 incelendiğinde, araştırmaya katılan öğrencilerin % 33'nün erkek, % 67'sinin ise kız olduğu görülmektedir. Bununla birlikte öğrencilerin % 24'ü 1. sınıf öğrencisi, % 25'i 2. sınıf, % 26'sı 3. sınıf ve % 25'i 4. sınıfta öğrenim görmektedir. Sınıf düzeyi yönünden öğrencilerin dağılımlarının birbirine yakın değerlerde olduğu görülmektedir. Bu durum sınıf düzeylerine göre öğrencilerin diğer bulgular yönünden herhangi bir farklılıkları olup olmadığını göstermesi yönünden araştırmaya önemli katkı sağlayacaktır.

Kız öğrenci sayısının, erkek öğrenci sayısının yaklaşık olarak iki katına yaklaştığı görülmekte, sınıf öğretmenliğinin kız öğrenciler tarafından tercih edilme oranının Erciyes Üniversitesi için oldukça fazla olduğunu göstermektedir.

Tablo- 2. İnternete Erişim Yeri, Giriş Süreleri Ve Bir Kurs Alma Verilerine Göre Öğrencilerin Dağılımı
(Distribution Of Students According To The Internet Access Location, Entry Deadlines And Taking Any Course)

Değişkenler		*f*	*%*
İnternete Erişim Yeri	*Evden*	*106*	*54,9*
	İnternet Kafeden	*36*	*18,7*
	Mobil Cihazdan	*19*	*9,8*
	Diğer	*28*	*14,5*
	Belirtmeyen	*4*	*2,1*
İnternete Giriş Süresi (Saat/Gün)	*0-1*	*126*	*65,3*
	1-3	*46*	*23,8*
	3 ve Üstü	*18*	*9,3*
	Belirtmeyen	*3*	*1,6*
Kurs Alma Durumları	*Evet*	*37*	*19,2*
	Hayır	*156*	*80,8*
Toplam		*193*	*100*

Öğrencilerin % 54,9'unun evden, % 18.7'sinin internet kafeden, % 9.8'inin mobil cihazından ve % 14.5'inin ise diğer yollarla eriştikleri görülmektedir. Araştırmaya katılan öğrencilerden % 2.1'i internete bağlanma şeklini belirtmemiştir. Bu sonuçlar bu nesil için interneti kullanma oranının yüksekliğini gösterirken, aynı zamanda internete erişimin artık kolaylıkla sağlanabildiğini göstermektedir.

İnternete günlük erişim süresi açısından bakıldığında; öğrencilerin % 65.3'nün 0–1 saat, % 23.8'inin 1–3 saat ve % 9.3'ünün de 3 saat ve üstü süreyle girdikleri görülmektedir. Öğrencilerin % 1.6'sı internete giriş süresini belirtmemiştir. Bu sonuçlarda internetin kullanımı konusunda, aşırı kullanımın fazla olmadığı ve internet bağımlılığının kabul edilebilir seviyede olduğunu göstermektedir.

Tablo- 3. Öğrencilerin İnterneti Öncelikli Kullanım Amaçları
(*The Priority Aims Of Using İnternet Of The Students*)

	Amaç	*f*	*%*
1	*Ödev Ve Araştırma Gibi Öğrenme Süreçlerine Destek Amacıyla*	*93*	*48*
2	*Eğlence Ve Oyun Amacıyla*	*52*	*27*
3	*Ekonomik, Siyasi ve Spor Gibi Güncel Haberler Takip Amacıyla*	*21*	*11*
4	*Diğer*	*27*	*14*
Toplam		*193*	*100*

Araştırmaya katılan öğrencilerin % 48'lik kısmının interneti, öncelikli olarak öğrenme süreçlerine destek amacıyla kullandığı görülmektedir. % 27'sinin eğlence ve oyun, % 21'inin haberler (ekonomi ve spor) ve % 14'ünün belirtilmeyen diğer sebepler için kullandığı ifade edilmiştir. Bulgular incelendiğinde öğrencilerin internete, oyun ve eğlence amaçlardan çok öğrenme süreçlerine destek amaçlı bağlandıkları görülmektedir.

4.2. İnternet Üzerinden İşlenen Bilişim Suç Kavramlarını Bilme Düzeyine Göre Bulgular (Results According To Knowing The Cyber Crime Concepts Commit On The Internet)

Bu başlık altında araştırmaya katılan öğrencilerin internet ortamında bir biçimde karşılaşabilecekleri bilişim suçlarını kavramsal olarak bilme düzeylerine yönelik görüşleri incelenmiştir.

Tablo-4. İnternet Üzerinden İşlenen Bilişim Suç Kavramlarını Bilme Düzeyine Göre Bulgular
(Results According To Knowing The Cyber Crime Concepts Commit On The Internet)

Kavramlar/ Düzey		*Bu Kavramın Ne Olduğunu Bilirim*		*Bu Kavramın Sadece Adını Duydum*		*Bu Kavram Hakkında Fikrim Yok*		*Cevap Belirtmeyen Öğrenci Sayısı*	
		f	*%*	*f*	*%*	*f*	*%*	*f*	*%*
1	*Ağ Solucanları*	*26*	*13,5*	*72*	*37,3*	*95*	*49,2*	*-*	*-*
2	*Bilgisayar Ve Ağ Güvenliği*	*128*	*66,3*	*54*	*28,0*	*10*	*5,2*	*1*	*0.5*
3	*Bilişim Korsanlığı*	*48*	*24,9*	*96*	*49,7*	*46*	*23,8*	*3*	*1.6*
4	*Bukalemun*	*19*	*9,8*	*29*	*15,0*	*143*	*74,1*	*2*	*1.1*
5	*Cracker*	*17*	*8,8*	*35*	*18,1*	*138*	*71,5*	*3*	*1.6*
6	*Çocuk Pornografisi*	*91*	*47,2*	*60*	*31,1*	*39*	*20,2*	*3*	*1.6*
7	*Elektronik İmza*	*66*	*34,2*	*85*	*44,0*	*40*	*20,7*	*2*	*1.1*
8	*Hacking*	*61*	*31,6*	*49*	*25,4*	*79*	*40,9*	*4*	*2.1*
9	*İstem Dışı Alınan E-Posta*	*77*	*39,9*	*63*	*32,6*	*50*	*25,9*	*3*	*1.6*
10	*Kredi Kartları Sahteciliği Ve Dolandırıcılığı*	*113*	*58,5*	*66*	*34,2*	*13*	*6,7*	*1*	*0.5*
11	*Kurtlar*	*14*	*7,3*	*34*	*17,6*	*144*	*74,6*	*1*	*0.5*
12	*Logic Bombs*	*2*	*1,0*	*12*	*6,2*	*178*	*92,2*	*1*	*0.5*
13	*Mantık Bombaları*	*8*	*4,1*	*15*	*7,8*	*168*	*87,0*	*2*	*1.1*
14	*Maskeleme*	*12*	*6,2*	*23*	*11,9*	*158*	*81,9*	*-*	*-*
15	*Oltalama*	*8*	*4,1*	*24*	*12,4*	*161*	*83,4*	*-*	*-*
16	*Phishing Saldırıları*	*4*	*2,1*	*13*	*6,7*	*175*	*90,7*	*1*	*0.5*

17	*Phreakers*	*1*	*,5*	*14*	*7,3*	*178*	*92,2*	*-*	*-*
18	*Sahne Kapısı*	*6*	*3,1*	*14*	*7,3*	*171*	*88,6*	*2*	*1.1*
19	*Salam Tekniği*	*3*	*1,6*	*14*	*7,3*	*175*	*90,7*	*1*	*0.5*
20	*Sırtlama*	*5*	*2,6*	*10*	*5,2*	*174*	*90,2*	*4*	*2.1*
21	*Siber Dolandırıcılık*	*30*	*15,5*	*52*	*26,9*	*109*	*56,5*	*2*	*1.1*
22	*Siber Kumar Ve Bahis*	*28*	*14,5*	*56*	*29,0*	*107*	*55,4*	*2*	*1.1*
23	*Siber Şantaj Ve Tehdit*	*25*	*13,0*	*52*	*26,9*	*108*	*56,0*	*8*	*4.1*
24	*Spam*	*36*	*18,7*	*61*	*31,6*	*94*	*48,7*	*2*	*1.1*
25	*Tavşanlar*	*8*	*4,1*	*17*	*8,8*	*167*	*86,5*	*1*	*0.5*
26	*Trojen Horse*	*31*	*16,1*	*26*	*13,5*	*134*	*69,4*	*2*	*1.1*
27	*Truva Atı*	*78*	*40,4*	*51*	*26,4*	*63*	*32,6*	*1*	*0.5*
28	*Warez*	*4*	*2,1*	*13*	*6,7*	*175*	*90,7*	*1*	*0.5*
29	*Web Sayfası Hırsızlığı*	*49*	*25,4*	*85*	*44,0*	*57*	*29,5*	*2*	*1.1*
30	*Worms*	*6*	*3,1*	*22*	*11,4*	*165*	*85,5*	*-*	*-*

Tablo-4'te "Bu Kavramın Ne Olduğunu Bilirim" kısmı incelendiğinde; katılımcılar tarafından en az bilinen kavramların, "Phreakers" (N=1), "Logic Bombs" (N=2), "Salam Tekniği" (N=3), "Warez" (N=4), "Phishing Saldırıları" (N=4), "Sırtlama" (N=5), "Worms" (N=6), "Sahne Kapısı" (N=6), "Mantık Bombaları" (N=8), "Oltalama" (N=8) ve "Tavşanlar" (N=8) olduğu görülmüştür.

Ayrıca en fazla bilinen kavramların, "Bilgisayar ve Ağ Güvenliği" (N=128), "Kredi Kartı Sahteciliği ve Dolandırıcılığı" (N=113), "Çocuk Pornografisi" (N=91), "Truva Atı" (N=78) ve "İstem Dışı Alınan e-posta" (N=77) olduğu tespit edilmiştir.

Araştırmaya katılan öğrencilerin "Bu Kavramın Sadece Adını Duydum" başlığına vermiş oldukları cevaplar incelendiğinde, "Sırtlama" (N=10), "Logic Bombs" (N=12), "Phishing Saldırıları" (N=13), "Warez" (N=13), "Phreakers" (N=14), "Sahne Kapısı" (N=14) ve "Salam Tekniği" (N=14) kavramların öğrenciler tarafından en az duyulan kavramlar olduğu görülmektedir. Bu durum Hekim ve Bölükbaşı tarafından; bilişim suçlarının kapsadığı geniş alan nedeniyle, suçların değişik şekil ve içeriklerde olabileceğini, klasik suçların siber alan ile farklı biçim ve yoğunlukta temas edebileceği şeklinde ifade edilmektedir. Dolayısıyla teknolojideki gelişiminin tahmin edilemezliği, böyle kavram genişliğini zaruri kılmaktadır [12]. Nitekim kavramlardaki yoğunluk ve çeşitlilik bu savı doğrulamaktadır.

Aynı kategoride verilen cevaplara bakıldığında ise en fazla duyulan kavramların "Bilişim Korsanlığı" (N=96), "Web Sayfası Hırsızlığı" (N=85), "Elektronik İmza" (N=85) ve "Ağ Solucanları" (N=72) kavramları olduğu görülmüştür.

"Bu Kavram Hakkında Bilgim Yok" başlığına bakıldığında katılımcıların en az "Bilgisayar ve Ağ Güvenliği" (N=10), "Kredi Kartı Sahteciliği ve Dolandırıcılığı" (N=13), "Çocuk Pornografisi" (N=39) ve "Elektronik İmza" (N=40) kavramlarını işaretledikleri görülmektedir. Bu kavramların öğrenciler tarafından bilinme sıklığı diğerlerine göre fazladır.

Öğrenciler tarafından en fazla bilinmeyenler; "Phreakers" (N=178), "Logic Bombs" (N=178), "Salam Tekniği" (N=175), "Warez" (N=175), "Phishing Saldırıları" (N=175), "Sırtlama" (N=174), "Sahne Kapısı" (N=171), "Mantık Bombaları" (N=168), "Tavşanlar" (N=167), "Worms" (N=165), "Oltalama" (N=161), "Maskeleme" (N=158), "Kurtlar" (N=144), "Bukalemun" (N=143), "Cracker" (N=138) ve "Trojen Horse" (N=134) kavramlarıdır. Muhtemeldir ki bu kavramların bilinme sıklığının azlığı İngilizce ve teknik kavramlar olmasıdır.

Araştırmada hem Türkçesi hem İngilizcesi verilen kavramlara öğrencilerin farklı cevaplar verdikleri görülmüştür. Aynı anlamda olan Truva Atı ve Trojen Horse kavramları ayrı ayrı verilmiş, öğrencilerin Truva Atı kavramına % 40.4 oranında "Bu Kavramın Ne Olduğunu Bilirim" düzeyinde cevap verdikleri, Trojen Horse kavramına ise %16.1 oranında "Bu Kavramın Ne Olduğunu Bilirim" cevabını verdikleri görülmektedir.

Yine aynı anlama gelen Mantık Bombaları ve Logic Bombs kavramlarından öğrenciler Mantık Bombalarına %4.1 oranında "Bu Kavramın Ne Olduğunu Bilirim" düzeyinde cevap verirken, Logic Bombs kavramına %1 oranında "Bu Kavramın Ne Olduğunu Bilirim" cevabını vermişlerdir. Truva Atı-Trojen Horse ve Mantık Bombaları-Logic Bombs kavramlarında, Türkçe olanların öğrenciler tarafından daha fazla bilindikleri görülmektedir. Bu durumda bilişim suçlarına yönelik kavramlarda Türkçe karşılığı olan kavramlara öncelik verilmesi gerektiğini göstermektedir.

4.3. Bilişim Suçlarına Karşı Çalışmaları Ve Cezaları Bilmeye Göre Bulgular Ve Yorumlar (The Findings and Comments Related To Attitudes Of Students Twowards İnformation Tecnology Crime)

Bu bölümde araştırmaya katılanların bilişim suçlarına karşı güvenlik güçleri tarafından alınan önlemler ve yapılan çalışmalar hakkında bilgi sahibi olup olmadıklarına ve yasalarda bilişim suçlarına yönelik yer alan cezaları bilip bilmediklerine yönelik bulgular ve yorumlar verilmiştir.

Tablo- 5. Öğrencilerin Güvenlik Güçlerinin Bilişim Suçlarına Yönelik Çalışmalarını ve Cezaları Bilme Durumlarına Yönelik Bulgular

(Results İnformation About Cyber Crime Of Students According To Works Made By Security Forces And Fines)

Değişkenler		***f***	***%***
Güvenlik Güçlerinin (Kolluk Kuvvetleri) Bilişim Suçlarına Karşı Çalışmalarını Bilme Durumu	***Evet***	***9***	***4,7***
	Hayır	***97***	***50,3***
	Kısmen	***87***	***45,1***
Bilişim Suçlarına Yönelik Cezaları Bilme Durumu	***Evet***	***8***	***4,1***
	Hayır	***121***	***62,7***
	Kısmen	***61***	***31,6***
	Belirtmeyen	***3***	***1,6***
Toplam		***193***	***100***

Araştırmaya katılan öğrencilerin % 4.7'sinin güvenlik güçlerinin bilişim suçları üzerine yaptıkları çalışmalar hakkında bilgi sahibi olduğu, % 50.3'ünün bu çalışmalar hakkında bilgi sahibi olmadığı ve % 45.1'inin de kısmen bilgi sahibi olduğu görülmektedir. Bilgi sahibi olmayanlar ile kısmen bilgi sahibi olanları düşündüğümüzde oldukça yüksek bir oranda (% 95,4) grubun bilişim suçlarıyla ilgili yetersiz bilgisi olduğu gözlenmektedir. Bu konuda güvenlik birimlerinin öğrencileri bilgilendirme, kamuoyu oluşturma konusunda yeterli çalışmalar yapmadığı göstermektedir. Halbuki bilişim teknolojilerinin toplumda geniş şekilde kullanılması, bu suçların bilinçli veya bilinçsizce işlenme olasılığını arttırmaktadır. Dolayısıyla güvenlik birimlerinin önleyici ve bilgilendirici çalışmaları çok önemlidir.

Yine benzer şekilde, öğrencilerin % 4.1'lik kısmının bilişim suçlarına yönelik cezalar hakkında bilgi sahibi olduğunu, % 62.7'lik kısmının bilgi sahibi olmadığını ve % 31.6'lık kısmının ise kısmen bilgi sahibi olduğu görülmektedir. Araştırmaya katılan öğrencilerden %1.6'sı bu konudaki bilgi durumlarını belirtmemiştir. Öğrencilerin bilişim suçları ve cezalarıyla ilgili bilgi düzeylerinin düşük olması aslında riskli bir durumu karşımıza çıkarmaktadır. Bu suçlarla ilgili ceza kanununda yer alan suçların ve cezaların toplumda yeterince bilinmemesi suçun işlenmesine yönelik caydırıcılığı azaltabileceği söylenebilir.

Halbuki ceza, bir davranışın suç olarak tanımlanıp tanımlanmayacağını belirleyen hukuksal bir terim olup, hangi davranışın suç olduğunu ve öngörülen cezai yaptırımın ne olduğunu belirleyen yasal bir tanımlamadır. Cezanın/cezalandırmanın amacı**,** daha önceden suç işlemiş olan bireylerin yeniden suç islemelerini engellemek ve suç isleme eğiliminde olan bireyleri de bu davranışı gerçekleştirmekten caydırmaktır [34]. Bu alanın örencilerde eksik olması, muhtemel ki bilişim teknolojilerini kullanan ve hatta kullanmak zorunda kalma olasılığı oldukça yüksek olan öğrenciler için de olumsuzlar doğurması ihtimalini arttırmaktadır. Üstelik öğrencilerde var olan bu eksiklik, muhtemeldir ki öğrencilerine eğitim verme aşamasında eksik bilgilerin aktarılması sonucunu doğurabilecektir.

4.4. Öğrencilerin Bilişim Suçları Hakkındaki Görüşlerine İlişkin Bulgular ve Yorumlar (Questions That Produced Significant Difference According to Veriable of Students Trainings About Tecnology Crime)

Öğrencilerin bilişim suç bilgisine sahip olup olmadığının irdelenmesinin yanı sıra suça ve suçluya karşı tutumlarının da incelenmesinin önemli olduğu düşünülmektedir. Öğrencilerin bilişim suç ve suçlarına karşı tutumları nelerdir?, Nasıl bir davranış sergilemektedirler? gibi konuların bilinmesinin araştırmaya katkı sağlayacağı düşünülmektedir. Tutum, bireyin çevresindeki herhangi bir olgu veya nesneye ilişkin sahip olduğu tepki eğilimini ifade etmektedir. Bireyin bir durum, olay ya da olgu karşısında ortaya koyması beklenen olası davranış biçimi olarak tanımlanmaktadır[35].

Bu bağlamda öğrencilere Likert tipi hazırlanan 16 adet ifadeye yönelik "tamamen katılıyorum" ile "tamamen katılmıyorum" arasındaki 5 düzeyden birini seçerek tavırlarını belirtmeleri istenmiştir. Söz konusu görüşlerin aritmetik ortalama ve standart sapma değerleri Tablo-6'da sunulmuştur. Ayrıca tutum maddelerinin çoğunda kız ve erkek öğrenciler arasında anlamlı farklılık bulunmamıştır. Kız ve erkek öğrenciler arasında anlamlı farklılık bulunan maddeler Tablo-7'de gösterilmiştir.

Tablo-6. Öğrencilerin Bilişim Suçlarına Yönelik Tutumlarına İlişkin Bulgular

(The Findings Related To Attitudes Of Students Towards İnformation Tecnology Crime)

No	***Bilişim Suçlarına Yönelik Tavır Maddeleri***	$\overline{X}$	***S***
1	***Mail adresimin ya da benzeri sayfalarımın şifresinin kırılması durumunda ne yapacağımı bilirim.***	***2,01***	***1,081***
2	***Lisans eğitimimizde aldığımız bilgisayar derslerinde bilişim suçlarına yönelik bilgiler verilmelidir.***	***4,45***	***0,781***
3	***Mail adreslerimin şifrelerini samimi arkadaşlarım bilir.***	***1,95***	***1,204***
4	***İnternet dolandırıcılığı hakkında yeterli bilgiye sahip değilim.***	***3,84***	***0,943***
5	***Mail ya da kendime ait kişisel kullanım sayfalarımın başkalarının eline geçmesi beni çok üzer.***	***4,45***	***0,871***
6	***Bana gelen virüslü maili fark edebilirim.***	***2,5***	***1,17***
7	***Tanımadığım kişileri mail adresime ve kişisel sayfalarıma eklemem.***	***4,58***	***0,893***
8	***Kredi kartımla internetten rahatlıkla alışveriş yaparım.***	***1,91***	***1,197***
9	***Bilgisayarım virüslere karşı korunaklıdır.***	***3,56***	***1,14***
10	***Basın ve medya internet suçları***	***3,84***	***1,017***

	hakkında insanları bilgilendirmiyor.		
11	***Herhangi bir bilişim suçuna şahit olduğumda ne yapacağımı bilirim.***	***2,3***	***1,134***
12	***Bilişim suçlarına verilen cezaların ağır olması gerekmektedir.***	***4,16***	***0,921***
13	***Bilişim suçlarına yönelik bilgilendirmenin ilköğretimden itibaren başlaması gerekmektedir.***	***3,98***	***1,064***
14	***Bilişim suçları gözde büyütülecek düzeyde tehlikeli değildir.***	***1,44***	***0,679***
15	***Bilişim suçlarına yönelik, öğrencilere konferanslar veya seminerler düzenlenmelidir.***	***4,42***	***0,737***
16	***Bilişim suçlarını işleyebilen insanlar çok zeki insanlardır.***	***3,4***	***1,219***

Bulgular incelendiğinde öğrencilerin; "Mail adresimin ya da benzeri sayfalarımın şifresinin kırılması durumunda ne yapacağımı bilirim." (Madde-1) maddesine Katılmıyorum düzeyinde ($\overline{X}$ =2.01), "İnternet dolandırıcılığı hakkında yeterli bilgiye sahip değilim." (Madde-4) maddesine Katılıyorum düzeyinde ($\overline{X}$ =3.84), "Bana gelen virüslü maili fark edebilirim." (Madde-6) maddesine Katılmıyorum düzeyinde ($\overline{X}$ =2.50), "Herhangi bir bilişim suçuna şahit olduğumda ne yapacağımı bilirim." (Madde-11) maddesine Katılmıyorum düzeyinde ($\overline{X}$ =2.30) görüş bildirdikleri görülmektedir. Yani öğrenciler karşılaşabilecekleri bir bilişim suçunda, nasıl ve ne şekilde mağduriyet yaşayabilecekleri, hangi işlemleri yapacağı ve hangi kuruma başvuracağı konusunda yeterli düzeyde tutum sergileyecek bilince sahip olmadığı görülmektedir.

Öğrenciler, "Mail ya da kendime ait kişisel kullanım sayfalarımın başkalarının eline geçmesi beni çok üzer." (Madde-5) maddesine Tamamen Katılıyorum düzeyinde ($\overline{X}$ =4.45), "Bilişim suçlarına verilen cezaların ağır olması gerekmektedir." (Madde-12) maddesine Katılıyorum düzeyinde ($\overline{X}$ =4.16), "Bilişim suçları gözde büyütülecek düzeyde tehlikeli değildir." (Madde-14) maddesine Hiç Katılmıyorum düzeyinde ($\overline{X}$ =1.44) görüş bildirirken, bu bulgular öğrencilerin, bilişim suçlarının mağduru olma konusunda çekince ve korkularının olduğu şeklinde yorumlanabilir. Çünkü bilişim suçlarının meydana gelmesi durumunda, maddi bir takım kayıpların yanında özellikle resim, arkadaşlık sohbeti gibi bazı özel kişisel verilerin yabancı şahısların eline geçmesi durumunda kişilerin özel hayatlarında büyük ve kalıcı acıların yaşanması ihtimali artmaktadır.

Hattı zatında bilişim suçlarına yönelik olarak çıkarılan yasal düzenlemelerdeki temel amaçlardan birisi kişilerin özel hayatına müdahalenin engellenmesi ve dış tehtidlerden korunması olduğu kabul edildiğinde [36], kişilerin bu değerinin korunması ve bu tür bir suç korkusunu yaşamaması adına yasal düzenlemelerle bu hakların korunduğu görülmektedir.

Bir tür mağduru olabilecekleri suç korkusunun yaşandığı karşımıza çıkmaktadır. Normalde, bireylerin bir suçun mağduru olmaktan çekinmesi ve kaygı duyması doğal görülebilir bir olsa da, geniş anlamda günümüz şartlarında, kişilerin suç nedeniyle mağdur olabilecekleri kaygısı, toplum içerisinde bir güvensizlik duygusuna dönüşebilmektedir [37]. Nitekim öğrencilerin, "Kredi kartımla internetten rahatlıkla alışveriş yaparım." (Madde-8) maddesine Katılmıyorum düzeyinde ($\overline{X}$ =1.91) görüş bildirerek bu tür bir güvensizliği yaşadıkları görülmüştür. 2011 verilerine göre 1786 adet Banka ve Kredi Kartlarının Kötüye Kullanılması olayının yaşandığı, bir önceki yıla göre olay sayısında, sayısında yaklaşık olarak %58 oranında artış olduğu görülmüştür [16]. Kredi kartlarında, 2013 yılı itibariye 57 milyon kredi kartının kullanımda olduğu, bu haliyle Türkiye'nin Avrupa ülkeleri içerisinde ikinci sıraya yerleştiği ifade edilmektedir [38]. Kullanımındaki artışın, bu suçun oranındaki artışa neden olacağı söylenebilir.

Öğrencilerin, "Basın ve medya internet suçları hakkında insanları bilgilendirmiyor." (Madde-10) maddesine ($\overline{X}$ =3.84) Katılıyorum düzeyinde görüş bildirdikleri tespit edilmiştir. Basın, bilişim suçları konusunda yeterli düzeyde yayının yapmadığına yönelik bir inanış vardır. Ancak internet üzerinden yapılan araştırmada, yazılı ve görsel basında, bilişim suçları konusunda birçok haberin çıktığı görülmektedir [39].

Öğrencilerin " Lisans eğitimimizde aldığımız bilgisayar derslerinde bilişim suçlarına yönelik bilgiler verilmelidir." (Madde-2) ve "Bilişim suçlarına yönelik, öğrencilere konferanslar veya seminerler düzenlenmelidir." (Madde-15) maddelerine Tamamen Katılıyorum($\overline{X}$ =4.45-$\overline{X}$ =4.42), düzeyinde ayrıca, "Bilişim suçlarına yönelik bilgilendirmenin ilköğretimden itibaren başlaması gerekmektedir." (Madde-13) maddesine Katılıyorum düzeyinde ($\overline{X}$ =3.98) görüş bildirdikleri görülmektedir Bu durumda öğrencilerin hem kendileri hem de yeni nesiller için bilişim suçları hakkında bilgilendirmeye fazlaca ihtiyaç duydukları söylenebilir. Nitekim Ulusal Siber Güvenlik Stratejisi ve Eylem Planı 2013-2014'te bilişim suçları ve güvenliği konusunda, ilköğretimden başlayarak üniversite öğrencilerini de içerisine alan etkinliklerin düzenlenmesi, kitapların, el ilanları ve broşürlerin yayınlanmasının amaçlanmakta olduğu görülmektedir [23]. Öğrencilerin bu görüşleri, bilişim suçlarına yönelik bir farkındalığa ihtiyaç olduğunu göstermesi açısından önemlidir. Nitekim gelecek dönemlerde, bilişim teknolojilerindeki inanılmaz gelişme, suçların çoğunun artık bu teknolojiler üzerinde işlenmesi ve suçlara aracılık eden araçlara dönüşmesini kaçınılmaz kılacaktır.

Öğrenciler "Mail adreslerimin şifrelerini samimi arkadaşlarım bilir." (Madde-3) maddesine "Katılmıyorum" düzeyinde ($\overline{X}$ =1.95), "Tanımadığım kişileri mail adresime ve kişisel sayfalarıma eklemem." (Madde-7) maddesine Tamamen Katılıyorum düzeyinde ($\overline{X}$ =4.58) ve "Bilgisayarım virüslere karşı korunaklıdır." (Madde-9) maddesine Katılıyorum düzeyinde ($\overline{X}$ =3.56) görüş bildirmişlerdir. Bu görüşler, öğrencilerin bilişim suçları konusunda mağdur olmamak konusunda tedbirli davrandıklarını göstermektedir. Olumlu bir gelişmedir. Çünkü şifrelerin ikinci kişilerin eline geçmesi, tanınmayan kişilere tehtid, hakaret, içeriğinde suç bulunan mesajların atılması gibi suçların oluşmasına neden olabilmektedir. Ayrıca virüsler kişilerin özel yaşamına ve verilerine müdahale edebilmekte, elde edilen bilgiler yoluyla; şantaj, tehtid, hakaret ve maddi kayıpların oluşmasını sağlayan suçların işlenmesine neden olabilmektedir.

Öğrenciler, "Bilişim suçlarını işleyebilen insanlar çok zeki insanlardır." (Madde-16) maddesine Kısmen Katılıyorum düzeyinde ($\overline{X}$ =3.40) görüş bildirmişlerdir. Yani öğrenciler bu suçların herkes tarafından kolaylıkla işlenebilecek suçlar olarak görmektedir. Nitekim bilişim teknolojileri araçları günümüzde, eski dönemlere oranla, çok az bir bilgi ve para ile geliştirilebilmekte ve internet üzerinden dünyanın doğusundan batısına, kuzeyinden güneyine her noktaya bu araçlar kullanılarak bu suçlar işlenebilmektedir [40].

Tablo-7. Cinsiyet Değişkenine Göre Anlamlı Farklılık Çıkan Maddeler

(Items That Produced Significant Difference On The Variable Of Sex)

Madde-No	***Cinsiyet***	$\overline{X}$	***SS***	***t***	***P***
6	***Erkek***	***2,79***	***,1634***	***2.26***	***.02***
	Kadın	***2,36***	***,0967***		
8	***Erkek***	***2,25***	***,1710***	***2.62***	***.01***
	Kadın	***1,73***	***,0951***		
16	***Erkek***	***3,68***	***,1257***	***2.47***	***.01***
	Kadın	3,26	,1159		

P<.05

Tablo-7'ye bakıldığında sadece; 6, 8 ve 16. maddelerde cinsiyetlere göre anlamlı farklılıklar oluşmuştur. "Bana gelen virüslü maili fark edebilirim. (Madde-6)" görüşüne erkek öğrenciler ($\overline{X}$ =2.79) "Kısmen katılıyorum" düzeyinde görüş bildirirken, kız öğrenciler ($\overline{X}$ =2.36) "Katılmıyorum" düzeyinde görüş bildirmişlerdir. Bu durumda erkek öğrencilerin virüslü e-mailler konusunda kız öğrencilere göre daha duyarlı oldukları söylenebilir.

"Kredi kartımla internetten rahatlıkla alışveriş yaparım. (Madde-8)" görüşüne erkek öğrenciler ($\overline{X}$ =2.25) "Katılmıyorum" düzeyinde görüş bildirirken kız öğrenciler ($\overline{X}$ =1.73) "Hiç katılmıyorum" düzeyinde görüş bildirmişlerdir. Burada kız öğrencilerin kredi kartı kullanımında erkeklere göre daha duyarlı davrandıkları görülmektedir.

"Bilişim suçlarını işleyebilen insanlar çok zeki insanlardır (Madde-16)" görüşüne erkek öğrenciler ($\overline{X}$ =3.68) "Katılıyorum" düzeyinde görüş bildirirken kız öğrenciler ($\overline{X}$ =3.26) "Kısmen katılıyorum" düzeyinde görüş bildirmişlerdir.

Tablo-8: Öğrencilerin Kurs Alma Durumları Değişkenine Göre Anlamlı Farklılık Çıkan Maddeler

(Items That Produced Significant Difference On The Variable Of Training About Technology Crime)

Madde-No	***Cinsiyet***	$\overline{X}$	***SS***	***t***	***P***
6	***Evet***	***2,83***	***,171***	***2.04***	***.04***
	Hayır	***2,43***	***,096***		
8	***Evet***	***2,41***	***,253***	***2.33***	***.02***
	Hayır	***1,79***	***,087***		

P<.05

Tablo-8'e bakıldığında 6. ve 8. maddelerde öğrencilerin kurs alma durumları değişkenine göre görüşlerinde anlamlı farklılıklar görülmüştür. "Bana gelen virüslü maili fark edebilirim. (Madde-6)" görüşüne bilgisayar kursu alan öğrenciler ($\overline{X}$ =2.83) "Kısmen Katılıyorum" düzeyinde, bilgisayar kursu almayan öğrenciler ($\overline{X}$ =2.43) "Katılmıyorum" düzeyinde, "Kredi kartımla internetten rahatlıkla alışveriş yaparım (Madde-8)" görüşüne bilgisayar kursu alan öğrenciler ($\overline{X}$ =2.41) "Katılmıyorum" düzeyinde görüş bildirirken, bilgisayar kursu almayan öğrenciler ($\overline{X}$ =1.79) "Hiç Katılmıyorum" düzeyinde görüş bildirmişlerdir. Bilgisayar ve benzeri kursları alan öğrencilerin bilişim suçlarına duyarlılığının arttığı söylenebilir.

5. SONUÇ (CONCLUSION)

Bilişim suçları, teknolojik gelişmelere dayalı olarak ortaya çıkan, bireyleri ve toplumu etkilemesi kaçınılmaz olan suçlardır. Hemen her alanda kullanımının zorunluluğu bu teknolojileri kullanan bireyleri, bilişim suçlarının kullanımı konusunda bilinçlendirilmelerini zorunlu kılmaktadır.

Günümüzde bilgi ve iletişim teknolojileri olarak adlandırılan bilgisayarlar, akıllı telefonlar hemen herkesin çok rahatlıkla ulaşabileceği araçlar haline gelmiş, bilişim suçlarının işlenmesini kolaylaştırmıştır. Bu durum bilişim suçlarının mağduru olması muhtemel kişilerin artmasına neden olabilmektedir. Dolayısıyla bilişim suçları konusunda yeni nesillerin bilgilendirilmesi büyük önem taşımaktadır. Sadece kolluk kuvvetlerinin çalışmalarıyla suçların önlenmeye çalışılması yeterli olmamakta,

toplumun önemli bir kesimine etkili şekilde ulaşma imkanı olan sınıf öğretmenlerine önemli görevler düşmektedir.

Araştırma, sınıf öğretmenleri adaylarının, bilişim suçları, içeriğindeki farklı kavramlar ve bu suçlara karşı sergileyecekleri tutumlar konusunda yeterli bilince sahip olmadıklarını göstermektedir. Ancak bilişim suçlarından kendilerini nasıl koruyacakları konusunda bilgiye ve yönlendirmeye ihtiyaç duydukları da görülmektedir. Öğrencilerin bilişim suçlarından kendilerini korumak amacıyla gösterdikleri duyarlılığın, şifreleri veya kredi kartlarını diğer kişilerden korumak şeklinde kısmen yetersiz bir korumacı tepkiyle sınırladıkları söylenebilir. Bu nedenle öğrencilerin doğru yönlendirilmesi gerekir. Yönlendirmeyi yapması gereken kurumların başlıcaları; üniversiteler, güvenlik birimleri ve sivil toplum kuruluşları olarak sayılmalıdır. Özellikle güvenlik birimleri, suçun aydınlatılması ve önlenmesiyle sorumlu olan kurumlar olarak bu konuda lider kurumlar olarak rol almalıdır.

Öğrencilerin, bilişim suçlarının yasal alt yapısı konusunda ve güvenlik birimlerinin bilişim suçlarını önlemede ne tür çalışmalar yaptığına dair bilgi eksikliklerinin olduğu görülmektedir. Şüphesiz kanunların ve kamu kurumlarının yaptığı çalışmaların tümünün kişiler tarafından bilinmesi imkansız olsa da, tüm bireylerin kaçınılmaz olarak kullanmak veya kullanmak zorunda kalacağı bilişim teknolojilerinin yanlış ve bilinçsiz kullanımının kendilerine yasal olarak ne tür zararlar verebileceği anlatılmalıdır.

Bilişim suçlarının, diğer klasik suçlardan farklı olarak çok farklı yöntemlerle işlendiği ve isimlendirildiği görülmektedir. Klasik suçlarda adı geçen; hırsızlık, dolandırıcılık, cinayet, gasp, silahla yaralama, bıçakla yaralama gibi suç kavramları ve yöntemlerinin zihinlerde bıraktığı izlenim açık ve berraktır. Bilişim suç literatüründe geçen kavramların büyük çoğunluğunun ise yabancı dillerden devşirilerek dilimize geçtiği görülmektedir. Bu durumda, kavramları bilmemekte suça karşı duyarsızlığa neden olabilmektedir. Nitekim araştırmada, hem Türkçe hem de İngilizce aynı anlamı içeren farklı kavramların öğrenciler tarafından algılanmasının farklılaştığı görülmektedir. Bilişim suç literatürüne adı geçen kavramların Türkçeleştirilmesi de önemli bir çalışma olacaktır.

KAYNAKÇA (REFERENCES)

[1] M. Çelikten, M. Şanal, Y. Yeni, "Öğretmenlik Mesleği ve Özellikleri", **Erciyes Üniversitesi Sosyal Bilimler Enstitüsü Dergisi**, 19, 207–237, 2005.

[2] T. Gürkan, **İlkokul Öğretmenlerinin Öğretmenlik Tutumları ile Benlik Kavramları Arasındaki İlişki**, Sevinç Matbaası, Ankara, 1993.

[3] İnternet: E. Balkı, A. Saban, Öğretmenlerin Bilişim Teknolojilerine İlişkin Algıları ve Uygulamaları: Özel Esentepe İlköğretim Okulu Örneği, http:// ilkogretim-online.org.tr/vol8say3/v8s3m12.pdf (14.03.2015).

[4] İnternet: http://arama.hurriyet.com.tr/arsivnews.aspx ?id=4818411 (14.03.2015)

[5] E.D. Aydın, **Bilişim Suçları ve Hukukuna Giriş**, Doruk Yayınları, Ankara, 1992.

[6] A. Köksal, **Bilişim Terimleri Sözlüğü**, Türk Dil Kurumu Yayınları, Sayı: 476, Ankara, 1981.

[7] B. Sankur, Y. İstefanopulos, **Elektrik Elektronik Bilgisayar Mühendisliği Terimler Sözlüğü**, Boğaziçi Üniversitesi Yayınları, İstanbul, 1997.

[8] B.T. Kaya, **Bilgi Teknolojileri ve Örgütsel Değişim**, TODAİE, Ankara, 1996.

[9] S. Dönmezer, **Kriminoloji**, Beta Basım, İstanbul, 1994.

[10] İnternet: http://www.internetarsivi.metu.edu.tr/tarih ce.php (09.10.2014)

[11] Z. Avşar ve G. Öngören, **Bilişim Hukuku**, Türkiye Bankalar Birliği Yayınları, Yayın No: 270, İstanbul, 2010.

[12] H. Hekim ve O. Başıbüyük, "Siber Suçlar ve Türkiye'nin Siber Güvenlik Politikaları", *Uluslararası Güvenlik ve Terörizm Dergisi*, 4 (2), 135-158, 2013.

[13] R.L. Perry, **Computer Crime**, Franklin Watts, New York, 1986.

[14] D.B. Parker, **Computer Crime: Criminal Justice Resource Manual,** National Institute of Justice, Washington D.C., 1989.

[15] Internet: D. Strothcamp, Fraud and Computer Crime. http://www.csuohio.edu/accounts/Strothcamp/TOPI C07/sld001.htm (12.12.2014)

[16] Ö. Tekeli, "Bilişim Suçlarıyla Mücadelede Polisin Yeri", *Sayder Dış Denetim Dergisi*, S. 183, 183-192, 2011.

[17] H.İ. Dilek, **Bilişim Suçları ve Türk Hukuk Sistemindeki Yeri**, Yüksek Lisans Tezi, Dicle Üniversitesi, Sosyal Bilimler Enstitüsü, Diyarbakır, 2007.

[18] İnternet: T.A. Johnson, International Review of Criminal Policy – United Nations Manual on the prevention and control of the computer- related crime http://www.uncjin.org/Documents/irpc4344. pdf) (10.02.2015)

[19] B. Günay, **Siber Terörist Saldırı**, 12 Mayıs 1999 Tarihli Türkiye Gazetesi

[20] T.A. Johnson, **Forensic Computer Crime Investigation**, CRC Press, 2005.

[21] İnternet: E. Kurt, "Hacker'lığın Kısa Tarihçesi" http://www.olympos.net/belgeler/hacking/hackerligi n-kisa-tarihcesi-5532.html (10.01.2015).

[22] Ç. Gümüş, **Bilişim Suçlarıyla Mücadelede Polisin Eğitimi,** Doktora Tezi, Fırat Üniversitesi, Sosyal Bilimler Enstitüsü, Elazığ, 2008.

[23] Resmi Gazete, 20.06.2013 tarih ve 28683 sayı.

[24] M. N. Güngör, **Yeni Türk Ceza Kanunu Kapsamında Bilişim Suçları ve Emniyet Genel**

[25] **Müdürlüğü Uygulamaları,** Yüksek Lisans Tezi, İstanbul Üniversitesi Sosyal Bilimler Enstitüsü Kamu Yönetimi Anabilim Dalı, İstanbul, 2007.
[26] İnternet: M. A. Köksal ve Ç. İlbaş, "Türkiye'de Bilişim Suçları: 1990-2011", http://www.slideshare.net/melihbayramdede/trkiyenin-siber-su-haritas-19902011 (10.02.2015).
[27] İnternet: http://www.internetworldstats.com/stats.htm (15.11.2014)
[28] O. Dolu, **Suç Teorileri: Teori, Araştırma ve Uygulamada Kriminoloji**, Seçkin Yayınları, Ankara, 2011.
[29] İnternet: C. Özel, "Bilişim Suçları ile İletişim Faaliyetleri Yönünden Türk Ceza Kanunu Tasarısı", http://www.hukukcu.com/bilimsel/kitaplar/bilisimsuclari_TCKtasarisi.htm (05.03.2015)
[30] İnternet: http://www.bilisimruzgari.com/default.asp?L=TR&mid=250 (08.03.2015)
[31] A. Berrin: "TCK'nın 525a, 525b, 525c Maddeleri ile 1997 Tasarısının Karşılaştırılması", **Adalet Bakanlığı Hâkim ve Savcı Adaylarının E.M.B. Bilişim Suçları Paneli**, Ankara Açık Cezaevi Matbaası, 17-24, Ankara, 2001.
[32] D. Olgun, **Bilişim Suçları**, Yüksek Lisans Tezi, Marmara Üniversitesi, Sosyal Bilimler Enstitüsü, İstanbul, 2002.
[33] A. Karagülmez, "Bilişim Suçları, Mevzuatımızdaki Yeri ve Uygulama Örnekleri", **1. Polis Bilişim Sempozyumu**, Ankara, 2003.
[34] M.B. Kızıltan, **5237 Sayılı Türk Ceza Kanununda Bilişim Sistemine Girme, Sistemi Engelleme ve Bozma Suçları**, Yüksek Lisans Tezi, İstanbul Üniversitesi, Sosyal Bilimler Enstitüsü, İstanbul, 2007.
[35] Z. Kızmaz, "Ceza veya Kriminal Yaptırımın Suç Oranları Üzerindeki Caydırıcı Etkisi" *Afyon Kocatepe Üniversitesi Sosyal Bilimler Dergisi*, 7(2), 221-245, 2005.
[36] M. İnceoğlu, **Tutum Algı İletişim**, Beykent Üniversitesi Yayınevi, İstanbul, 2010.
[37] A.İ. Erdağ, "Bilişim Alanında Suçlar: Türk Ve Alman Ceza Hukukunda", *Gazi Üniversitesi Hukuk Fakültesi Dergisi,* C. 14, 2, 275-303, 2010.
[38] Ö. Ömeroğlu, (2012), "Suç Korkusu, Cezanın Caydırıcılığı ve Küçük Suçlar", *Gazi Üniversitesi Hukuk Fakültesi Dergisi***,** 16, 329-370, 2012.
[39] İnternet: Bankalararası Kart Merkezi 2013 Yılı Faaliyet Raporu http://www.bkm.com.tr/basin/Faaliyet-Raporu-2013.pdf, , (06.03.2015).
[40] www.google.com.tr ("Basında Bilişim Suçları" Etiketli Arama Sonuçları) (06.03.2015).
[41] İnternet: M. Ünver, ve C. Canbay, "Ulusal ve Uluslararası Boyutlarıyla Siber Güvenlik", http://www.btk.gov.tr/bilgi_teknolojileri/siber_guvenlik/dokumanlar/siber_guvenlik.pdf (21.02.2015).