Sosyal Ağlarda İşlenen Suçlar, Facebook Sosyal Ağı Örneği

Nursel Yalçın1, Filiz Gürbüz2
1 Gazi Üniversitesi, Bilgisayar ve Öğretim Teknolojileri Eğitimi Bölümü, Ankara
2 Gazi Üniversitesi, Bilişim Enstitüsü, Ankara
nyalcin@gazi.edu.tr, gurbuz.flz@gmail.com

Özet: Toplum hayatında sosyal ağ ve paylaşım sitelerinin yeri gün geçtikçe artmaktadır. Kişiler sosyal ağlar sayesinde paylaşmak istediği fikirlerini zaman mekan ya da ortama bağlı kalmaksızın paylaşabilmekte sosyal çevreleri ile iletişim halinde kalabilmektedir. Sosyal ağların insanlar bakımından sosyalleşme platformu olarak görülmesi ve gün geçtikçe yaygınlaşması ile birlikte sosyal ağlar suçlularında suç işleme alanı haline gelmiştir. Sosyal medya alanında işlenen suçlar hem Türk Ceza Kanunlarında düzenlenen ve teknik olarak bilişim suçu olarak tanımlanan suçlar, hem de bilişim sistemleri aracılığıyla işlenen klasik suçlar olarak ortaya çıkabilmektedir. Zaman zaman gazete haberlerine konu olan sosyal medya ortamında işlenen bu suçlar nedeniyle kişiler, işlerini kaybetmekte aile içi huzursuzluklar yaşanmakta maddi ve manevi zarara uğramaktadır. Bu çalışmada da Türkiye çevrimiçi nüfusunun çok büyük bir kısmının kullandığı Facebook sosyal paylaşım ağı üzerinde gerçekleşen, gazete ve internet ortamında zaman zaman gündeme gelen suçlara yönelik bir araştırma yapılmış ve hangi suçlarla daha çok karşılaşıldığının tespitine yönelik bir anket çalışması gerçekleştirilmiştir. Anket 18 sorudan oluşmaktadır. 224 kişinin internet ortamında çevrim içi olarak katıldıkları ankette 18 soru sorulmuştur. Sorulan 18 sorunun 6'sı ankete katılan kişilerin genel özelliklerinin belirlenmesine 12 soru ise Facebook ortamında işlenen bilişim ve klasik suçlara yönelik suçlarla karşılaşıp karşılaşmadıklarına dairdir. Elde edilen bilgilere sayısal veriler ve grafikler halinde çalışma sonunda yer verilmiştir.

Anahtar Sözcükler: Facebook, bilişim suçları, sosyal ağlar, bilişim sistemleri aracılığıyla işlenen suçlar

Cyber Crimes Committed in Social Media, Facebook

Abstract: The importance of social media and websites in society, are increasing day by day. Daily users of social media already became active member of this life and already sharing all their own ideas without any observation to any limitations. Furthermore; these users are also critically became active communicators. The increasing importance of social media as a socialization platform and becoming commonplace; are also increased the number of social media offenses. Those points are also described as Turkish Penal Statute, technical information statutes and classical statutes which relates to information systems. Regarding to the some newspapers by reason of social media offenses; people are sacking down from their jobs, having serious familial problems and having spiritual & material damages. This study has especially worked on a survey (about on the internet or social media statutes) where we have been facing with the most statutes on social media life. The survey has designed in 18 questions and these questions have asked to 224 people on an online internet platform. The 6 questions out of 18, have mainly focused on general information about survey participants and the rest of the questions have focused on if they've faced with informatics and classics statutes. The attainments have shown up by numerical data's and graphics at the end of this study.

Keywords: Facebook, cyber crimes, social networks, crimes committed via information systems

1.Giriş

Bireylerin sınırları belirlenmiş bir sistem içinde halka açık ya da yarı açık profil oluşturmasına, sistem ile bağlantıda olan kullanıcıların listesini açıkça verilmesine, diğer kullanıcıların sistemdeki listelenmiş bağlantıları görmesine ve aralarında gezinmesine izin veren web tabanlı hizmetlerin tümüne sosyal ağ denilmektedir. Twitter, Facebook ve Linkedin bu tür ağlara örnektir.

Bir sosyal ağın kullanım amacı ve kullanım yoğunluğu kullanıcılar ve toplumlar tarafından farklılık göstermektedir. Örneğin Fransa'da öğrencilerin arkadaşlarıyla irtibatta kalmak ve eski ilişkileri tazelemek amacıyla kullandıkları Facebook, Japonya'da güvenli görülmediğinden çok fazla tercih edilmemektedir. Meksika'da ise Fransa ile benzerlik göstermekle beraber, yeni arkadaşlar edinmek için kullanılmaktadır [4].

Facebook istatistiklerine göre; Türkiye'nin çevrimiçi nüfusunun %94'ü Facebook kullanmaktadır. Haziran 2013'ten aralık 2013'e kadar aylık aktif kullanıcı sayısı %3 lük bir artışla 33 milyon'dan 34 milyon'a çıkmıştır. Haziran 2013'ten Aralık 2013'e kadar günlük aktif kullanıcı sayısı 20 milyondan %5 lik artışla 21 milyona çıkmıştır. Facebook her gün Türkiye'nin çevrimiçi nüfusunun %58'ine ulaşmaktadır [15].
Başlangıçta ağa kayıtlı kişilerin yeni insanlarla tanışmak ya da mevcut çevreleri ile iletişime geçmek için kullandıkları sosyal ağlar zamanla iletişim ve etkileşimde büyük bir potansiyel güç halini almıştır. Sosyal ağları kullanarak şirketlerin maddi kazanç elde etmeyi başarmaları ya da Arap devriminde ve Gezi Parkı olaylarında sosyal medyanın rolü göz önüne alındığında ve Facebook istatistikleri incelendiğinde sosyal ağların internet ortamında nasıl bir güce sahip olduğu görülmektedir.
Sosyal ağların bu denli büyümesi ve büyük bir güce sahip olması beraberinde sosyal ağların suçlular içinde bir suç işleme ortamı halini almasına neden olmaktadır. Ayrıca sosyal ağların hızlıca yayılması onun takibini ve kontrolünü de zorlaştırmaktadır.

Bu çalışmada, sosyal ağ platformlarından Facebook sosyal ağında zaman zaman gazete ve internet haberlerine konu olmuş; bilişim suçları ve internet ortamında işlenen klasik suçlar araştırılmıştır. Çalışmada 18 soruluk bir anket çalışması hazırlanmıştır. Anket çalışması ile katılımcıların Facebook üzerinde maruz kaldıkları suçların oranları tespit edilmeye çalışılmıştır. Online olarak hazırlanan anket formu internet üzerinden kullanıcılara ulaştırılmıştır. Anket sonucu elde edilen veriler çalışmanın sonuç kısmında yer almaktadır.

2. Bilişim Suçları ve İnternet Ortamında İşlenen Geleneksel Suçlar

Bilişim suçları genel olarak "bilişim sistemleri aracılığıyla işlenen suçlar" ve "bilişim alanındaki suçlar-bilişim suçları" olarak ikiye ayrılmaktadır. İlk gruptaki suçlar geleneksel suçların bilişim ortamında işlenmiş şeklidir. E-posta aracılığıyla tehdit bu grupta işlenen suçlara örnektir. İkinci gruptaki bilişim suçları kapsamına giren suçlardır. Bilişim suçu genel olarak "Bilişim alanındaki gelişmelere paralel artış gösteren ve teknolojinin yardımı ile genellikle sanal bir ortamda kişi veya kurumlara maddi veya manevi zarar verecek davranışta bulunmaktır" [13] olarak tanımlanmaktadır. Bir suçun bilişim suçu kategorisine girebilmesi için;

• "İşlenmesinde ve soruşturulmasında teknik bilgi gerekir, bilgi paylaşımı son derece hızlı ve geniş kapsamlıdır,
• Soruşturma aşamasında kanuni ve teknik zorluklar kaçınılmazdır,
• Olası suç yöntemleri hayal gücü ile sınırlıdır,
• Sınır ötesi suçlardan olduğu tartışılmazdır" [13] Özelliklerini taşıması gerekmektedir.

Çalışmamız kapsamında sosyal medyada sıkça görülmesi mümkün zaman zaman gazete ve haberlere konu olmuş suçlar ele alınmıştır. Bu suçlar alt başlıklar halinde kısaca açıklanmıştır.

2.1 Yetkisiz Erişim

Yetkisiz erişim fiili, bilişim sistemlerinde en eski, en yaygın ve en çok bilinen bilişim suçu türüdür. Kişilere veya kurumlara ait Facebook sayfalarına erişerek sistemin yetkisiz kişilerce kullanılması ve sistemde yer alan verilere ulaşılması olayıdır. Sisteme yetkisiz kişi ya da kişiler tarafından bilgisayara yakın bir yerden erişilebileceği gibi uzak bir mesafeden, internet üzerinden de erişim mümkün olabilmektedir.

Yetkisiz erişim yöntemleri genel olarak iki sınıfta incelenmektedir. Bunlardan ilki kullanıcı tabanlı yetkisiz erişimlerdir. Kullanıcı tabanlı yetkisiz erişim yöntemlerinde herhangi bir teknik unsur kullanmadan doğrudan kullanıcının dikkatsizlik, dalgınlık veya tecrübesizlik gibi zayıf yönlerinden yararlanılmaktadır. Bu sınıfta en yaygın olarak kullanılan yöntem kişilerin parolasını unutması durumdan cevaplaması istenilen güvenlik sorusunun tahmin edilmesidir. Bu sınıfta kullanılan bir diğer yöntem ise "omuz sörfü" olarak ifade edilen kullanıcıların erişim parolarını yazarken gözlenmesi, ajanda ve not kağıtları gibi parola yazılabilecek materyallerin incelenmesi ile parolaların elde edilmesidir.

İkinci sınıfta ise yazılım tabanlı yetkisiz erişimler yer almaktadır. Yazılım tabanlı yetkisiz erişim yöntemlerinde bir bilişim sistemine erişim için; sözcük atağı (dictionary attackt), kaba kuvvet algoritmaları (brute force attackt), trojen, keylogger ve screen logger gibi algoritmalar kullanılmaktadır.

Sözcük atağı yönteminde temel olarak bir metin dosyasındaki sözcüklerin otomatik olarak hedeflenen sistemdeki parola yerine denenmesi ile erişim sağlanmaktadır. Bu yöntemde eğer sisteme erişim parolası, oluşturulan metin dosyasındaki kayıtlı verilerden birisi ise erişim sağlanmaktadır.

Kaba kuvvet algoritmaları yönteminde ise bir sistemin parolasını, bütün harf, rakam ve özel karakter kombinasyonlarını kullanan bir algoritma aracılığıyla çözümlenmektedir. Bu yöntemde parola ne kadar karmaşık ve uzun olursa olsun mutlak suretle sonuç elde edilmekte ve sisteme giriş için gerekli parola elde edilmektedir.

Tuş kaydedici yazılımlar ile de kullanıcının klavyeden basmış olduğu tuşlar, basım sırasına göre kayıt edilmekte ve daha sonra e-posta veya uzaktan erişim yöntemi ile bu dosya ve dolayısıyla içerisinde yer alan bilgilere ulaşılabilmektedir.

Ekran kaydedici yazılımlar sayesinde de kullanıcının her fare hareketi ile tıklama olayında ekran görüntüsü kaydedilmekte ve daha sonra e-posta ya da uzaktan erişim ile bu kayıtlı bilgiler elde edilmektedir.

Yetkisiz erişim için kullanılan bir diğer yöntemde Truva atlarıdır. Truva atları, kullanıcı bilgisayarında açılışta çalışma özelliği bulunan gizli bir sunucu oluşturarak bütün sistem kaynaklarını uzak sistemdeki kişinin kullanmasını sağlayan, bilgisayarda yapılan bütün işlemleri izleme, dinleme ve müdahale etme yetkisini uzak sisteme devreden yazılım türleridir.

Ortadaki adam saldırıları yönteminde ise sahte arayüzler kullanılarak erişim bilgileri elde edilir. Örneğin Facebook giriş sayfası tasarımsal olarak birebir taklit edilerek oluşturulan bir arayüz hedefteki kişiye e-posta atılarak giriş yapması istenir. Kişinin dikkatiz davranması ve gönderilen linke tıklaması durumunda sahte Facebook arayüzü açılır kişi Facebook'a giriş yaptığını düşünerek erişim bilgilerini sisteme girer bunun üzerine sahte sistem bu giriş bilgilerini kaydeder ve kullanıcıyı gerçek sistem üzerine yönlendirir kullanıcı ise bir anlık parola ya da kullanıcı adı bilgilerini yanlış girdiğini düşünerek sisteme tekrar giriş yapmayı dener ve Facebook profiline erişir fakat bu arada erişim bilgileri elde edilmiş olur.

Yetkisiz erişim ile Facebook profiline ulaşılarak mağdur bırakılan birçok kişi vardır. Bunlar arasında sanatçı Yıldız Tilbe de bulunmaktadır. Sanatçı Yıldız Tilbe, Facebook hesabının çalınarak bu hesap üzerinden insanlara hakaretler ve küfürler edildiğini belirterek savcılığa suç duyurusunda bulunmuştur [17].

2.2 Sahte Kişilik Oluşturma ve Kişilik Taklidi

Kendisine veya bir başkasına menfaat sağlamak veya zarar vermek amacıyla gerçek kişilerin taklit edilmesi veya hayali kişilerin oluşturulmasıdır. Bu yöntemle gerçek kişilerin arkasına saklanılmakta ve o kişi muhtemel bir suçlu durumuna düşürülmekte ya da ortada hiç olmayan bir kişiye ait profille kişi kendini saklamaya çalışmaktadır. Örneğin ünlü diyetisyen Canan Karatay adına oluşturulan bir hesapta "Gıda mühendisliği diye bir saçmalık çıktı! Gıda doğal olmalı neyin mühendisliği bu? Gıda mühendisliği olmaz" şeklinde paylaşımlar yapılmış bunun üzerine ise Gıda Mühendisleri Odası Adana Şube başkanı, Canan Karatay hakkında suç duyurusunda bulunmak için hukuki bir çalışma başlattıklarını açıklamıştır [16].

İzmir'de yaşanan bir olayda ise kanlılarını öldürmek isteyen kişiler bunun için Facebook'da bir kadın profili oluşturmuşlar ve oluşturdukları bu profil üzerinden kan davalıları ile iletişime geçip buluşma ayarlamışlar ve bu buluşmada kan davalılarını öldürülmüşlerdir [19].

2.3 Cinsel Taciz

Sosyal medyada sık görülen suçlardan birisi de cinsel tacizdir. Suçu düzenleyen TCK m. 105, cinsel taciz suçu için failin fiziksel temasını aramamış, mağduru "cinsel amaçlı olarak taciz etmek" davranışını suç için yeterli görmüştür [11]. Bu nedenle sosyal ağlar üzerinden bir kimseye karşı cinsel içerikli sözler söylemek veya bu amaçla görseller paylaşmak tarzındaki eylemler cinsel taciz suçu kapsamına girmektedir.

2.4 Sanal Kumar

Online Kumar, e-kumar, internette kumar, online Casino veya sanal kumar gibi değişik ifadeler ile adlandırılmaktadır. Sanal kumarın hukuki olarak bir tanımı yapılmamıştır. Ancak "bilişim ortamlarında, şansa ve beceriye dayanan, oyun araç ve gereçleri ile veya bir kasaya karşı para veya benzeri maddi değerler karşılığı oynatılan oyunlardır." [1] Olarak tanımlanabilmektedir.

Sanal Kumar, internet ortamında beliren en önemli tuzaklardan birisidir. Kumar bağımlılığının internet ortamına taşınmasıyla, internet kullanımının bir bağımlılık halini alması, internete istenilen anda bilgisayarlardan, telefonlardan, akıllı televizyonlardan kolaylıkla ulaşılabilmesi internette kumar oynama alışkanlığı daha güçlü bir bağımlılık haline almasına neden olmaktadır. Ayrıca bu ortamın denetimsiz olması internet erişiminin ise sanal kumar bağımlığını artırmaya yönelik bir diğer tehdittir.

2.5 Müstehcenlik ve Çocuk Pornografisi

TCK 226. Maddesi, çocukları müstehcen görüntü, ses ya da yazıya maruz bırakmayı, gerekse de müstehcen görüntü, ses ya da yazı içeren ürünlerde çocukların kullanılması suç

olarak tanımlamıştır. Ayrıca müstehcen malzeme kullanımı bazı etik ve ahlaki sorunları da beraberinde getirmektedir.

Pornografinin serbest bırakılmasıyla internet pornografisi giderek uçlara savrulmakta saldırgan pornografi türleri çoğalmaktadır. Agresif pornografinin önemli bir bölümü tecavüz mitini çoğaltmaktadır [6].

İnternette her türlü içeriğin çok kolay bir şekilde yayılması nedeniyle bu tür materyaller bulmayı aklından bile geçirmeyen ve görmek de istemeyen yetişkinlerin dahi karşısına pornografik görüntüler çıkabilmektedir. Bu tür görüntülerden tamamıyla yetişkin bireylerin bile kendisini koruyamadığı ortamda küçük yaşlarda internet ve sosyal medya ile tanışan çocukları olumsuz etkilemektedir.

2.6 İstem Dışı Alınan Elektronik Postalar (Spam)

Spam, internet üzerinde aynı mesajın yüksek sayıdaki kopyasının, bu tip bir mesajı alma talebinde bulunmamış kişilere zorlayıcı nitelikte gönderilmesidir [1]. Spam elektronik postaların, posta kutularımızı doldurmasına sebep olan kişilere ise spammer denilmektedir. Reklam, pornografik yayınlara kişileri sokmak, ideolojik görüşleri geniş kitlelere iletmek veya kanun dışı ürünleri ya da ilanları pazarlamak amacıyla spammerlar spam postalar göndermektedir.

2.7 Kişilere Tehdit ve Şantaj

Sözlü yazılı veya görsel şekilde işlenen klasik tehdit ve şantaj suçları gibi sosyal medya üzerinden işlenen tehdit ve şantaj suçları da, tipik fiilde belirtilen unsurları taşıdıkları sürece bu hükümlere göre suç unsuru teşkil etmektedir.

Kişilerin Facebook profillerine yetkisiz kişiler tarafından erişilerek özel bilgilerinin ele geçirilmesi ya da paylaştığımız bir içerik, tanıdığımız veya tanımadığımız kişiler tarafından tehdit ve şantaj amaçlı kullanılabilmektedir.

Adıyaman da yaşanan bir olayda 25 yaşında bir kişi liseli kızların Facebook adreslerine yetkisiz olarak erişerek, kızların resimlerini ve özel bilgileri ele geçirmiştir. Daha sonra bu kızlara ulaşarak resimler üzerinde oynama yapacağı ve elde ettiği özel bilgiler ile birlikte internet sitelerine atacağını söyleyerek tehdit eden şahıs, kişilerden para ve ilişki isteğinde bulunmuştur. Şahıs bu yöntemle yaklaşık 100 kızın Facebook hesabını ele geçirerek şantajda bulunmuştur. Kızlardan birisinin emniyete şikayeti üzerine ise kişi yakalanmıştır [18].

Ankara'da ise Facebook'da tanıştığı kadınlara korsan yazılım göndererek kişisel bilgilerini ele geçirerek şantajda bulunduğu iddia edilen bir kişi yakalanmıştır. Zanlının kadınlar adına sahte profil adresleri oluşturduğu ve bu adreslerde kişilerin ele geçirdiği fotoğraflarıyla birlikte pornografik fotoğraflar ve videolar yükleyerek kadınları tehdit ettiği iddia edilmektedir. Ayrıca sahte adreslerle kişilerin aile ve iş yerinden arkadaşlarına ulaşarak adına sahte hesap oluşturulan kişilerin fuhuş yaptığı söylenerek ve hatta emniyet ve sosyal politikalar bakanlığı aranarak fuhuş yapıyor çocuğunu elinden alın ihbarlarında bulunduğu belirtilmektedir. Kişisel bilgileri çalınarak adına sahte hesaplar oluşturulan kişilerden para ve birlikte olma teklifi ile şantaja boyun eğmeye zorlandığı iddia edilmiştir. Bu yolla 90 kadına şantajda bulduğu iddia edilmektedir [23].

2.8 Kanunsuz Silah Satışı

İnternet ortamında elektronik posta, web sayfalarında, chat kanallarında tanıtım ve pazarlama yöntemleri ile silah satışının yapılmasıdır.

Libya'da 23 yaşında bir genç Facebook'da kurulan bir grupta yer alan fotoğraflı silah ilanına yanıt vermesi üzerine şehrin tam ortasında silah satışı gerçekleştirilmiştir [20].

2.9 Uyuşturucu Ticareti

İnternet ortamında elektronik posta, web sayfaları, chat kanalları, sesli ya da görsel iletişim teknikleri ile uyuşturucunun imalatı ya da nerelerden alınabileceğine yönelik uyuşturucu ticaretinin yapılması ve yönetilmesine yönelik yapılan eylemlerdir.

İstanbul il Jandarma Komutanlığı ekipleri sosyal medya üzerinden "Bonza-i Jamaican Gold" adlı uyuşturucu maddesinin satışının yapıldığı iddia edilen adrese baskın gerçekleştirmiştir. Sosyal Medya'da "Corvus Corvinus" takma adıyla oluşturulan hesaptan söz konusu uyuşturucu maddenin satışının yapıldığı ortaya çıkmıştır [21].

2.10 Organ Ticareti

İnternet ortamında elektronik posta alıp verme yoluyla, chat yaparak veya internet üzerinden sesli veya görsel iletişim tekniklerinden faydalanılarak kişinin kendi isteği veya zorla bir başkasına ait organların alınması yoluyla işlenen suçlardır.

Antalya polisi tarafından düzenlenen bir operasyonda organ ticareti yapan bir grubun Facebook üzerinden bir grup açarak organlarını satmak isteyen kişileri buldukları ve daha sonra organ nakli bekleyen varlıklı hastaları tespit ederek sahte

evraklarla organ nakli gerçekleştirdiklerini ortaya çıkarmıştır. 2012 yılında haber olan bu olayda örgütün, organ nakli olan kişilerden 40 bin ile 80 bin lira arasında para aldığı, organ verenlere ise 15 bin ile 20 bin arasında para verdiği iddia edilmiştir [22].

3. Anket Çalışması

Yapılan anket çalışmasının problemi, amacı, örneklemi, anketin oluşturulması, uygulanması ve sonuçları alt başlıklar halinde açıklanmıştır.

3.1 Problem

Çok hızlı ve denetimsiz bir şekilde büyüyen sosyal ağlarda bilişim suçlarının takibinin yapılamaması.

3.2 Amaç

Çalışmada Facebook sosyal ağı üzerinde en çok karşılaşılan suçların tespit edilmesi.

3.3 Örneklem

Gelişigüzel örnekleme yani herhangi bir şekilde evrenin bir parçası seçilmesi yöntemi ile örneklem kümesi oluşturulmuştur. Örneklemimiz internet kullanıcısı 224 kişiden oluşmaktadır. Araştırmacılara kolaylık olması için α=0.05, α=0.03, α=0.10 örnekleme hataları için farklı evren büyüklüklerinde çekilmesi gereken örneklem büyüklükleri Tablo 1'de gösterilmektedir [25].

	±0.03 örnekleme hatası (d)			±0.05 örnekleme hatası (d)			±0.10 örnekleme hatası (d)		
p= q=	0.5 0.5	0.8 0.2	0.3 0.7	0.5 0.5	0.8 0.2	0.3 0.7	0.5 0.5	0.8 0.2	0.3 0.7
100	92	87	90	80	71	77	49	38	45
500	341	289	321	217	165	196	81	55	70
750	441	358	409	254	185	226	85	57	73
1000	516	406	473	278	198	244	88	58	75
2500	748	537	660	333	224	286	93	60	78
5000	880	601	760	357	234	303	94	61	79
10000	964	639	823	370	240	313	95	61	80
25000	1023	665	865	378	244	319	96	61	80
50000	1045	674	881	381	245	321	96	61	81
100000	1056	678	888	383	245	322	96	61	81
1000000	1066	682	896	384	246	323	96	61	81
100 milyon	1067	683	896	384	245	323	96	61	81

Tablo 1. Farklı örneklem hataları için çekilmesi gereken örneklem büyüklükleri

Anket başında olabildiğince çok katılımcıya ulaşarak hata aralığının düşük tutulması hedeflense de istenilen sayıda katılımcıya ulaşılamamış çalışma 224 kişi ile sınırlı kalınmıştır. Tablo 1'e bakıldığında 224 kişilik bir örneklemden elde edilecek bilgiler +- %10 hata aralığında gerçek kitleyi temsil edeceği görülmektedir.

3.4 Anketin Oluşturulması

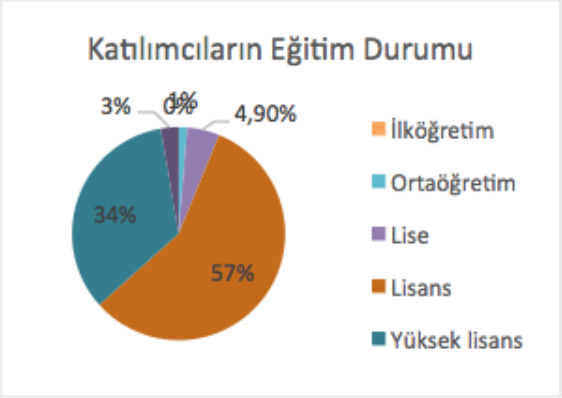
Anket oluşturulurken belirlenen anket amacı doğrultusunda sorular teknik ifadelerden uzak örneklem hedefindeki herkesin sorulan soruyu net anlayıp aynı anlamı çıkarması için yalın ve basit düzeyde hazırlanmıştır. Sorular hazırlandıktan sonra farklı yaş ve bilgi grubundaki 10 denek üzerinde yüzyüze anket yöntemi uygulanarak soruların anlaşılırlığı test edilmiştir.

3.5 Verilerin Toplanması

Anketimiz internet tabanlı anketform internet sitesinde oluşturulmuştur [24]. Anket internet ortamında yayınlanarak dağıtılmış ve gönüllü kişilerin katılımı ile çalışma gerçekleştirilmiştir.

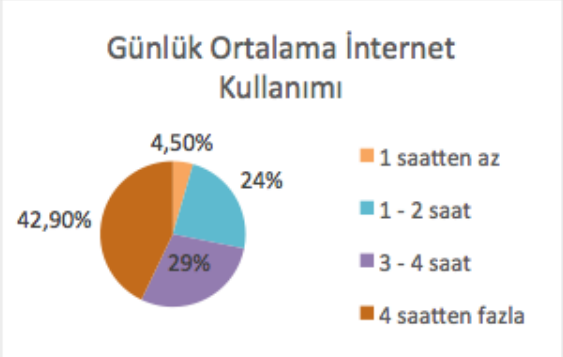
3.6 Anket Sonuçlar

Anket çalışmasında sorulan "Facebook kullanmakta mısınız?" sorusuna 4 katılımcı hayır 220 katılımcı evet cevabını vermiştir. Anket katılımcı sayısı, 120 erkek 104 bayan toplam 224 kişiden oluşmaktadır. Katılımcı yaş aralığı 17-55 aralığında değişmektedir. Katılımcıların ortalama yaşı 27'dir. Anket katılımcıları arasında ilkokul mezunu bulunmamaktadır. 3 kişi ortaöğretim mezunu, 11 kişi lise mezunu, 128 kişi üniversite mezunu, 76 kişi yüksek lisans mezunu ve 6 kişide eğitim durumunu diğer olarak belirtmiştir. Şekil 1'de anket katılımcılarının eğitim durumu yüzdelik dilimlerini gösteren pasta grafiği görülmektedir.



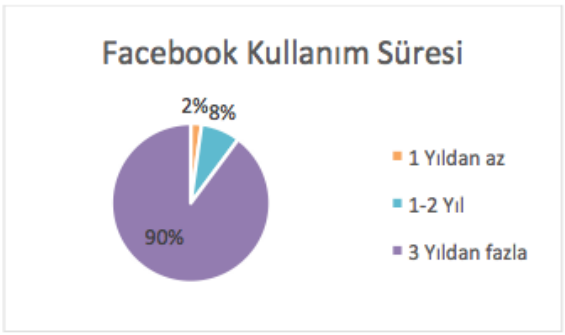
Şekil 1. Katılımcıların eğitim durumu

"İnterneti günde ortalama kaç saat kullanıyorsunuz" sorusuna katılımcılardan 10 kişi 1 saatten az, 53 kişi 1 – 2 saat arasında, 65 kişi 3-4 saat arasında 96 kişide 4 saatten fazla internet kullandığı cevabını vermiştir. Sonuçlar Şekil 2'de görülmektedir.



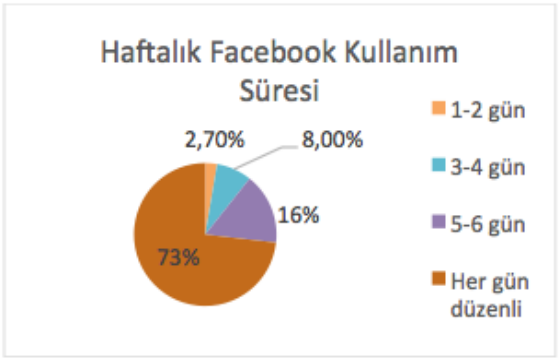
Şekil 2. Katılımcıların günlük ortalama internet kullanım oranı

"Ne kadar zamandır Facebook kullanıyorsunuz?" soruna katılımcıların 5'i 1 yıldan az, 18'i 1- 2 yıl, 201 kişide 3 yıldan fazla Facebook kullanıcısı olduklarını belirtmişlerdir.



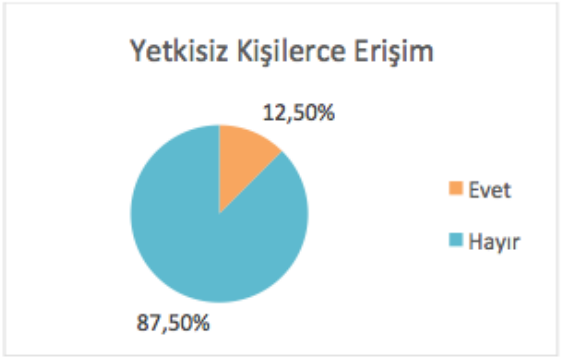
Şekil 3. Facebook kullanım süresi

"Haftada kaç gün Facebook kullanıyorsunuz?" sorusuna katılımcıların 6'sı 1-2 gün, 18'i 3-4 gün, 36'sı 5-6 gün, 164'ü her gün düzenli cevabını vermiştir. Şekil 4'de elde edilen sonuçların grafiği gösterilmektedir.



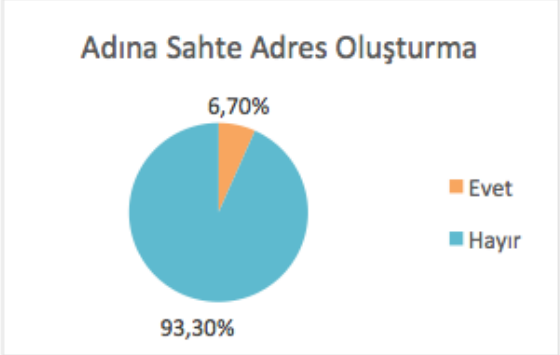
Şekil 4. Haftalık Facebook kullanım süresi

"Size ait Facebook adresinize yetkisiz kişilerce giriş yapıldı mı?" sorusuna katılımcıların 28'i evet, 196'sı hayır cevabını vermiştir. Şekil 5'de yetkisiz kişilerce erişim suçu ile karşılaşılma durumunu gösteren grafik görülmektedir.



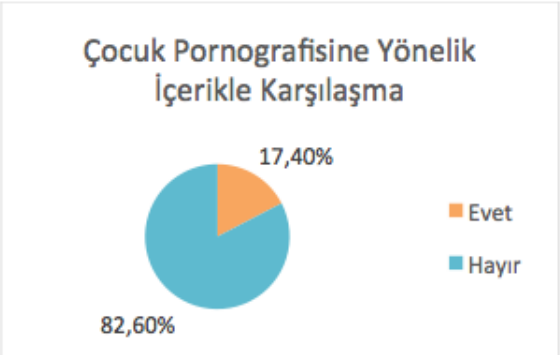
Şekil 6. Yetkisiz kişilerce erişim

"Facebook üzerinden adınıza sahte adres oluşturularak size zarar verilmeye çalışıldı mı?" sorusuna katılımcıların 15'i evet, 209'u hayır cevabını vermiştir. Şekil 7'de adına sahte adres oluşturulan katılımcıların oranını gösteren grafik görülmektedir.



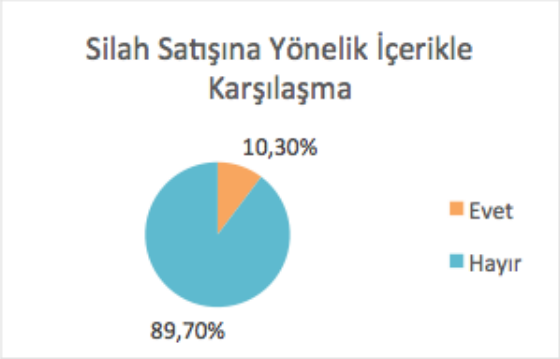
Şekil 7. Adına sahte adres oluşturulması

"Facebook üzerinden çocuk pornografisine yönelik bir içerikle karşılaştınız mı?" sorusuna katılımcılardan 39'u evet, 185'i hayır cevabını vermiştir. Şekil 8'de elde edilen sonuçların grafiği gösterilmektedir.



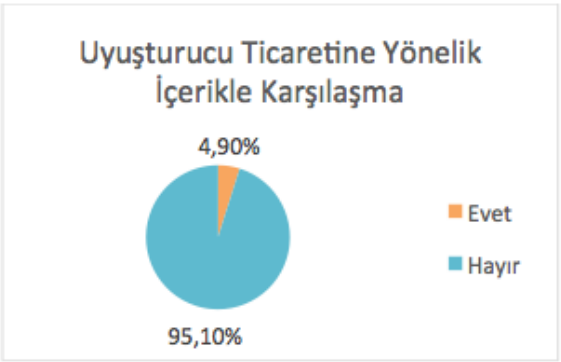
Şekil 8. Çocuk pornografisine yönelik içerikle karşılaşılma

"Facebook üzerinde silah satışına yönelik bir içerikle karşılaştınız mı?" sorusuna katılımcıların 23'ü evet, 201'i hayır cevabını vermiştir. Sonuçları gösteren grafik Şekil 9'da görülmektedir.



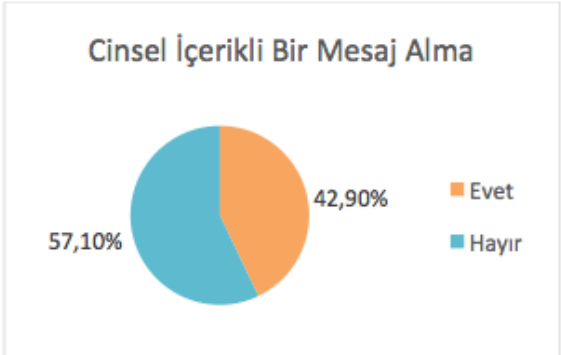
Şekil 9. Silah satışına yönelik içerikle karşılaşılma

"Facebook üzerinde uyuşturucu ticaretine yönelik bir içerikle karşılaştınız mı?" sorusuna katılımcıların 11'i evet, 213'ü hayır cevabını vermiştir. Elde edilen sonuçlar Şekil 10'da görülmektedir.



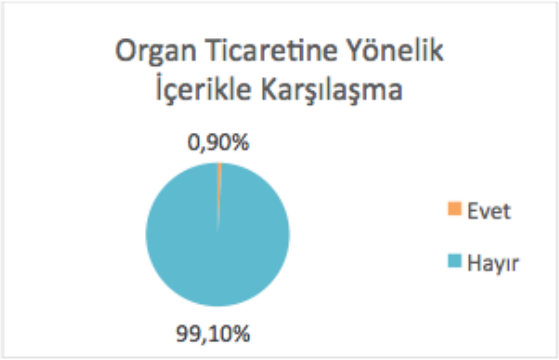
Şekil 10. Uyuşturucu ticaretine yönelik içerikle karşılaşma

"Facebook üzerinden cinsel içerikli bir mesaj aldınız mı?" sorusuna katılımcıların 96'sı evet, 128'i hayır cevabını vermiştir. Sonuçlar grafiksel olarak Şekil 10'da görülmektedir.



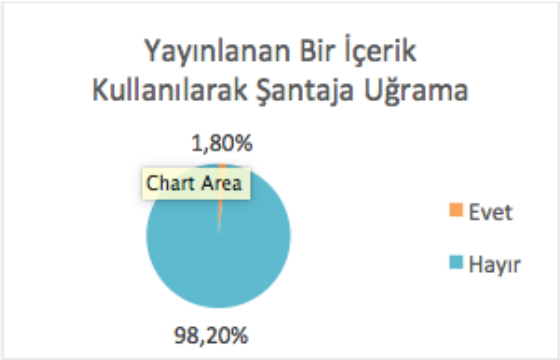
Şekil 10. Cinsel içerikli mesaj alanların oranı

"Facebook üzerinden organ ticaretine yönelik bir içerikle karşılaştınız mı?" sorusuna katılımcıların 2'si evet, 222'si hayır cevabını vermiştir. Elde edilen sonuçların grafiksel gösterimi Şekil 11'de gösterilmektedir.



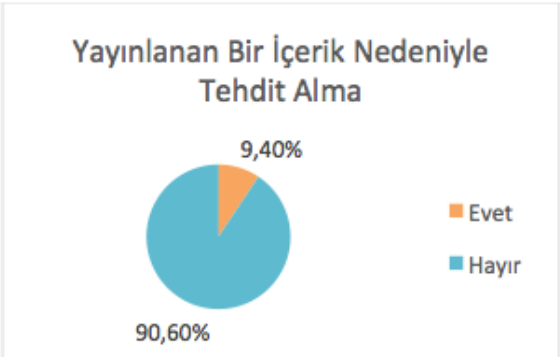
Şekil 11. Organ ticaretine yönelik içerikle karşılaşma oranı.

"Facebook profilinden yayınladığınız bir içerik kullanılarak şantaja uğradınız mı?" sorusuna katılımcıların 4'ü evet, 220'si hayır cevabını vermiştir. Şekil 12'de verilen cevapların oranı gösterilmektedir.



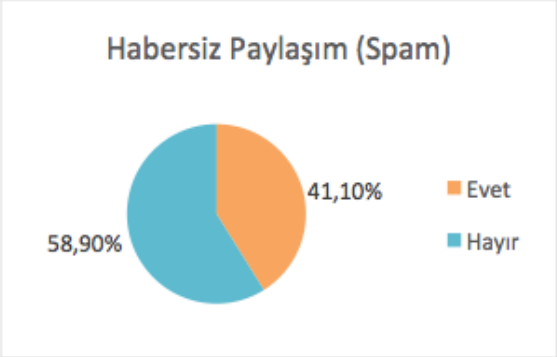
Şekil 12. Yayınlanan bir içerik kullanılarak şantaja uğrama

"Facebook profilinizden yayınladığınız bir içerikten dolayı tehdit edildiniz mi?" sorusuna katılımcıların 21'i evet, 203'ü hayır cevabını vermiştir. Sonuçlar Şekil 13'de görülmektedir.



Şekil 13. Yayınlanan bir içerik nedeniyle tehdit alma.

"Facebook üzerinden sizin onayınız olmadan paylaşım yapıldı mı?" sorusuna katılımcıların 92'si evet, 132'si hayır cevabını vermiştir. Şekil 14'de sonuçlar görülmektedir.



Şekil 14. Habersiz paylaşım

Sonuç

Çalışmada anket sonuçlarından elde edilen bilgiler göz önünde bulundurularak anket katılımcılarının en çok cinsel içerikli mesaj alma durumuyla cinsel taciz suçuna maruz kaldıkları görülmüştür. Facebook sosyal ağı üzerinde en çok karşılaşılan suçlar sırasıyla;

1. Cinsel taciz (katılımcıların %42.9'u)
2. İstem dışı alınan elektronik postalar (Spam) (%41.1)
3. Çocuk pornografisi (%17.4)
4. Yetkisiz kişilerce erişim (%12.5)
5. Silah Satısı (%10.3)
6. Paylaşılan bir içerik nedeniyle tehdit edilme (%9.4)
7. Adına sahte adres oluşturularak zarar verme (%6.7)
8. Uyuşturucu ticareti (%4.9)
9. Paylaşılan bir içerik nedeniyle şantaj (%1.8)
10. Organ ticareti (%0.9)

olduğu gözlenmiştir.

Çalışma gelişigüzel örnekleme yöntemi ile örneklendirilmiş ve 224 katılımcıya ulaşılabilmiştir. Örneklem sonucu elde edilen veriler +- %10 hata düzeyine sahiptir. Çalışma daha büyük kitleler üzerinde uygulanarak katılımcı sayısı artırılarak hata oranı düşürülebilir. Çalışmada örneklem çoğunluğunun %57 ile lisans mezunları, %34 ile yüksek lisans mezunları oluşturmaktadır. Bu verilerde aslında anket
katılımcılarının bilgisayar ve internet konusunda bilgili bir kitlenin ağırlıkta olduğunu göstermektedir ankete katılımcı sayısı artırılarak eğitim durumuna göre tabakalı örnekleme yöntemi kullanılarak örneklemin ana kitleyi temsil etme gücü artırılabilir. Fakat en doğru genelleme için Facebook kayıtlı üyelerinin eğitim durumu dağılımının da bilinmesi gerekmektedir.

Anket çalışması sonrası elde edilen veriler kota örnekleme yöntemi ile evren sınırlandırılarak lisans ve sonrası eğitim düzeyine sahip kişilerin Facebook sosyal ağında en çok maruz kaldıkları suçlara yönelik bir çalışma da gerçekleştirilebilir.

Facebook ve benzeri sosyal ağlarda suç oranını azaltmak ya da bu suç oranlarının artmasına engel olabilmek için yine aynı ağlar üzerinden çalışmalar yürütülmelidir. Bu çalışmalar için Facebook grupları sayfaları oluşturulmalıdır. Facebook üzerinden yapılacak paylaşımlar ile kişilerin bireysel alabilecekleri önlemler ve karşılaştıkları olumsuz bir olayda başvuru yapabilecekleri kaynaklar konusunda bilgilendirme yapılmalıdır.

Ayrıca cinsel taciz, çocuk pornografisi, ya da sanal kumar gibi özünde kendisine ya da bir başkasına zarar vermek olan bu tür eylemlerin kişilerde ileride yaratacağı olumsuz durumlara yönelik bireyler bilinçlendirilerek kişilerin farkındalık düzeyi artırılmalı kişilerin bu tür suç içeriklerini önemsiz olarak görerek yönelmelerinin önüne geçilmeli ve vazgeçirilmelidir.

Kaynaklar

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

[2] Burak T. B. (2012) Bilişim Suçları ve Üniversite Lisans Öğrencilerinin Bilişim Suçlarına Yönelik görüşleri, Gazi Üniversitesi Bilişim Enstitisü, Yüksek Lisans Tezi , Ankara

[3] Büyükşener, E. (2009). Türkiye'de Sosyal Ağların Yeri ve Sosyal Medyaya Bakış, XIV. Türkiye'de İnternet Konferansı Bildirileri, Bilgi Üniversitesi, İstanbul

[4] Dikme G.,(2013). Üniversite Öğrencilerinin İletişimde ve Günlük Hayatta Sosyal Medya Kullanım Alışkanlıkları: Kadir Has Üniversitesi Örneği, Yüksek Lisans Tezi, İstanbul

[5] Dijle H., Doğan N. (2011) Türkiye'de Bilişim Suçlarına Eğitimli İnsanların Bakışı, Bilişim Tekonolojileri Dergisi, Cilt 4, Sayı 2

[6] Denizci M. (2009) Bilişim Toplumu Bağlamında İnternet Olgusu ve Sosyolojik Etkileri, Mar-

mara İletişim Dergisi, Sayı 15, Marmara Üniversitesi iletişim Fakültesi, İstanbul

[7] Gözüşirin M. "5237 Sayılı Türk Ceza Kanununda Bilişim Suçları ve Bilişim Suçları ile Mücadeleye İlişkin Model Önerisi", Yüksek Lisans Tezi, T.C. Kara Harp Okulu Savunma Bilimleri Enstitüsü Güvenlik Bilimleri Anabilim Dalı, 2011

[8] Kalaman S. (2011) İnternette Özel Hayatın Gizliliğinin İhlal Edilmesi: Facebook, Selçuk Üniversitesi sosyal Bilimler Enstitüsü Radyo Televizyon Anabilim Dalı Radyo Televizyon Bilim Dalı, Yüksek Lisans Tezi, Konya

[9] Koç S. (2013). Hukuksal Bağlamda Sosyal Medya Analizi ve Kıyaslamalı Mevzuat Önerileri, İstanbul Bilgi Üniversitesi Sosyal Bilimler Enstitüsü Hukuk Yüksek Lisans Programı, İstanbul

[10] Koç S., Kaynak S. "Bilişim Suçları Bağlamında Yeni Medya Olarak İnternet ve Kişisel Güvenlik", Akademik Bilişim 2010, Muğla

[11] Özocak G. (2013). Sosyal Medyada İşlenen Suç Tipleri ve Suçluların Tespiti, Yeni Medya Çalışmaları I. Ulusal Kongresi, Kocaeli Üniversitesi, Kocaeli

[12] Taş İ. M. "Bilgisayar Tabanlı Bilişim Suçlarının Adli Bilişim Çerçevesinden İncelenmesi", Yüksek Lisans Tezi, Marmara Üniversitesi Fen Bilimleri Enstitüsü, İstanbul, 2013

[13] Taş K. A. "Bilişim Suçları ve Adana İlinde 2006-2009 Yılları Arasında Meydana Gelen Bilişim Suçlarının Değerlendirilmesi"

[14] Tulum İ. (2006). Bilişim suçları ile Mücadele, Süleyman Demirel Üniversitesi Sosyal Bilimler Enstitüsü Kamu Yönetimi Anabilim Dalı, Yüksek Lisans Tezi, Isparta

[15] İnternet: http://www.campaigntr.com/2014/02/20/68209/facebook-turkiye-rakamlarini-acikladi/
Son erişim tarihi:09.12.2014

[16] internet: http://www.samanyoluhaber.com/medya/Canan-Karataya-Facebook-tuzagi/1041779/
Son erişim tarihi: 09.12.2014

[17] internet: http://www.sabah.com.tr/Gunaydin/2013/10/23/yildiz-tilbe-calinan-facebook-hesabinin-pesine-dustu
Son erişim tarihi: 09.12.2014

[18]internet: http://www.sabah.com.tr/Yasam/2013/04/14/facebook-sapigi-yakalandi
Son erişim tarihi: 09.12.2014

[19]internet: http://www.sabah.com.tr/Yasam/2012/07/28/oyle-bir-tuzak-kuruldu-ki
Son erişim tarihi: 09.12.2014

[20]internet: http://www.bbc.co.uk/turkce/basinozeti/2013/09/130918_basin_ozeti.shtml
Son erişim tarihi: 09.12.2014

[21] İnternet:
http://www.beykozguncel.com/1651-facebook-uzerinden-uyusturucu-satisi.html
Son erişim tarihi: 09.12.2014

[22] İnternet: http://www.cnnturk.com/2012/saglik/01/11/facebookta.organ.ticareti/644389.0/index.html
Son erişim tarihi: 09.12.2014

[23] internet: http://www.hurriyet.com.tr/teknoloji/25998549.asp
Son erişim tarihi: 09.12.2014

[24] İnternet:
http://anketform.com/a/sosyalmedyadaislenenbilisimsuclari
Son erişim tarihi: 09.12.2014

[25] İnternet:
www.baskent.edu.tr/~matemel/courses/ornekleme_notlari
Son erişim tarihi:09.12.2014