

**T.C.
ÇUKUROVA ÜNİVERSİTESİ
BAĞIMLILIK VE ADLİ BİLİMLER
ENSİTİTÜSÜ
ADLİ BİLİMLER ANABİLİM DALI**

**BİLİŞİM SUÇ ARACI OLARAK MOBİL/AKILLI TELEFON
KULLANIMI: ADANA ÖRNEĞİ**

Charles SSERUTTE

**ADLİ BİLİMLER YÜKSEK LISANS PROGRAMI
YÜKSEK LISANS TEZİ**

DANIŞMANLAR

- 1. Danışman: Prof. Dr. Mete Korkut GÜLMEN**
- 2. Danışman Dr. Öğr. Üyesi Nuri EMRAHOĞLU**

ADANA - 2020

**T.C.
ÇUKUROVA ÜNİVERSİTESİ
BAĞIMLILIK VE ADLİ BİLİMLER
ENSİTİTÜSÜ
ADLİ BİLİMLER ANABİLİM DALI**

**BİLİŞİM SUÇ ARACI OLARAK MOBİL/AKILLI TELEFON
KULLANIMI: ADANA ÖRNEĞİ**

Charles SSERUTTE

**ADLİ BİLİMLER YÜKSEK LİSANS PROGRAMI
YÜKSEK LİSANS TEZİ**

DANIŞMANLAR

- 1. Danışman: Prof. Dr. Mete Korkut GÜLMEN**
- 2. Danışman Dr. Öğr. Üyesi Nuri EMRAHOĞLU**

**Bu tez Çukurova Üniversitesi Bilimsel Araştırma Projeleri tarafında FYL- 2019-
12157 Nolu proje ile desteklenmiştir.**

ADANA - 2020

KABUL VE ONAY

Adli Bilimler Anabilim Dalı

Adli Bilimler Yüksek Lisans Programı çerçevesinde yürütülmüş olan

“BİLİŞİM SUÇ ARACI OLARAK MOBİL/AKILLI TELEFON KULLANIMI: ADANA ÖRNEĞİ”

Adlı çalışma aşağıdaki jüri tarafından Yüksek Lisans tezi olarak kabul edilmiştir.

Tarihi: 16/ 06/ 2020

TEZ SINAV JÜRİSİ

Prof. Dr. Mete Korkut GÜLMEN

Başkan

Prof. Dr. Muzaffer SÜMBÜL

Üye

Doç. Dr. Neylan ZİYALAR

Üye

Doç. Dr. Sunay FIRAT

Üye

Dr. Öğr. Üyesi Nuri EMRAHOĞLU

Üye (2. Danışman)

Yukarıdaki tez, yönetim kurulunun/...../..... Tarih ve sayılı kararı
ile kabul edilmiştir.

Prof. Dr. Mete Korkut GÜLMEN

Bağımlılık ve Adli Bilimler Enstitüsü Müdürü

T.C. ÇUKUROVA ÜNİVERSİTESİ BAĞIMLILIK VE ADLİ BİLİMLER
ENSTİTÜSÜ
YÜKSEK LİSANS / DOKTORA TEZ ÇALIŞMASI
ETİK BEYANI

Çukurova Üniversitesi Bilimsel Araştırma ve Yayın Etiği Yönergesini okuduğumu ve anladığımı ve Çukurova Üniversitesi Bağımlılık ve Adli Bilimler Enstitüsü Tez Yazım Kurallarına uygun olarak hazırladığım bu tez çalışmada;

- Tez içinde sunduğum verileri, bilgileri ve dokümanları akademik ve etik kurallar çerçevesinde elde ettiğimi,
- Tüm bilgi, belge, değerlendirme ve sonuçları bilimsel etik kurallarına uygun olarak sunduğumu,
- Tez çalışmasında yararlandığım eserlerin tümüne uygun atıfta bulunarak kaynak gösterdiğimi,
- Kullanılan verilerde ve ortaya çıkan sonuçlarda herhangi bir değişiklik yapmadığımı,
- Tez olarak sunduğum bu çalışmanın özgün olduğunu,

bildirir, aksi bir durumda bu konuda hakkımda yapılacak tüm yasal işlemleri ve aleyhime doğabilecek tüm hak kayıplarını kabullendiğimi beyan ederim. 16 / 06 /2020


Charles SSERUTTE

Kayıtlı olunan Program : Adli Bilimler Tezli Yüksek Lisans
Tezin Konusu : Bilişim Suç Aracı Olarak Mobil / Akıllı Telefon
Kullanımı: Adana Örneği
Tezin Türü : Yüksek Lisans : X Doktora:
Danışmanın Adı-Soyadı : Prof. Dr. Mete Korkut GÜLMEN
Danışmanın İletişim Bilgileri:
Telefon : 0 530 777 41 047
E-Posta : mete.gulmen@gmail.com
Öğrencinin İletişim Bilgileri
Telefon : 0 507 598 24 85
E-Posta : charlessserutte@gmail.com
Adresi : Adana

**Bu belgenin Lisansüstü eğitim tezleri savunmaya alınmadan önce öğrenci tarafından doldurulup imzalanarak Enstitü Müdürlüğüne teslim edilmesi gerekmektedir.*

TEŞEKKÜRLER

İlk olarak Türk Hükümeti ve Çukurova Üniversitesi'ne hayalimi gerçekleştirmeme izin verdikleri için şükranlarımı sunmak istiyorum. Tüm aile üyelerime doğumumdan bu yana bana verdikleri desteği hiç esirgemediklerinden dolayı teşekkür ederim; özellikle de bay C.K. Ssemakula'ya hayatım boyunca orada olduğu ve eğitim hayatım boyunca bana verdiği desteklerden dolayı çok teşekkür ederim. Ayrıca tezimi yazma fırsatı verdikleri için Çukurova Üniversitesi Bağımlılık ve Adli Bilimler Enstitüsü'ne teşekkür ederim.

Tez çalışmam boyunca yardımları ve önerileri için danışmanlarım Prof. Dr. Mete Korkut GÜLMEN ve Dr. Öğr Üyesi Nuri EMRAHOĞLU'na çok müteşekkirim. Çukurova Üniversitesi Bağımlılık ve Adli Bilimler Enstitüsü'ndeki tüm hocalarıma; Prof. Dr. Mete Korkut GÜLMEN'e, Prof. Dr. Necmi ÇEKİN'e, Prof. Dr. Ayşe SERİN'e, Doç. Dr. Nebile DAĞLIOĞLU'na ve Doç. Dr. Sunay FIRAT'a çok teşekkür ediyorum. Uganda Cumhuriyeti, Maliye Bakanı Müsteşarı Keith J. MUHAKANİZİ ve eşi Janet MUHAKANİZİ'ye destekleri için çok teşekkür ederim.

Balcalı Hastanesi Adli Tıp Anabilim Dalı asistan doktorlarına, özellikle Dr. Sıla ASLAN DEMİR, Dr. Kemal YILMAZ ve Dr. Ziya ELOĞLU'na yardımlarınız ve önerileriniz için teşekkür ederim. Tüm sınıf arkadaşlarıma ve Türk arkadaşlarıma; özellikle Kevser TURAN'a ve Mehmet Aykut ERK'e yardımları ve önerileri için çok teşekkür ediyorum. Tıp Fakültesi Adli Tıp Anabilim Dalı tüm araştırma görevlilerine çok teşekkür ediyorum.

Çukurova Üniversitesi, Bağımlılık ve Adli Bilimler Enstitüsü sekreteri Şener Elmas'a ve tüm Enstitü çalışanlarına teşekkür ediyorum.

Tezimi, büyükannem Alice NAKKU'ya ithaf ediyorum.

Charles SSERUTTE

İÇİNDEKİLER

KABUL VE ONAY	ii
ETİK BEYANI	iii
TEŞEKKÜRLER	iv
ŞEKİLLER DİZİNİ	vii
ÇİZELGELER DİZİNİ	ix
KISALTMALAR DİZİNİ.....	xi
ÖZET	xiii
ABSTRACT.....	xiv
1. GİRİŞ	1
1.1. Giriş.....	1
1.2. Çalışmanın Amacı	6
2. GENEL BİLGİ.....	7
2.1 Akıllı Telefon nedir?	7
2.2. Mobil Cihazların Özellikleri	7
2.3. Mobil Cihaz Güvenliği.....	8
2.4. Mobil Tehditler ve Saldırıları.....	8
2.5. Cihazlardaki Kötü Amaçlı Yazılımlar	8
2.6. Cihaz Arama ve El Koyma	9
2.7. Mobil Erişim Kontrolü.....	9
2.8. Bilgisayar Korsanları Tarafından Mobil Cihazlarda Yapılan Yaygın Siber Suçlar....	9
2.9. Mobil Cihazlarda Faaliyet Gösteren Siber Suç Türleri.....	10
2.10. Adli Mobil Cihaz Nedir?.....	13
2.11. Mobil Adli Bilimler Tarihi	14
2.12. Mobil Cihaz Mimarisi	15
2.13. Dosya Sistemleri	15

2.14. Adli Mobil Zorlukları.....	15
2.15. Cep Telefonundan Faydalı Bilgilerin Çıkarılması	16
2.16. SIM Kartlar ve SD Kartlar	17
2.17. SIM (Subscriber Identification Module) (Abone Kimlik Modülü).....	18
2.18. SIM Kart Üzerinde Hangi Bilgiler Bulunur?	18
2.19. SIM Kart İnceleme Araçları (26)	19
2.20. Mobil Cihazları Analiz Etmek	20
3. GEREÇ VE YÖNTEM.....	21
4. BULGULAR.....	23
4.1. Değerlendirme.....	57
5. TARTIŞMA	59
5.1. Elektronik Cihazlarda VPN Kullanımı	59
5.2. Sahte Sosyal Medya Hesapları.....	60
5.3. Sosyal Medya ve Suç	61
5.4. Akıllı Telefonlarda Kötü Amaçlı Yazılımlar	64
5.5. Akıllı Telefon Hırsızlığı.....	66
5.6. Akıllı Telefon Dolandırıcılığı ve Sahtekârlık	66
5.7. Uluslararası Mobil Ekipman Kimliği.....	69
6. SONUÇLAR VE ÖNERİLER.....	71
6.1. Sonuçlar	71
6.2. Öneriler	74
KAYNAKLAR	77
EKLER.....	82
EK 1. ANKET FORMU	82
ÖZGEÇMİŞ	86

ŞEKİLLER DİZİNİ

Şekil no	Sayfa no
Şekil 1. Kaynak; dünyada polis kayıtlarında olan suç dağılımı	4
Şekil 2. Katılımcıların yaşlarına göre dağılımları	24
Şekil 3. Katılımcıların Eğitim seviyesine göre sınıflandırılması.	25
Şekil 4. Katılımcıların akıllı telefonları sayısının dağılımı	26
Şekil 5. Katılımcıların akıllı telefon markalar sayısı dağılımı.	26
Şekil 6. Akıllı telefon kullanma amaç dağılımı.	27
Şekil 7. Katılımcıların akıllı telefon işletim sistem sayısı.	28
Şekil 8. Katılımcıların internet kullanma dağılımları.	29
Şekil 9. Katılımcıların internet kullanma amaç dağılımları.	29
Şekil 10. Akıllı telefonlarda katılımcıların VPN kullanma dağılımları.	30
Şekil 11. Katılımcıların günlük internet kullanma dağılımı	31
Şekil 12. Katılımcıların akıllı telefonda en çok kullandığı uygulamalar dağılımları.	32
Şekil 13. Sosyal medyada uygulamaları oluştururken gerçek adı ve soyadı kullanım dağılımları	33
Şekil 14. Katılımcıların birisinin tavsiye üzerine, sosyal medya uygulamalarının kullanımının dağılımları.	34
Şekil 15. Katılımcılara akıllı telefonlarına uygulamaları yüklerken, indirmeden önce uygulama şart ve koşullarını okuma dağılımları.	35
Şekil 16. Katılımcılara sosyal medya uygulamalar sahte hesap oluşturma dağılımları.	36
Şekil 17. Kullanıcıların, sahte bir Facebook hesabından rahatsız edilmelerinin yaşa göre dağılımları.	37
Şekil 18. Katılımcıların, sahte bir Twitter hesabından yaş göre rahatsız edilme dağılımları.	38
Şekil 19. Katılımcıların sahte bir hesapla Whatsapp'ta rahatsız edilmelerinin bir yaş göre dağılımları.	40
Şekil 20. Katılımcıların Instagramda sahte bir hesap kullanılarak rahatsız edilmelerinin yaşa göre dağılımları	41
Şekil 21. Katılımcıların rahatsız edilme diğer sosyal medya uygulamalar sahte hesabı kullanılarak yaş göre dağılımları	42
Şekil 22. Katılımcıların akıllı telefonlarda sosyal medyada siber takip veya zorbalığı muhatap olan dağılımları	43
Şekil 23. Katılımcıların konu bildiren uygulamalar tarafından takip edilme dağılımları.	44

Şekil 24. Bir bağlantısı yoluyla paylaşılan virüslerden katılımcılarının telefon işletim sistem olumsuz etkilenme oranlarının dağılımları.....	45
Şekil 25. Katılımcıların ikinci el akıllı telefonlar kullanma oranlarının dağılımları.....	46
Şekil 26. İkinci el akıllı telefon kullanırken katılımcıların sorun yaşama oranlarının dağılımları.....	47
Şekil 27. Katılımcılar izin almadan başkasına ait IMEI numarasını kullanma oranlarının dağılımları.....	48
Şekil 28. Katılımcılar başkasına ait IMEI numarası olan bir telefon kullanma oranları.....	49
Şekil 29. Katılımcılarının akıllı telefonlarının çalınma oranları.....	50
Şekil 30. Katılımcılarının akıllı telefon kişisel bilgileri tehlikeye atılma oranları.....	51
Şekil 31. Dolandırıcılardan telefonla aranma ya da mesaj alınma ve talepte bulunulanların oranları.....	52
Şekil 32. Katılımcılarının E-dolandırıcılık yaşama oranları.....	53
Şekil 33. Katılımcılar akıllı telefonlar ile kredi kartıyla alışveriş yapma dağılımları.....	54
Şekil 34. Akıllı telefonlarda kredi kartıyla alışveriş yaparken sorun yaşayanların oranları.....	55
Şekil 35. Akıllı telefonlarda banka uygulamalar kullanma dağılımları.....	56
Şekil 36. Akıllı telefonlarda banka uygulamalar kullanırken yaşayan sorunlar dağılımları.....	57

ÇİZELGELER DİZİNİ

Çizelge no	Sayfa no
Çizelge 1. Ankete cevap veren katılımcılar.	23
Çizelge 2. Katılımcılarının yaş guruplarına göre oranlarının dağılımları.	24
Çizelge 3. İnternet kullanma göre anketörlerin değerleri.	28
Çizelge 4. VPN kullanımına göre katılımcıların dağılımları.	30
Çizelge 5. Katılımcılarının, sosyal medyada uygulamaları oluştururken gerçek ad ve soyadı kullanıp kullanmadıklarının dağılımları.	33
Çizelge 6. Katılımcılara sosyal medya uygulamalarını tavsiye üzerine kullanma oranlarının dağılımları.	34
Çizelge 7. Katılımcıların soysal medya uygulamalar indirmeden şartlar ve koşullar okuma oranlarının dağılımları.	35
Çizelge 8. Katılımcıların sosyal medya uygulamalar sahte hesap oluşturma oranlarının dağılımları.	36
Çizelge 9. Sahte bir Facebook hesabından sosyal medyadaki biri tarafından rahatsız edilme oranlarının dağılımları.	37
Çizelge 10. Katılımcılara sahte bir Twitter hesabından sosyal medyadaki biri tarafından rahatsız edilme oranlarının dağılımları.	38
Çizelge 11. Katılımcılara sahte bir Whatsapta hesabı kullanılarak sosyal medyadaki biri tarafından rahatsız edilme oranlarının dağılımları.	39
Çizelge 12. Katılımcılara sahte bir Instagramda hesabı kullanılarak sosyal medyadaki biri tarafından rahatsız edilme oranlarının dağılımları.	41
Çizelge 13. Katılımcılara diğer sosyal medya uygulamalara sahte hesabı kullanılarak sosyal medyadaki biri tarafından rahatsız edilme oranlarının dağılımları.	42
Çizelge 14. Katılımcıların sosyal medyada sosyal medyada siber takip veya zorbalığı muhatap olan oranlarının dağılımları.	43
Çizelge 15. Katılımcıların akıllı telefonlarda konu bildiren uygulamalar tarafından takip edilme oranlarının dağılımları.	44
Çizelge 16. Bir bağlantı yoluyla paylaşılan virüslerden katılımcıların telefonlarının olumsuz etkilenme oranlarının dağılımları.	45
Çizelge 17. Katılımcıların ikinci el akıllı telefon kullanma oranlarının dağılımları.	46
Çizelge 18. İkinci el akıllı telefon kullanırken katılımcıların sorun yaşama oranlarının dağılımları.	47

Çizelge 19. Katılımcıların izin almadan başkasının İMEİ numarasını kullanma oranlarının dağılımlar. ...	48
Çizelge 20. Katılımcılar başkasının IMEI numarasını kullanırken yasal sorun yaşama oranlarının dağılımları.	49
Çizelge 21. Katılımcıların akıllı telefonlarının çalınma oranlarının dağılımları.	50
Çizelge 22. Katılımcıların akıllı telefonda bulunan kişisel bilgilerinin tehlikeye atılma oranları.	51
Çizelge 23. Katılımcıların E-dolandırıcılık yaşama oranlarının dağılımları.	52
Çizelge 24. Kredi kartlarıyla akıllı telefonlarında alışveriş yapanlar oranlarının dağılımları.	53
Çizelge 25. Akıllı telefonlarda kredi kartıyla alışveriş yaparken sorun yaşayanların oranlarının dağılımları. .	54
Çizelge 26. Akıllı telefonlarda banka uygulamalar kullanma oran.	55
Çizelge 27. Akıllı telefonlarda Banka uygulamalar kullanırken yaşayan sorunlar oranlarının.	56

KISALTMALAR DİZİNİ

OS	İşletim sistemi
ABD	Amerika Birleşik Devletleri
SMS	Kısa Mesaj Servis
MMS	Mülimedya mesaj
GSM	Mobil İletişim için Küresel Sistem
SIM	Abone Tanımlama Modülü
NFC	Yakın Alan İletişimi
URL	Tekdüzen Kaynak Bulucu.
ESN	Elektronik Seri Numarası
PDA	Kişisel Dijital Yardımcı.
GPS	Küresel Konumlama Sistemi
OEM	Orijinal Ekipman Üreticisi
PC	Kişisel Bilgisayardır
UFED	Fiziksel Analizde Kullanarak Mobil İnceleme Gerçekleştirme.
MPE	Medya İşleme Motoru
USB	Evrensel Seri Veri yolu
SD	Güvenli Sayısal Hafıza Kartı
ICCİD	Tümleşik Devre Kartı Kimliği
IMSI	Uluslararası Mobil Abone Kimliği
IIN	Verici Kimlik Numarasını
PIN	Kişisel Kimlik Numarası
SPN	Hizmet Sağlayıcı Adı
MM	Mobil Ülke Kodu
MNC	Mobil Şebeke Kodu

MSIN	Mobil Abone Kimlik Numarası
MSISDN	Mobil İstasyon Uluslararası Abone Dizin Numarası
ADN	Kısaltılmış Arama Numaraları
LDN	Son Aranan Numaralar
LP	Dil Tercihi
KC	Şifreleme Anahtarı
FDN	Sabit Arama Numaraları
TMSI	Geçici Mobil Abone Kimliği
RIA	Yönlendirme Alan Tanımlayıcı
SDNS	Servis Arama Numaraları.
AT	Yardımcı Teknoloji
VPN	Sanal Özel Ağ
TCK	Türk Ceza Kanunu
BBC	Britanya Yayın Şirketi
CNN	Kablolu Haber Ağı
TRT	Türkiye Radyo Televizyon Kurumu
CCTV	Kapalı Devre Televizyon
ECC-Net	Avrupa Tüketici Merkezleri Ağı
FBI	Federal Soruşturma Bürosu
CSIS	Stratejik ve Uluslararası Araştırmalar Merkezi
IMEI	Uluslararası Mobil Ekipman Kimliği

ÖZET

Yirmi birinci yüzyılın en önemli icatlarından biri akıllı telefonlardır ve insanların hayatlarında önemli bir rol oynamaktadırlar. Telefonla sesli konuşma, görüntülü konuşma ve arama, haberleşme, internet bankacılığı, cep bankacılık işlemleri, internet alış-verişleri, e-devlet, e-bilet, sınav belgeleri, sınav sonuçları, medya paylaşımları, mesajlaşma gibi örnekler, akıllı telefonların yaygınlaşmasıyla giderek artmıştır. Akıllı telefonların yaygınlaşmasıyla, insanların günlük yaşamlarını basitleştirmesine rağmen, beraberinde olumsuzlukları da getirmiştir. Kötü amaçlı akıllı telefon kullanımı hukuki sorunlarında artmasına ve kullanıcıların problem yaşamalarına da neden olmaya başlamıştır. Günümüzde akıllı telefonlarla yapılan suçlar da artmıştır. Genellikle mobil hırsızlık, mobil dolandırıcılık, mobil hack, hizmet engelleme saldırısı vb. gibi bir suçlarda artışlar meydana gelmeye başlamıştır.

Bu çalışmada temel olarak, akıllı telefonlar kullanılarak işlenen suçlara odaklanılmıştır. Çalışmada kullanıcıların akıllı telefonla ilgili yaşadıkları ve suç teşkilenden olayları yaşayıp yaşamadıklarıyla ilgili bilgiler toplamak amacıyla anket hazırlanmış ve anketörlerin cevaplaması için sorular yöneltmiştir. Katılımcılara akıllı telefonların kullanımı ve bu cihazları kullanırken karşılaştıkları sorunlarla ilgili sorulan soruların cevapları SPSS (23) istatistik programı ile analiz edilmiştir.

Akıllı telefon kullanımından dolayı katılımcıların karşılaştıkları sorunlar, geçmiş literatür ve resmi kurumların özellikle de hukuktaki çözüm sisteminin bu tür sorunları nasıl çözdüğü ile ayrıntılı olarak tartışılmıştır. Çalışma sonunda, akıllı telefonların kullanıcılar üzerindeki olumsuz etkilerini azaltmak amacıyla toplumu bilgilendirmek, bilinçlendirmek ve olumsuz durumlara karşı kendilerini nasıl savunmaları gerektiği hususunda davranış değişikliği kazandırma amaçlanmıştır.

Anahtar kelimeler: Akıllı telefona, Suç, İnternet, Hack, Medya.

ABSTRACT

One of the most important inventions of the twenty-first century are smartphones. They play an important role in people's lives. Telephone conversations, video chat and call, communication, internet banking, mobile banking transactions, internet shopping, e-government, e-ticket, exam documents, exam results, messaging etc have gradually increased the demand and usage of smartphones. Although smartphones simplify the daily lives of people, they have brought so many negative effects in the lives of the users. Malicious usage of smartphones has rapidly in the recent years. Nowadays crimes committed due to the usage of smartphones have also increased for example mobile phone theft, mobile fraud, mobile hacking, denial of service attack etc. Increase in such crimes has begun to occur in the recent years.

This study mainly focuses on crimes committed by use of smartphones. In this study a questionnaire has been prepared to collect information about users' experience of smartphones, any problems faced while using smartphones and any kind of crimes committed while using smartphones. The answers to the questions given by the participants about the use of smartphones and the problems they encountered while using these devices were analyzed with the SPSS (23) statistics program.

The problems faced by the participants due to malicious usage of smartphones are discussed in detail with the past literature and also laws made by official institutions of the government for example how the judicial system solves such problems. The purpose of this study is to show the malicious usage of the smartphones and crimes committed by the use of smartphones by some of smartphone user. The aim of this study is to inform the society and raise awareness about the malicious smartphones users and crimes that can be committed by the use of smartphones and also how people can defend themselves against malicious smartphone users as well as how these negative effects can be reduced and solved.

Keywords: Smartphones, Crime, Internet, Hacking, Media

1. GİRİŞ

1.1. Giriş

İnsanoğlu (Homo sapiens) 225 bin yıl öncesinden günümüze gelinceye değin birçok başarıya imza atmıştır. 20. yüz yıldan itibaren bilimsel anlamada gelişmelerin başlamasıyla insanlık yeni bir çağa başlamıştır. Telgraf ve telefonun icadıyla haberleşme alanında çağ atlanmıştır. 1960 larda itibaren yaşam alanlarıyla ilgili kavramlar da değişmeye başlamıştır.

Kamusal alan tanımı ilk kez Jürgen Habermas tarafından 1962 de yaptığı "Kamusal Alanın Yapısal Dönüşümü: Burjuva Toplumunun Bir Kategorisi Üzerine Araştırmalar" adlı kitabında tanımlanmıştır (1). Habermas kamusal alanı “modern toplum kuramlarında, toplumun ortak yararını belirlemeye ve gerçekleştirmeye yönelik düşünce, söylem ve eylemlerin üretildiği ve geliştirildiği ortak toplumsal etkinlik alanına işaret etmek için kullanılan kavramdır” olarak tanımlamıştır.

Bununla birlikte kamusal alan, değişen sosyal, bilimsel ve ticari ekonomi anlamında değişime uğramıştır. Teknolojideki baş döndürücü değişim ve yenilikler kamusal alan kavramına yeni bir boyut kazandırmıştır. Günümüzü, enformasyon ve Ağ toplumu olarak tanımlamak yanlış olmaz. 20. yüzyılın sonları ve 21. Yüzyılın ilk on yılı içerisinde bu kavrama ilave olarak medya tanımı da eklenmiştir (2).

Manuel Castells 1990 yılından sonra yeni bir “Ağ Toplumu” kavramını ortaya sürmüştür. 20. Yüzyılın sonlarına doğru bilgi ve iletişim alanlarında baş döndürücü gelişmeler, yeni bir tanımı zorunlu kılmıştır. Ağ toplumu kavramı içinde yaşadığımız teknolojik değişimin yaşamımızdaki etkisini oldukça güçlü bir şekilde hissetmekteyiz (3). Yaygınlaşan ve gittikçe ekonomik olarak ucuzlayan internet akıllı telefon ve diğer elektronik sayısal (dijital) araçlar sayesinde, bilgiye ulaşma ve paylaşma da giderek artmaktadır.

Bu yaygınlaşma beraberinde yeni bir olgunun ortaya çıkmasına neden olmuştur. Dijital suçlar. Bu sayısal elektronik cihazlarla işlenen suçlar internet ve akıllı telefonların yaygınlaşmasıyla artmaya ve yaşamımıza bilişim suçları olarak girmesine neden olmuş ve hukukta da ayrı bir iş yükü haline gelmiştir (4).

Yirmi birinci yüzyılın en yararlı icatlarından biri akıllı telefonlardır. Bu icat insanları masa üstü bilgisayarlara bağımlı olmaktan uzaklaştırmıştır. Bunlara “Akıllı telefonlar ya da taşınabilir bilgisayarlar” da denmektedir. Bu taşınabilir telefonlar insanların günlük yaşamlarını kolaylaştırılmıştır. İlk taşınabilir telefonların ortaya çıkmasıyla bunlara destek olan temel istasyonlar da gelişmeye başlamıştır. İlk zamanlar son derece büyük hacimlerde olan bu telefonlar bir sonraki nesilde küçülmüştür. Bunda en büyük pay pil ve elektronik destek ünitelerinin gelişimidir. İkinci nesil telefonlar küçülmüş ancak sadece konuşma amacıyla kullanılmıştır. Üçüncü nesil telefonlar ise artık mesaj alan veren konuşmayı sağlayan boyutları küçük uzun pil ömürlü telefonlara dönüşmüştür. Dördüncü nesil telefonlar ise ekranlar renklenmiş internete bağlanabilen medya paylaşımı olan telefonlara dönüşmüştür. 5. Nesilden itibaren telefonlar tamamen değişmiş bugünkü halini almıştır (5). Bu telefonlar ekranları büyük dokunmatik, medyaya paylaşımlı internete bağlanıp birçok işlemlerimizi yapan bir araca dönüşmüştür. Hızları artmış tıpkı bilgisayarlar gibi çok çekirdekli işlemciler kullanan taşınabilir bilgisayarlara evrilmiştir.

Bilgisayarların disk işletim sistemi gibi akıllı telefonlarda bir işletim sistemine sahiptir. Bugün en yaygın olanları Android ve İOS işletim sistemleridir (6). Tıpkı bilgisayarlarda olduğu gibi, akıllı telefonlarda da işletim sistemlerinin desteklediği grafik tabanlı birçok uygulamalar vardır. Bu uygulamalar kullanıcıları masa başından uzaklaştırmış, zamandan ve mekândan bağımsız bir hale getirmiştir (7) Bu uygulamalar sayesinde dünyanın her yerinden bankacılık, büro, alışveriş, medya paylaşımı, gibi birçok işlemleri yapılmasını sağlamaktadır. Akıllı telefonlarla artık internette gezinilebilir, haritalar araştırılabilir, fotoğraf paylaşılabilir, video izlenebilir vb. gibi. İşlemler yapılabilir.

Kullanıcılar akıllı telefonların sosyal medya uygulamaları ile bir birleriyle etkileşime geçebilir, sosyalleşebilir, fikir ve bilgi paylaşımı yapabilir, instagram, twitter, whatsapp, facebook vb. gibi sosyal medya hesaplarına girebilir (8). Akıllı telefon

kullanıcıları telefonlarındaki uygulamalar yoluyla, paylaşımlara yorum yapar, arkadaşları ile oyunlar oynar, konuşur (görüntülü ya da sesli).

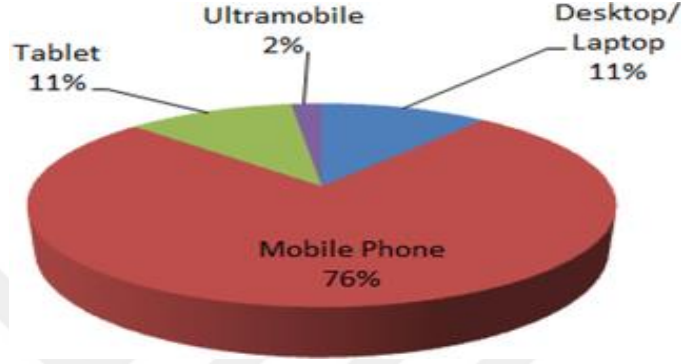
Günümüzde akıllı telefon kullanmak riskleri de beraberinde getirmektedir. Bilgisayarlarda kullanılan birçok uygulamalar eğer güvenli sitelerden sağlanmamışsa, uygulamalar içerisine gizlenmiş virüs, klavye kopya eden birçok programlarını da beraberinde taşımaktadır (9). Bu uygulamalar başkaları tarafından kullanıcılara tuzak olarak yüklenmiş demektir. Bu tuzaklar sayesinde bilgisayarlarınızda yapmış olduğunuz birçok işlem özellikle şifreli kullanılan uygulamalar ele geçirilmiş olur. Özellikle internet yardımı ile uzaktan bankacılık hizmetlerinin tümü başkasının eline geçmiş olur. Aynı problem günümüzde akıllı telefonlar için de geçerlidir. O nedenle internet aracılığı ile yapılan bu işlemlerin tümü “siber” suçlar olarak adlandırılır.

Kimlik avcıları, dolandırıcılık, çocuk istismarcıları vb. Siber suçlular bu hizmetleri sahte kimliklerle kaydedebilirler, böylece çevrimiçi öncülerin suçları işlemesi ve böylece toplumu düzensiz hale getirmesi için platform sağlarlar (10). Genç nesil günümüzde arkadaşlarıyla ve tanımadıkları insanlarla sohbet etmeyi ve mesajlaşmayı tercih ediyor.

Akıllı telefonlar ve sosyal medya uygulamaları, kullanıcıları dolandırıcılardan ve hackerlerden gizliliklerini ve güvenliklerini koruyabilir mi? Bu sorunun cevabını vermek zor olmakla beraber, daha çok kullanıcının dikkatine bağlıdır. Akıllı telefonlar, sosyal medya hesap hackerları ve dolandırıcılar tarafından sürekli olarak ele geçirilmek istenmektedir. Bu nedenle kullanıcıların; e-posta adresi, kişisel fotoğrafları, banka hesap bilgilerine vb. ulaşabilirler. Fierce kablosuz web sitesi; akıllı telefonların güvenliği hakkında bir deney yaptı. Saldırıya uğramış akıllı telefonların çoğunun Andriod kullanıcıları için olduğu tespit edildi. Deney, demoda test edilen telefonların% 92'sinin saldırıya uğradığını göstermektedir. Bu ciddi artışın açıklaması, pek çok güvenli olmayan uygulamanın Google Store'dan, bazı bilgisayar korsanları ve hilekarlar (hacker) tarafından oluşturulan uygulama programların telefonlara indirilmesiyle, insanların bilgilerini çalmak amacıyla olmaktadır (11).

Akıllı telefonlar insanlar için çok yararlı olmasının yanı sıra, adalet sistemi üzerinde etkisi oldu. Günümüzde suç mahalli araştırmaları sırasında, akıllı telefonlar genellikle suç mahallinde bulunmaktadır. Son yıllarda akıllı telefonların dâhil olduğu siber suçlar

özellikle ABD, Çin, Hindistan gibi yoğun nüfuslu ülkeler arasında ciddi bir artış olmuştur (12). 2017, polis soruşturmalarının siber suç oranları aşağıdaki şekilde gösterilmektedir.



Şekil 1. Kaynak; dünyada polis kayıtlarında olan suç dağılımı

Günümüzde birçok elektronik mağazalarında ikinci el akıllı telefonlar satılıyor. Ancak bu akıllı telefonların çoğunun çalıntı veya suç işlemek için kullanıldığı tespit edilmiştir. “Elektronik Tutma” tarafından yapılan son çalışmada, suçluların belirli suçlarda birçok ikinci el akıllı telefonun kullanıldığını ve daha sonra diğer insanlara satıldığını göstermektedir. Birçok ikinci el telefon kurbanı var, çünkü önceki kullanıcı hakkında herhangi bir bilgiye sahip değiller. Bu araştırmada en çok ikinci el telefonlarla yasal sorunlar yaşandığını gösteriyor (13).

Elektronik dünyasının en çok satışı istenen ve sürekli yenilenen akıllı telefonlara artan talep nedeniyle, siber zorbalık gibi suç faaliyetlerinde bulunma olasılığı da artmıştır. Sahte sosyal medya hesapları artmıştır. Bu tür faaliyetler insanlar için tehdit oluşturmaktadır. Bazı insanları rahatsız etmek, ölüm mesajları göndermek için sahte sosyal medya hesapları açmışlar. Bu faaliyetler özellikle gençler arasında ölüme neden olmuştur. Bazı sahte sosyal medya hesapları, özellikle Facebook ve Twitter başta olmak üzere yanlış ölüm bildirisi duyurmak için kullanılmaktadır (14).

Burada tanımlanabilecek bir kavram da “siber zorbalık” tır. Siber zorbalık, sosyal medyada, mesajlaşma, oyun uygulamalarında ve cep telefonlarında hedef seçilen kişileri korkutmaya, kızdırmaya ya da utandırmaya yönelik olarak tekrarlanan bir davranış olarak

tanımlanabilir. Siber zorba vakalarının çoğu liseli öğrenciler arasında gerçekleşir. Örneğin; bir öğrencinin, arkadaşının çıplak bir fotoğrafını diğer öğrencilerle paylaşması. Dolayısıyla fotoğrafı paylaşılan öğrencinin psikolojisini kötü yönde etkiler (bu vakaların çoğu lise öğrencileri arasında gerçekleşir). Bazen bu tür olaylar, birçok gencin, intihar etmesine neden olur (14).

Teknoloji ilerledikçe, akıllı telefonlarda; siber suçlar uygulama sistemlerinde ve yazılımlarında zayıflıklar var. Çünkü bunların bazılarının güvenilirliği yüzde yüz değil. Bu nedenle akıllı telefonlara yapılan siber saldırılar, yasadışı faaliyetler özellikle Andriod telefonlarda arttı. Günümüzde özellikle akıllı telefonları hedefleyen birçok bilgisayar korsan grubu vardır (15).

Bu bilgisayar korsanları, kullanıcıların telefonlarına zarar veren, mesaj şeklinde bir virüs bağlantı gönderir. Bu bağlantı mesajları, android akıllı telefonların güvenlik sistemini ele geçirir. Aslında bu bağlantı mesajları herkes tarafından bilmeden paylaşılabiliyor. Ancak bu, kişinin mülkünü tahrip etmesi kanuna aykırı olduğu için kişinin hapse girmesine neden olabilir. Bu bilgisayar korsanları sadece cep telefonunu tahrip etmekle kalmaz, aynı zamanda telefonlarında çevrimiçi bankacılık uygulamalarını, e-postalar gibi özel bilgileri ve diğerleri arasında kişisel fotoğrafları kullandığından, örneğin kredi kartı ve banka bilgileri gibi önemli bilgileri çalar. Ege Üniversitesi, Yunanistan'ın Samos Bilgi ve İletişim Sistemleri Mühendisliği Bölümü tarafından 2018 yılında yayınlanan makaleye göre, 7 yıllık Mobil Cihaz Adli Tıp incelemesinin eleştirel bir incelemesi, günümüzde birçok insanın akıllı telefonlarında internet bankacılığı uygulamaları kullandığını söylüyor. Böylece banka hesap bilgileri ve kredi kartı bilgileri akıllı telefonlarında saklanır. Bir akıllı telefon hacklenirse, bilgisayar korsanı bilmeden kurbanın kredi kartını kullanabilir ve ayrıca yasadışı öğeleri çevrimiçi olarak satın alabilir ve böylece kurban için sorun yaratabilir. Bilgisayar korsanları da kurbanın hesabından para çalabilir (16).

Akıllı telefonlarda SIM kartları kullanıyor. Ancak son yıllarda sim kartlarında da dolandırıcılık oluyor. Sahtekârlık SIM değişimi olarak bilinir ve finansal hesaplarınızı ele geçirmek için kullanılabilir. SIM değiştirme, telefon tabanlı kimlik doğrulamasına dayanır Başarılı bir SIM takas dolandırıcılığı, siber suçlular cep telefonu numaranızı ele geçirmek ve hassas kişisel verilerinizi ve hesaplarınıza erişmek için kullanabilirsiniz. İşte böyle

çalışır. Metin tabanlı iki faktörlü kimlik doğrulama kullanan banka hesaplarınızdan birine erişmeyi deneyebilirsiniz. Bu, kullanıcı adınızı ve şifrenizi girerek hesabınıza erişmeye başladığınız anlamına gelir. Daha sonra bankanız, oturum açma işlemini tamamlamanız için cep telefonunuza bir erişim kodu gönderir. Ancak, dolandırıcıların cep telefonu numaranıza bağlı SIM kartı değiştirebilmesi durumunda ne olur? Bu onlara bu numara üzerinde kontrol sağlar ve hesabınıza erişim kodunu alırlar (17).

Ebeveynler, akıllı telefonlar kullanırlar. Çocuklarına kolay ulaşabilmek için, onlara da akıllı telefon satın alırlar. Ancak akıllı telefonlar çocuklara zarar veriyor. Son araştırmalarda, akıllı telefonlara sahip çocuklar arasında çevrimiçi taciz, siber zorbalık, çocuk pornografisi, terörist grup üyeleriyle iletişim artmaktadır. Bu yüzden ABD gibi gelişmiş ülkeler de; özellikle çocuklar arasında ölümlere neden olmuştur. İngiltere, Kanada da bunların arasında son terör, Irak İslam Devleti ve Levant gibi terörist gruplarına katılan gençlere tanık olunmuştur. Bu teröristlerin genellikle gençlerin beyinlerini yıkamayı denedikleri ve bu gençlere yüklü miktarda para verdikleri düşünülmektedir. Bunlara iyi bir gelecek vaat ederek kandırdıkları bilinmektedir. Genellikle bu teröristlerin bu çocuklarla iletişim kurmak için cep telefonları kullandıkları, bu çocukların yaptıkları eylemlerden ülke vatandaşlıklarının iptal edildiği hatta hayatlarını kaybettikleri düşünülmektedir (18) .

1.2. Çalışmanın Amacı

Son yıllarda kullanımı artan akıllı telefonlarla suç işleme oranları da artmıştır. Birçok suç unsuru oluşturacak uygulamalar da çoğalmıştır. Bu çalışma, akıllı telefonlarda kullanılan uygulamaların suç teşkil edecek yazılım, yapılan suçlar (örn. mobil hazırlık gibi) ve uygulamalarını belirlemek ve bazı değişkenler açısından betimsel olarak incelemek amacıyla yapılmıştır.

2. GENEL BİLGİ

2.1 Akıllı Telefon nedir?

Akıllı telefon, taşınabilen bir el bilgisayarı olarak adlandırılır. Taşınabilir bilgisayarlar, tabletleri de kapsar. Kısaca bunlara mobil cihazlar denilmektedir.

Akıllı telefonların gelişimi, kullanıcıların birbirleriyle haberleşmelerini sağlamak amacıyla üretilmiş ve bu gün bilgisayar tabanlı hale gelmiştir. Kullanıcılar akıllı telefonlarla haberleşmenin dışında, fotoğraf, video, önemli tarihler ve notlar, SMS ve MMS mesajlar gibi çeşitli kişisel bilgileri kaydetmek için de kullanılmaktadırlar. Akıllı telefonlar ayrıca bunların kullanıcılar arasında paylaşımını da sağlamakta, bu telefonlarda kullanılan uygulamalar sayesinde (WhatsApp vb gibi) video, e-posta, internette gezinme bilgileri, konum bilgileri, sosyal ağ mesajları ve kişileri de içerebilmektedir (19).

2.2. Mobil Cihazların Özellikleri

Mobil cihazlar genellikle aynı özelliklere sahiptir. Hemen hemen bunların hepsi, mutlaka bir GSM operatörünün üyesidirler.

Mobil cihazların genel özelliklerini aşağıdaki sıralayabiliriz (20):

- SIM kart yuvası
- Pil ve şarj aleti ve yuvası. (port)
- Dâhili hafıza (kişisel bilgi için)
- Kullanılabilir hafıza (uygulamalar ve medya vb. için)
- Bluetooth
- Wi-Fi

- Bilgi giriři için fiziksel bir ekrana sahiptir.
- Kolay taşınmasının yanı sıra diğerk el ile manipüle edilebilmesini sađlayan boyut ve ağırlıktadırlar.
- Kablosuz ađa bađlanabilir.

2.3. Mobil Cihaz Güvenliđi

Günümüzde internet üzerinden bilgisayarlara ulaşmaya çalışan kişiler tarafından hazırlanan ya da bulaştırılmak istenilen ve virüs diye adlandırılan yazılımlar bilgisayar kullanıcılarına tehdit oluşturmaktadır. Bu durum, bilgisayar alt yapısına dönüşen mobil cihazlar için de geçerlidir. Bu nedenle mobil cihazlar da tehdit altındadır. Bu tehditleri aşğıdaki şekilde sıralamak mümkündür (21).

2.4. Mobil Tehditler ve Saldırılar

- Mobil cihazların cazip hedefleri bulunmaktadır:
 - a. İnsanlar üzerlerinden çok fazla kişisel bilgileri depolar; e-posta, takvimler, kişiler, resimler vb.
 - b. Hassas organizasyon bilgilerini elde etme.
 - c. Kolayca kaybolan/çalınan akıllı telefonlar ceplere sığabilir.
 - d. Dâhili faturalama sistemi; SMS/MMS (mobil operatör), uygulamaların içinden çeşitli satın alımlar yapma (kredi kartı) vb.
- Birçok yeni cihaz temassız ödemelerde vb. kullanılan yakın alan iletişimine (NFC) sahiptir.
- Cihaz kredi kartı olabilir.
 - a. Konum gizliliđi sorunları olabilir.

2.5. Cihazlardaki Kötü Amaçlı Yazılımlar

- IOS kötü amaçlı yazılım (malware); çok az

- Android kötü amaçlı yazılımı fazla ve artmaya devam ediyor (\$\$\$)
- Ana kategoriler:
- Trojans
- Uygulamaları/casus yazılımları izleme
- Adware
- Botnet

2.6. Cihaz Arama ve El Koyma

- Tutuklanma durumlarında, polis mobil cihazını arama izni olmadan arayabilir.
- Faillerin delilleri yok etmesini önleme gerekçesiyle.
- Yasayı çiğnemek oldukça kolay (aşırı ayrımcılık)
- a. Suç ciddiyeti: cinayet, ihanet vs. vs. ödenmemiş alıntılar.
- b. Kitaplardaki “on binlerce” suçun

Kolluk kuvvetlerinin mobil cihazlardan veri toplaması artık daha kolay (adli tıp).

2.7. Mobil Erişim Kontrolü

- Fiziksel erişimi varsa, saldırganın bir mobil cihazı kontrol etmesi çok kolaydır.
- a. Özellikle kullanıcının kimliğini doğrulamanın bir yolu.
- b. Sonra cihaz botnet’e katılabilir, SMS spazm gönderebilir.

2.8. Bilgisayar Korsanları Tarafından Mobil Cihazlarda Yapılan Yaygın Siber Suçlar

Mobil cihazların işletim sistemleri açık kaynaklı sistemlerdir. Bu, yetkisiz kişilerin cihaza kolayca girip hackleyebileceği anlamına gelir. İnsanlar genellikle Apple ve Samsung telefonlar gibi yeni gelişmiş mobil cihazlara kolayca bağımlı olabilirler. Her yıl bu cihazlara bağımlı olma potansiyeli teknik olarak daha da geliştirilmekte ve bu durum

bireyleri bu cihazlara daha da bağımlı hale getirmektedir. Dolayısıyla hackerler tarafından daha çekici bir hedef haline gelmektedir (27).

2.9. Mobil Cihazlarda Faaliyet Gösteren Siber Suç Türleri

1. Vishing

Bu siber suç türü, kişilerin banka hesap bilgileri ve kredi kartı numaraları gibi kişisel bilgilerini öğrenebilmek için saygın bir şirketten geliyormuş gibi sesli mesajlar bırakarak telefon görüşmesi yapabilmek için uygulanan bir yöntemdir. Bu süreçte suçlu istediği bilgileri toplayarak hedeflerine ulaşabilir (27).

2. Smishing

Smishing, bağlantı veya URL içerebilecek bir metin mesajı göndererek ve kullanıcıların mobil cihazının saldırıya uğradığı bağlantıyı tıklayarak kişilerin bu yolla kandırılmasıdır (27).

3. Bluebugging

Bu yetenekli bir bilgisayar korsanının keşfedilebilir moda veya aralıktaki Bluetooth özellikli cihazlarda mobil kodlara erişmesine izin veren bir tekniktir. Buna bazen Bluetooth saldırısı da denilmektedir (27).

4. Bluejacking

Bu bir Bluetooth'tan cep telefonları ve tabletler gibi başka bir Bluetooth cihazına istenmeyen mesajların gönderilmesidir. Bu süreçte bir bilgisayar korsanı 10 metrelik mesafe içindeki diğer kullanıcılara mesaj, resimler ve PDA gönderebilmektedirler (27).

5. Bluesnarfing

Bluesnarfing, bir Bluetooth bağlantısı aracılığıyla kablosuz cihazdan gelen bilgiye yetkisiz erişim yoludur. Bu tür saldırılar genellikle telefonlar, dizüstü bilgisayarlar ve masaüstü bilgisayarlar üzerinden gerçekleştirilmektedir. Bu saldırı türü il, kişi listelerine, e-

postalara, takvimlere, resimlere, özel videolara ve metin mesajlarına erişim sağlamaktadır. Hem Bluejacking hem de Bluesnarfing, başkalarının Bluetooth bağlantılarını bilgisi olmadan kullanmaktır. Bluesnarfing, kullanıcıların mahremiyetini, gizliliğini tehlikeye attığı, hedeflenen cihaza veri aktardığı için kullanıcıların cihazlarına zarar vermemektedir. Bluejacking kullanıcının gizliliğini tehlikeye attığı için hedeflenen cihaza veri aktardığı için kullanıcıların cihazlarına zarar vermemekte ancak Bluesnarfing, hedeflenen cihazdan bilgileri çalınmaktadır (27).

6. Mobil Hackleme

Basit terimle hacklemek (28), bir bilgisayar sistemine ve/veya ağa yasadışı bir şekilde girilmesi anlamına gelmektedir. Bilgisayar korsanlığı ile eşdeğer bir terimdir. Cep telefonuna, iletişim cihazlarına, bilgisayara ve/veya ağa girmeye yönelik her hareket hacklenmektedir. Bilgisayar korsanları, hedef bilgisayara, mobil ve/veya iletişim aygıtlarına saldırmak için hazır bilgisayar programları yazmakta ve/veya onları kullanmaktadırlar.

7. Mobil Siber Hakaret

Bugün dünyada bu tür bir suç gittikçe yaygınlaşmaktadır. Suçlular, cep telefonlarını ve iletişim cihazlarını kullanarak, başkalarını karalamak ve itibarlarını düşürmek için aşağılayıcı, küçük düşürücü ve müstehcen SMS veya e-posta göndermektedirler (29).

8. Mobil Pornografi

İnternet artık çok hızlı bir şekilde ev eşyası haline gelmektedir. Çok sayıda ev internete erişebildiği için, daha çok çocuk cep telefonlarını, iletişim cihazlarını, kullanmakta ve bu tür saldırganlığa düşme olasılığı artmaktadır. Bu durum istismarcılar tarafından, dünya çapında çocuklara cinsel istismarda/saldırıda bulunmak için kullanılmaktadır (30).

9. Kimlik Hırsızı

Kimlik hırsızlığı için cep telefonu kullanılmakta ve suçlular abonelik dolandırıcılık vb. suçları çeşitli iletişim cihazları kullanarak işlemektedirler (31).

10. Cep telefonunu kopyalamak veya yeniden kopyalamak.

Bir klon, ESN ve telefon numarasını kullanarak meşru bir abone tarafından sahip olunan kişiyi taklit etmek için programlanmış bir analog cep telefonu (bu numaralar genellikle bir "tarayıcı" radyoya müdahale ederek, bir bayinin veya servis sağlayıcısının kayıtlarını veya doğrudan kimliğe bürünmüş telefondan). Birleşik Krallık'a ABD ve Hong Kong'dan yeni klonlanmış telefon türleri geliyor: 'yuvarlanan' telefonlar, önceden programlanmış bir listeden otomatik olarak bir kimlik arıyor ve en son 'sihirli' telefonlar, kullanımda olan yakındaki telefonlardan kimlikleri kopyalayan kendi tarayıcıları gibi davranıyor (33).

11. Mobil Siber Takipçilik

Siber Stalking, cep telefonlarını kullanarak, siber suçlunun mağdura yönelik taciz veya tehdit edici davranışını tekrarlayan davranışlar olarak tanımlanabilir. Genel olarak Stalking, mağduru hedef almak, mağdurun izini sürmek, taciz edici telefon görüşmeleri yapmak, mağdurların evcil hayvanlarını öldürmek, mağdurların mülkünü tahrip etmek, yazılı mesaj veya nesneler bırakmak gibi tekrarlanan taciz eylemleri olarak adlandırılabilir. Stalking'i, mağdurun fiziksel zararı gibi ciddi şiddet içeren eylemler izleyebilir ve aynı şekilde ciddiyetle muamele edilmeli ve görülmelidir. Her şey, takipçinin davranış tarzına bağlıdır (32).

12. Hizmeti Engelleme Saldırısı

Bu, mağdurun ağının bant genişliğini dolduran ya da e-posta kutusunu, erişmeye veya sağlamaya yetkili olduğu hizmetlerden mahrum bırakan spam postalarla doldurabilen bir suçtur (33)

13. Cep Virüsü Yaygınlaştırması

Mobil virüs, cep telefonlarını veya diğer iletişim cihazlarını hedefleyen elektronik bir virüstür. Tipik mobil virüs yayılımında kötü amaçlı yazılım kendini başka bir yazılıma bağlar(34).

14. Mobil Yazılım Korsanlığı

Orijinal yazılımların yasa dışı kopyalanması ya da orijinali geçmesi amaçlanan ürünlerin sahteciliği ve dağıtımı yoluyla mobil yazılım çalınmasıdır (35).

15. Mobil Kredi Kartı Dolandırıcılığı.

Ürün ve/veya hizmet satın almak için cep telefonu ile yetkisiz ve yasadışı kredi kartının kullanılmasıdır (36).

16. Mobil phishing (Oltalama)

Mobil servis sağlayıcılarından olan kimlik hırsızlığı (phishing), e-postaları ile cep telefonu kullanıcılarının kimlik hırsızlığı eylemi anlamına gelmektedir. Ayrıca, kullanıcının kimlik özel bilgilerini sahtekâr bir teşebbüs olduğunu iddia eden bir kullanıcıya göndererek e-posta gönderme eylemini içerir (37).

2.10. Adli Mobil Cihaz Nedir?

Çalınan, uygulamalar sayesinde kişisel hesaplarda hırsızlık yapılan, ülkesel güvenliği tehdit eden paylaşım ve uygulamalar kullanılan cihazları ve üzerlerinde hukuki işlemler yapılması gereken cihazları ‘Adli Mobil Cihaz’ olarak tanımlamak mümkündür. Mobil cihazda mevcut dijital bilgilerin ya da verilerin adli kayıt koşullarına uygun şekilde kurtarılmasını sağlayan adli bilimler bünyesi altında bir daldır (23).

Adli kayıt gerektiren Mobil cihaz ifadesi genellikle cep telefonlarına atıfta bulunur, ancak bu, PDA cihazları, GPS cihazları ve tablet bilgisayarlar dâhil olmak üzere hem dâhili belleğe hem de iletişim yeteneğine sahip dijital cihazlarla da ilgili olabilmektedir.

2.11. Mobil Adli Bilimler Tarihi

Kriminal olaylarda cep telefonu/cihazların kullanımı birkaç yıl öncesinden itibaren tanınmasına rağmen adli çalışmalar 2000'lerin başından 1990'ların sonlarına kadar başlayan yeni bir alandır. Cep telefonlarının kriminal olaylardaki rolü, bu tür cihazların tüketici pazarında artan kullanılabilirliği ve adli muayene talebini destekledikleri daha geniş iletişim platformları (örneğin, e-posta, internette gezinme) nedeniyle kolluk kuvvetleri tarafından uzun zaman önce tanınan bir alan olmuştur. Tüketici pazarındaki telefonların (özellikle akıllı telefonların) ve diğer dijital cihazların artması, o sırada kullanılmakta olan mevcut bilgisayar sistemlerinin yetersizliği, bu cihazların adli boyutta incelenmesi talebine neden olmuştur. Bu durum, hem akıllı telefonların hem de bilgisayarların aynı adli bilgisayar teknikleriyle incelenemeyen farklı işletim sistemlerine sahip olmalarından kaynaklandığı düşünülmektedir (22).

Telefonun içeriğini doğrudan ekran üzerinden analiz etmek ve önemli içeriği fotoğraflamak gibi mobil cihazları incelemeye yönelik ilk denemeler, ilk bilgisayar adli tıp incelemelerinde benzer teknikler kullanılmıştır (22-23). Bununla birlikte, bu süreç çok zaman kaybına yol açtığı ve mobil cihazların sayısı artmaya başladıkça, araştırmacılar veri çıkarmak için daha verimli araçlar arama başlamışlardır. Girişimci mobil adli tıp denetçileri bazen cihaz verilerini görüntülemek ve yedeklemek için akıllı telefonu veya PDA senkronizasyon yazılımını kullanmışlar bazen de verilerin senkronize edildiği şüpheli bir bilgisayarın sabit diskinde araştırmalar yapmışlardır. Ancak, bu tür bir yazılım telefona yazılabilir ve okunabilirken silinen verileri kurtarma konusunda başarısız olmuşlardır (24). Bazı adli tıp uzmanları, "flâşör" veya "twister" kutuları, hata ayıklama veya güncelleme için bir telefonun belleğini "flaşlaşmak" için OEM'ler tarafından geliştirilen araçları kullanarak silinen bilgileri kurtarabileceklerini keşfetmişlerdir (25). Ancak, flâşör kutuları verileri değiştirebilmekte ve kullanmak için karmaşık olabilmektedir. Bunun nedeni, ne karşılaştırma doğrulamalarını ne de denetim izlerini gerçekleştiren adli araçlar olarak geliştirilmemesidir. Bu nedenle fiziksel adli tıp incelemelerinin daha iyi alternatiflere ihtiyacı olduğu düşünülmektedir.

Bu artan talepleri karşılayabilmek için, telefon belleğini daha az kesintiyle kurtarmak ve ayrı ayrı analiz etmek için denetçilere erişim sağlayan ticari araçlar tanıtılmış,

Zamanla bu ticari teknikler daha da geliştirilmiş ve özel mobil cihazlardan silinen verilerin kurtarılması bazı uzman araçlarla mümkün hale gelmiştir. Ayrıca, ticari araçlar ekstraksiyon sürecinin çoğunu bile bilgisayarlı hale getirmiş, triyaj ve veri ön izleme amacıyla temel çıkarma işlemleri yapan bilgisayarlara kıyasla daha az eğitimli ilk müdahale ekipleri için bile müdahaleyi mümkün hale getirmiştir (23).

2.12. Mobil Cihaz Mimarisi

Mobil cihazda ne var ve ne için kullanılıyor?

Tüm mobil cihazlar belirli bir tasarıma sahiptir. Bilgisayarlarda olduğu gibi mobil cihazların tasarımlarının cihazın temel bileşenlerini tanımlaması gerekmektedir. Veriler, bilgiler cihazda nasıl ve nerede depolanır? Cihazda ne tür bir işlemci kullanılmaktadır? Dosya sistemi neye benzemektedir? Bu ve benzeri diğer sorular analizin temelini oluşturmaktadır (19).

2.13. Dosya Sistemleri

Dosya sistemleri, dosyaların nasıl adlandırıldığını, depolandığını, organize edildiğini ve erişildiğini tanımlayan yazılım mekanizmasıdır. Android mobil cihazların çoğu, Linux İşletim Sistemini kullanmaktadırlar. Bu mobil cihazların parçalanmış dosya ve öğelerini bu sistem geri kazandırdığı için veriler kurtarılabilir. Çünkü veriler kurtarılabilir için Cellebrite UFED adlı bir program kullanılmakta ve fiziksel ekstraksiyonu kurtarabilmektedir (19).

2.14. Adli Mobil Zorlukları

Modern mobil cihazlar birçok açıdan küçük PC'lerden daha karmaşıktır (19). Mobil cihazlarda 1G, 2G, 3G ve 4G gibi mobil iletişim teknolojileri kullanılmaktadır. 1G mobil iletişim teknolojisi ile işleyen mobil cihazlar veri iletmek için değil ses iletmek için tasarlanan sistemlerdir ve bu mobil iletişim teknolojisi ile işleyen mobil cihazlar hala

dünyanın bazı bölgelerinde kullanılmaktadır ve insanlar bunları kullanmayı tercih etmektedirler. 1G mobil iletişim teknolojisinin kullanıldığı eski model mobil cihazlar bir bilgisayarda bulunan ve kullanılan teknolojilere sahip değildirler. Aslında, "işletim sistemi" olarak sınıflandırdığımız teknolojilere de sahip değildirler. Bu teknolojiye verilerin silinmesi işlemi tamamlanmamakta, aynı zamanda silinmiş verilerin kurtarılması da imkânsız görünmektedir.

1990'ların başında uygulamaya konulan 2G teknolojisi, ses sinyallerinin iletiminde dijital sinyallerin kullanıldığı, kablosuz iletişim teknolojilerinin hayatımıza girdiği dönem olarak bilinmektedir. Mobil cihazlarda yeni bir çağın başladığı dönemdir. Bu dönemde ses kalitesi geliştirilmiş, güvenlik önlemleri ve cihazlarda kullanılabilir kapasite arttırılmıştır. Çoğunlukla 2G işletim sistemleri Blackberry ve Palm gibi telefonlar için tasarlanmış bir üründür. Bazı 2G telefonlar, diğerlerine göre akıllı telefonlara daha yakın olan özelliklere sahiptir. Bununla birlikte, silinen verileri kurtarma becerisi, bir telefon modelinden başka bir telefon modeline önemli ölçüde değişmektedir.

Günümüzde farklı işletim sistemlerine sahip pek çok mobil telefon bulunmaktadır. Adli olarak her biri farklı şekilde tasarlandığı için bu cihazların farklı adli araç kitlerine ihtiyaç duyduğu bilinmektedir. Ancak 3G ve 4G telefonlar, PC'ye en yakın tasarımları olan cihazlar olduğu düşünülmektedir. Çünkü internete bağlanabilirler, çeşitli uygulamaları indirip yükleyebilirler, konum gösteren GPS özelliklerine sahiptirler. Bu uygulamalar, adli bilimler araştırmacısının bunlardan bilgi almasını kolaylaştırır.

Buradaki büyük sorun, bu cihazların bir kısmı bilgisayar benzeri işletim sistemlerine sahip küçük bilgisayarlar olsa bile, genellikle tipik bilgisayar adli araçları kullanılarak incelenemez. Her cihazın kendi farklılıkları vardır ve her cihaz, cihazın deposunda bulunanları deşifre etmek için inceleyen araçta özel bağlayıcılara ve özel cihaz sürücülerine gereksinim duyar.

2.15. Cep Telefonundan Faydalı Bilgilerin Çıkarılması

Araştırmacı ilk adımı, çalıştırdığı cihazın özelliklerini bilmelidir. Telefonun, ipad'lerin, iphone'un veya en son teknolojik özellikleri, bir önceki akıllı telefona göre

farklılıkları ve/veya üstünlüklerinin olup olmadığını bilmelidir. Bu yüzden, bu alandaki uzman araştırma yapmalı, uygun cihazı seçmeli ve daha sonra ne yapacağına karar vermelidir. Bu cihazlar fiziksel ve/veya mantıksal ekstraksiyon (veya her ikisi) yapılabilmekte, Cellebrite'ın UFED Touch gibi bazı araçları, cihazlardan veri almayı desteklemektedir (19).

UFED ve MPE+ gibi araçlar büyük ölçüde desteği basitleştirir. Parabin'i içeren verileri analiz eden çok sayıda başka araç bulunmaktadır (19). Adli uygulamalar için mobil bir cihaz seçilirken, dijital adli laboratuvarlarda birden fazla bilgisayar farklı özelliklerdeki cihazları kullandıkları için birden fazla cihaz seçilmelidir.

Araştırmacı cihazı analiz ettiğinizde, analiz için kullandığınız cihazın önerileri doğrultusunda uyguladığınızdan emin olmalıdır.

Uzman, cihazı ve onun verilerini çıkarma prosedürünü belirledikten sonra, bir sonraki adımda araçları, cihazları çalıştırmak ve konu ile ilgili adli çerçeve çizmelidir. Konusunda uzman genellikle konu ile ilgili cihazlardan iki kez görüntüyü almalı, bu görüntülerden birini kanıt olarak değerlendirmekte, diğerini ise üzerinde çalışmalar yapacağı çalışma görüntüsü olarak kullanabilmektedir. Üzerinde çalışılan kopyanın hasar görmesi durumunda, ilgili uzman kanıtın bir kopyasını tekrar alarak yeni bir çalışma kopyası olarak yapmasını sağlayabilmektedir. Uzman, cihaz için alet kitinden doğru konektörü veya pigtaili (USB) seçmesi önem kazanmaktadır.

2.16. SIM Kartlar ve SD Kartlar

SD'ler (güvenli dijital) kartlar, birçok mobil cihazın kabul edebileceği verilerin depolamasını sağlayan genişletme kartlarıdır. SD kartlar, fotoğraf ve müzik gibi verilerin saklamak için bellek ekler. SD kartlar, cihazda güç kapalı olsa bile, şarkıları, fotoğrafları ve/veya resimleri kaybetmeyecek bir anlam ifade etmektedir (19).

2.17. SIM (Subscriber Identification Module) (Abone Kimlik Modülü)

Farklı kartlarda her bir SIM'i, abonenin mobil ağıyla ilişkilendiren bir Uluslararası Mobil Abone Kimlik (IMSI) numarası bulunmaktadır. Bir mobil cihaza takılan kart, kullanıcının hesabını ağa göre tanımlamakta, kimlik doğrulama işlemlerini gerçekleştirmekte ve temel kullanıcının ağ bilgileri için depolama alanı sağlamaktadır (19).

SIM'ler ayrıca mesaj metinlerini, telefon rehberini ve cihazın telefon numarasını depolayabilmektedir. Tüm mobil cihazlar SIM kullanmaz. SIM'deki bilgiler de cihazda saklanabilmektedir. Ancak, ilgili uzman, adli amaçlı, adli analiz sırasında SIM kart ile belirsiz hedef cihazı tanımlayabilmekte ve gerekli verilere erişebilmektedir (19). Ayrıca ilgili uzman telefonu tanımlamak için bir takım işlemler yapabilmektedir. Bunun için her bir SIM'de entegre devre kartı tanımlaması (ICCID) bulunmaktadır. Kontrol amaçlı numara SIM'de yazdırılmakta, ICCID, Verici Kimlik Numarasını (IIN), bireysel hesap kimliklerini içermektedir. Mobil cihazın adli görüntüsü alınabilmekte ve ICCID kaydedilmektedir (19).

2.18. SIM Kart Üzerinde Hangi Bilgiler Bulunur?

SIM kartlar abone hakkında birçok veri ve bilgi içermektedir. SIM Kartlarda kişi listesi ve mesajların metinleri gibi veriler saklanabildiği gibi aşağıda belirtilen veri ve bilgilere de ulaşılabilmektedir (26).

-Hizmet sağlayıcı adı (SPN)	-Kart sahibi doğrulama (PIN ve PUK Kodu)
-Mobil ülke kodu (MM)	-Şifreleme anahtarı (KC)
-Mobil şebeke kodu (MNC)	-Tuş sırası numarası şifreleme
-Mobil abone kimlik numarası (MSIN)	-Acil çağrı kodu
-Mobil istasyon, uluslararası abone izin numarası (MSISDN)	-Sabit arama numaraları (FDN)
-Kısaltılmış arama numaraları (ADN)	-Geçici Mobil Abone Kimliği (TMSI)
-Son aranan numaralar (LDN)	-Yönlendirme alan tanımlayıcı (RIA)
-Kısa mesaj servisi (SMS)	-Şebeke kodu
-Dil tercihi (LP)	-Servis arama numaralar

2.19. SIM Kart İnceleme Araçları (26)

- Encase Smartphone Examiner.
Cep Telefonları üzerinde Adli İnceleme yapabilmeye olanak sağlayan program ile SIM Kartlar üzerinde de Adli İnceleme yapılabilmektedir.
- MOBILedit! Forensic.
Cep Telefonları üzerinde Adli İnceleme yapabilmeye olanak sağlayan MOBILedit! ile SIM Kartlar üzerinde Adli İnceleme yapılabilir, SIM Kart üzerinde silinen mesajları okuyabilirsiniz.
- XRY Logical & Complete Package with SIM id-Cloner.
Bu program ile SIM Kart' in orijinal bir kopyasını alarak aldığınız kopya üzerinde daha güvenli bir inceleme yapabilirsiniz.
- pySIM
SIM kart üzerinde bulunan kişi listesi ve mesajları düzenleme, yedekleme ve silme işlemlerini rahatlıkla yapabilirsiniz.
- Access Data Mobile Phone Examiner (MPE) Plus
Bütün cep telefonlarını destekleyen program ile SIM Kart üzerinde bulunan bütün dosya sistemlerini inceleyebilirsiniz.
- SIMpull
Bu program ile SIM Kart üzerinde kişi listesine erişebilir, silinmiş mesajlarınızı kurtarabilirsiniz.
- Cellebrite (UFED)
Bu program ile cep telefonu incelemesi yapabilmektedir. İlgili program ile SIM kart kopyası alınıp kopya üzerinden de inceleme yapabilmektedir.
- Simcon.
Bu program ile SIM Kart üzerinde kişi listesine erişebilmekte, silinmiş mesajlar da kurtarabilmektedir.

2.20. Mobil Cihazları Analiz Etmek

Mobil cihazların kullanımı yaygınlaştıkça, mobil cihazların çoğu suç mahallinde bulunduğundan, mobil cihazlar adli bilimler alanında daha da önem kazanmaktadır. Dijital adli bilimin (adli bilişim) bir parçası olan mobil cihazlardan adli amaçlı günlük hayatımızda cep telefonlarından ve benzer cihazlardan veri ve kanıt elde etmek veya kanıt toplamak amaçlanmaktadır (19).

Adli amaçlı mobil cihazların kullanım amacı, cihazdaki veriler değişmeden/değiştirilmeden o mobil cihazdan verileri elde etmektir. Çünkü mobil cihazlarda sabit donanım ve yazılımlarında hızlı değişikliklerin olması ve kritik güncellemelerin yapılması cihazdaki verileri ve güncelliğini etkileyebilmektedir.

Android ve IOS için bir örnek verelim. Bu işletim sistemlerinin dosya sistemine bakılarak (Şifreli Dosya Sistemi), UFED ekstraksiyon raporu kullanıcının UFED tarafından sağlanan rapora göre Web'de gezinip gezilmediğini ve web taramasının tarihçesini incelemeyi mümkün kılmaktadır.

Mobil cihazlar yeni çalışma saatine senkronize edilebilmektedir. Bu durum, AT, T, Verizon veya T-mobile gibi yeni çalışma sağlayıcısının saat sinyalini mobil cihaza gönderdiği anlamına gelmektedir. Şebeke sağlayıcısı, zaman sinyali almak için ABD Deniz Gözlemevi gibi standart bir zaman kullandığından, mobil cihazların son derece doğru saat sinyali göndermeleri mümkün olabilmektedir (20).

3. GEREÇ VE YÖNTEM

Bu çalışmada temel olarak, akıllı telefonlar kullanılarak işlenen suçlara odaklanılmıştır. Çalışmada kullanıcıların akıllı telefonla ilgili yaşadıkları ve suç teşkil eden olayları yaşayıp yaşamadıklarıyla ilgili bilgiler toplamak amacıyla bir anket hazırlanmıştır. Bu çalışma, Adana Sarıçam ve Seyhan ilçelerinde yaşayan 241 kullanıcıyla gerçekleştirilmiştir.

Yaşamımızın vazgeçilmez unsuru olan akıllı telefona sahip olan bireylerin, telefon kullanımları sırasında karşılaştıkları problemlerin belirlenmesi amacıyla, bu tez için oluşturulan anket sorularına verilen cevaplardan oluşan verilerin analiziyle anlaşılmaya çalışılmıştır.

Akıllı telefonların sadece anket yerine kriminal yazılımlarla da kullanıcılara akıllı telefonlarda inceleme yapılmak istenmesine rağmen, ortaya çıkacak hukuki sorunlardan dolayı vaz geçilmiştir. Ayrıca adı geçen yazılımlar sadece kurumlar için kullanımına izin verildiğinden dolayı satın alınması da gerçekleşmemiştir. Ek olarak kişisel veri ve bilgi güvenliği açısından da bu uygulamadan vaz geçilmiştir. Bu açıklamaya ek olarak ayrıca çeşitli web kullanıcıların oluşturduğu bloglarda belirtilen sorunlar ve çözüm yolları, Adli ve kriminal suçlar ve sıklığı gibi istatistiksel sonuçlardan derlenen çözüm önerileri ortaya konulacaktır.

Ayrıca çeşitli marka ve işletim sistemine ait telefonların kullanılacak çözümleyici programlarla tarama yapılarak sorun olup olmadığı ortaya çıkarılmak istedik ama mobil telefon analizleri kullanılan mobil adli programlar Türkiye'de satılmamaktadır ve Amazon, ebay gibi pazarda bulunanlar ve ürünlerini Türkiye gibi Ortadoğu ülkelerinde satmaları yasaklanmıştır. Ayrıca birisinin başka bir kişinin cep telefonunu analiz etmesi için polisten izin almanız ve cep telefonunun belirli bir suçla ilgili olduğundan şüphelenilmiş olması

gerekir. Bu nedenle yasalar birinin cep telefonunu analiz etmeme izin vermiyor çünkü cep telefonları kişisel bilgiler içeriyor

Anket 40 sorudan oluşmuştur. Ankette kişisel bilgilerin dışında, karşılaştıkları problemlere dair soruların cevaplanması istenmiştir. Ankette başlık olarak, kullanılan operatör, telefon markası, işletim sistemi, kullanılan uygulamalar, sosyal medya uygulamalarında karşılaştıkları sorunlar, casus yazılım ya da virüs yoluyla problem yaşıyıp yaşamadıkları, çalıntı telefon kullanıp kullanmadıkları ile ilgili sorular yöneltilmiştir. Bu sorulara cevap veren katılımcılara ait veriler analiz edilmiş, sonuçlar bulgular bölümünde verilmiştir. Anket soruları SPSS 23 paket yazılımı ile analiz edilmiştir. Ankette cinsiyet ve yaş guruplarına göre kullanıcıların yukarıda başlık olarak belirtilen soruların cevaplarına göre istatistiksel sonuçlar elde edilmiştir. Anket formu Ek 1. elde edilen istatistiksel sonuçlar literatür sonuçlarıyla karşılaştırma yapılarak tartışılmıştır.

4. BULGULAR

Bu çalışmada uygulanan anket, küçük bir örnekleme temsil etmektedir. Küçük bir örneklem olmasına rağmen sorunların belirlenmesi için bir kısım katılımcı olarak Çukurova Üniversitesi (Sarıçam Adana, Türkiye) öğrencileri (yaş grubu, eğitimi ve akıllı telefon kullanıcıları oldukları için) seçilmiştir. Seyhan ilçesinde (Adana) yaşayan diğer katılımcılar ise rastgele olmak üzere seçilmişlerdir. Katılımcıların vereceği cevaplar çalışmanın seyri ve büyük örneklem seçimi için bir yol gösterici olma kanaatini oluşturmuştur. Ankete 241 kişi katılmış ve rastgele seçilmişlerdir. Katılımcıların cinsiyetleri değerlendirildiğinde % 34,9 erkekler, % 65,1 kadınlar olduğu gözlemlenmiştir. Anketlerde kadınların çoğunlukta olmasının nedeni öğrencilerden kaynaklanmaktadır. Kadın öğrenciler daha fazla olduğu için oranları da fazladır. Bu değerler çizelge 1 de verilmiştir.

Çizelge 1. Ankete cevap veren katılımcılar

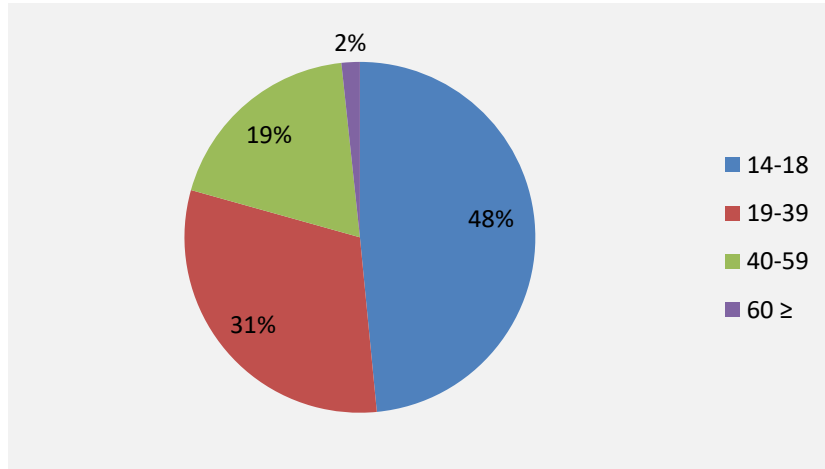
Cinsiyet	Toplam	Yüzde (%)
Kadınlar	157	% 65,1
Erkekler	84	% 34,9
Toplam	241	% 100

Katılımcıların yaşları sınıflandırıldığında, 0-19 arasında 116 katılımcının, 75'ini kadınlar ve 41'ini erkekler oluşturmaktadır. Yaşları 20-39 arasında olan 75 katılımcının, 57'i kadınlardan ve 18'i ise erkeklerden oluşmaktadır. 40-59 arasında 46 katılımcı vardır, 23'ü kadınlardan ve 23'ü de erkeklerden oluşmaktadır. Yaşları 60'den büyük 4 katılımcının 2'si kadın ve 2'si de erkektir. Katılımcıların cinsiyetleri ve yaşları değerlendirildiğinde, 20

den küçük olanların % 47,8'sini kadınlar, % 48,8'ini ise erkekler oluşturmaktadır. Yaşları, 21-29 arasında olanların % 36,3'ü kadınlar ve % 21,4'ü ise erkekler, 30-49 arasında olanların % 41,6'sı kadınlar ve % 27,4'si erkekler ve yaşları 50'den büyük olanların % 1,3'nü kadınlar ve % 2,4'ünü erkekler oluşturmaktadır. Bu değerler çizelge 2'de verilmiştir. Çalışmaya katılan ergenler, ailelerinin yanında ve gözetiminde anketi doldurmuşlardır

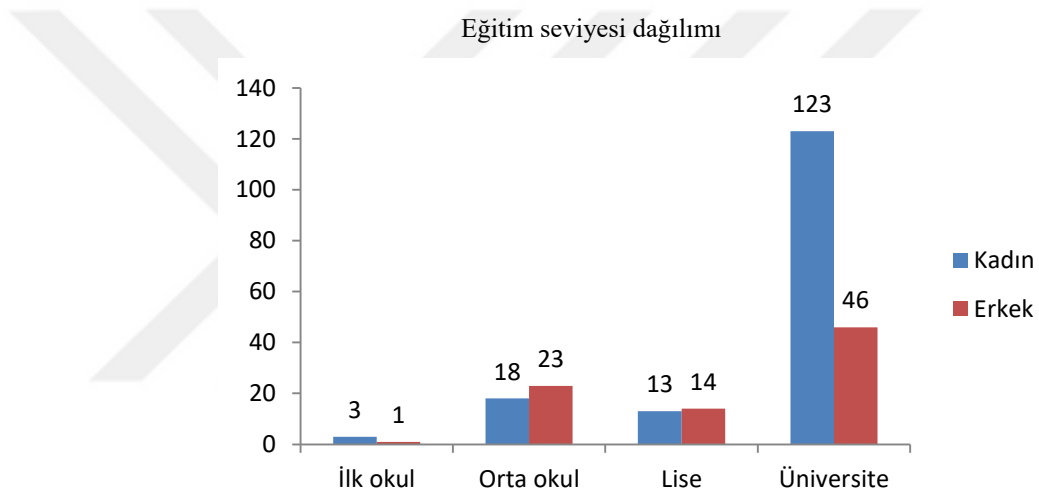
Çizelge 2. Katılımcılarının yaş guruplarına göre oranlarının dağılımları

Yaş gruplar	Cinsiyet				Toplam	
	Kadınlar		Erkekler			
	Sayı	Yüzde	Sayı	Yüzde	Sayı	Yüzde
14-18	75	% 47,8	41	% 48,8	116	% 48,1
19-39	57	% 36,3	18	% 21,4	75	% 31,1
40-59	23	% 14,6	23	% 27,4	46	% 19,1
60 ≥	2	% 1,3	2	% 2,4	4	% 1,7
Toplam	157	% 100	84	% 100	241	% 100



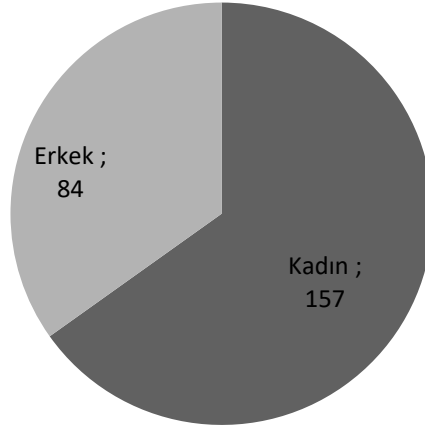
Şekil 2. Katılımcıların yaşlarına göre dağılımları

Katılımcılarımız eğitim seviyesi sınıflandığında, ilkokul mezunu 6 katılımcının, 3'ü erkek ve 3'ü ise kadınlardan oluşmaktadır. Ortaokul mezunu 41 katılımcının 18'i kadınlar ve 23 erkeklerden oluşmaktadır. Lise mezunu olan 27 katılımcının 13'ü kadınlardan ve 14'ü erkekler oluşturmaktadır. Üniversiteli olan 169 katılımcının 123'ünü kadınlar ve 46'sı ise erkeklerden oluşmaktadır. Şekil 3 de bu değerlerin grafiği verilmiştir.



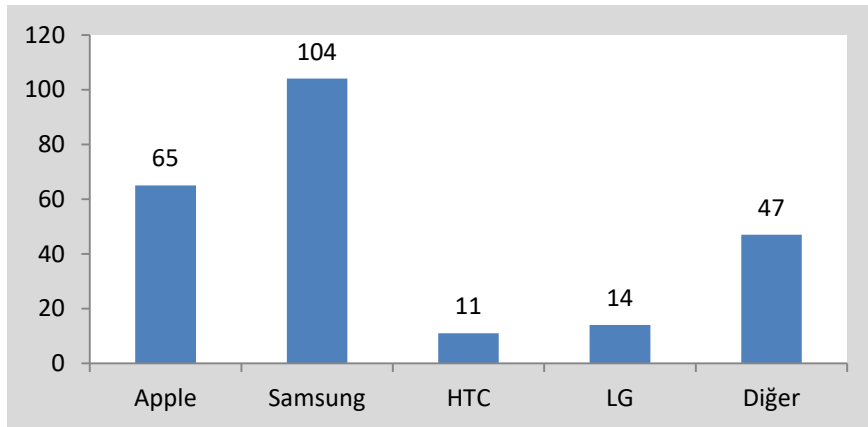
Şekil 3. Katılımcıları Eğitim seviyesine göre sınıflandırılması

Katılımcılarımıza yönelttiğimiz sorular içerisinde ilk akıllı telefonunuz var mı? İdi ve 157 kadın katılımcının ve 84 erkek katılımcının akıllı telefon kullandıklarını belirtmişlerdir. Bu değerlerin grafiği Şekil 3 ta verilmiştir.



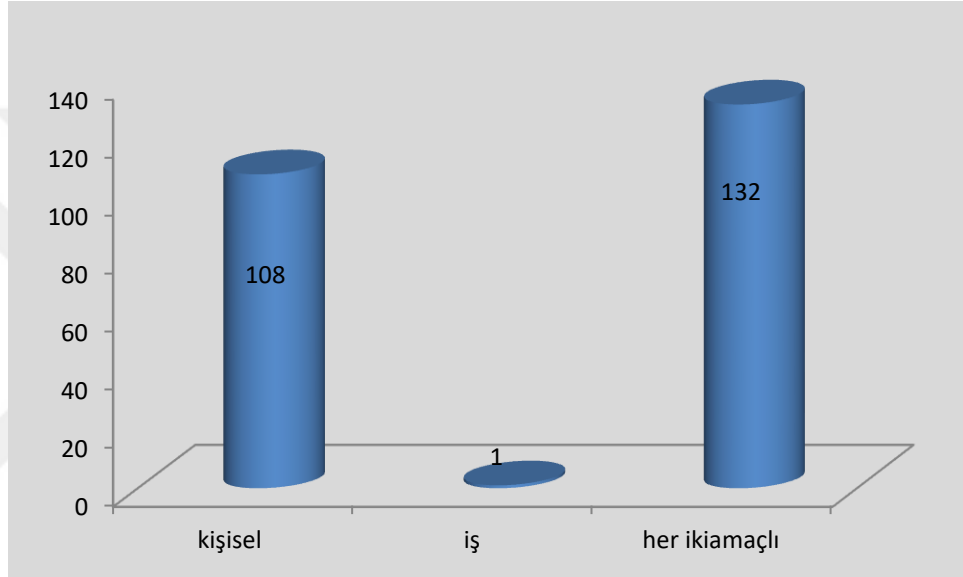
Şekil 4. Katılımcıların akıllı telefonları sayısının dağılımı

Bu çalışmada katılımcılara kullandıkları akıllı telefonları markası da sorulmuştur. Bu sorulara cevap veren katılımcıların Apple, Samsung HTC, LG ve venus, xioma gibi markaları kullandıklarını belirtmişlerdir. Katılımcılardan 65'i Apple, 104'ü Samsung, 11'i HTC, 14'ü LG, 47'i katılımcı ise diğer markaları kullandıklarını belirtmişlerdir. Şekil 4'te bu markaları kullanan katılımcıların grafiği verilmiştir.



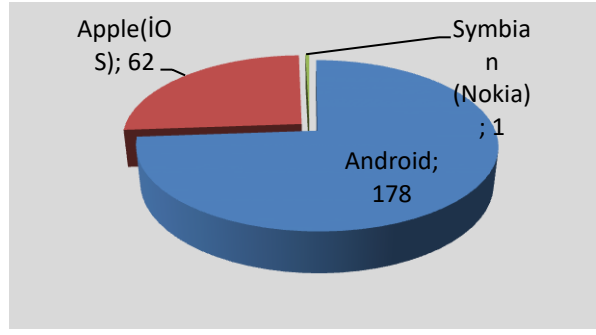
Şekil 5. Katılımcıların akıllı telefon markalar sayısı dağılımı

Bu çalışmada katılımcıların akıllı telefon kullanım amaçları da sorulmuştur. Bu sorulara cevap veren katılımcıların iş, kişisel kullanma veya her ikisi olarak da belirtmişlerdir. Katılımcılardan 108'i kişisel, 1'i iş ve her iki amaç için de diyen katılımcıların sayısı da 132'yi dır. Kullanım amaçlı katılımcıların değerlerini veren grafiği ise şekil 5'te verilmiştir



Şekil 6. Akıllı telefon kullanma amaç dağılımı

Bu çalışmada katılımcılara, kullanmakta oldukları akıllı telefonların işletim sistemi nedir? Sorusu yöneltilmiş ve cevap veren katılımcılar; işletim sistemlerinin 178'i Android, 62'i Apple (iOS), 1'i Symbian (Nokia) olduğunu belirtmişlerdir. Şekil 6'da bu değerlerin grafiği verilmiştir.

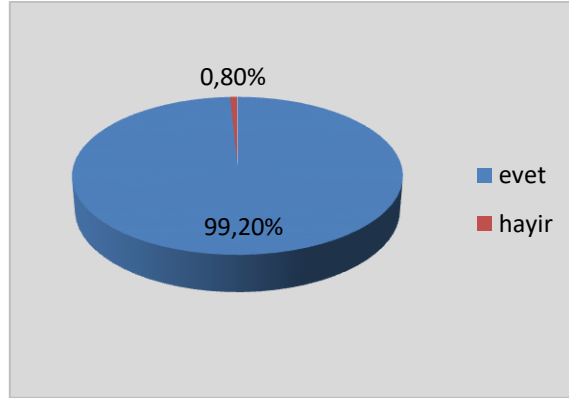


Şekil 7. Katılımcılarının akıllı telefon işletim sistem sayısı

Bu çalışmada katılımcılara akıllı telefonda internet kullanıp kullanmadıkları da sorulmuştur. 239'i katılımcı akıllı telefonda internet kullandıklarını ve 2'i katılımcı ise internet kullanmadıklarını belirtmişlerdir. Bu sonuçlar ve cinsiyet değerlendirildiğinde, internet kullananlar % 65,3'i kadınlar ve % 34,7'ini ise erkeklerden oluşmaktadır. İnternet kullanmayanlar katılımcıların cinsiyet dağılımı ise % 0,8'dir ve bu çizelge 3'de verilmiştir.

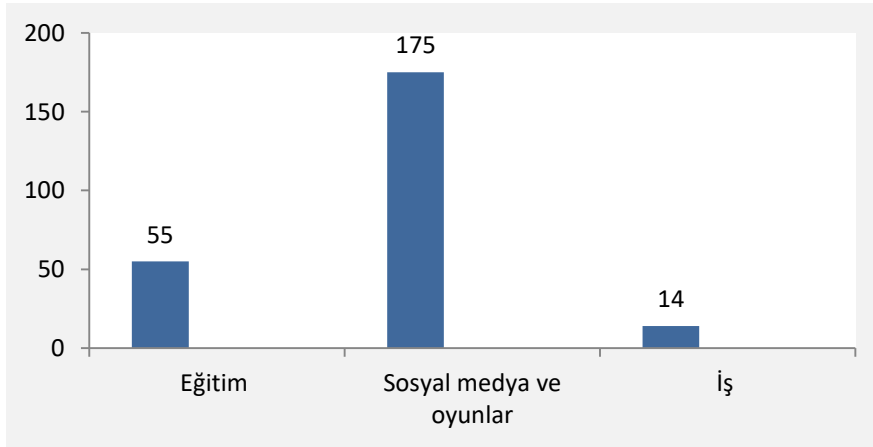
Çizelge 3. İnternet kullanma göre anketörlerin değerleri

İnternet kullanıyor musun?	Cinsiyet				Toplam	
	Kadın		Erkek			
	Sayı	Yüzde	Sayı	Yüzde	Sayı	Yüzde
Evet	156	% 99,4	83	% 98,8	239	% 99,2
Hayır	1	% 0,6	1	% 1,2	2	% 0,8
Toplam	157	% 100	84	% 100	241	% 100



Şekil 8. Katılımcıların internet kullanma dağılımları

Bu çalışmada katılımcılara, akıllı telefonları çoğunlukla ne için internet kullandıkları sorulmuştur. Bu sorulara cevap veren katılımcıların eğitim amacı, sosyal medya ve oyunlar ve iş amaçlı kullandıklarını belirtmişlerdir. 55'i eğitim amacı, 175'i sosyal medya 175'i ve oyunlar ve 14'ü iş amaçlı kullandıklarını belirtmişlerdir. Şekil 8'de katılımcılar internet kullanma amaçları grafiği verilmiştir.

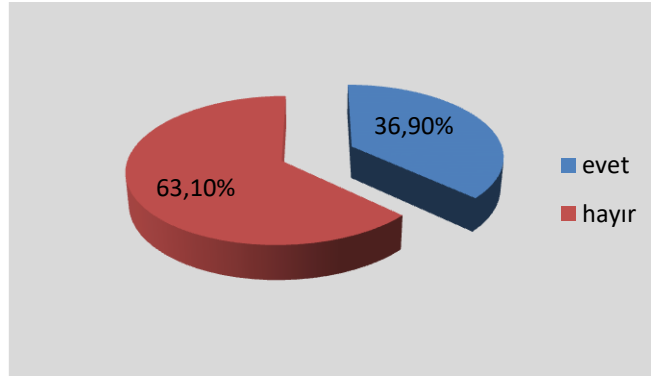


Şekil 9. Katılımcıların internet kullanma amaç dağılımları

Bu çalışmada katılımcılara yasaklı web sitelerine erişmek için VPN'yi kullanıp kullanmadığı sorulmuştur. Kadın katılımcıların %33,8(53)'i ve erkek katılımcıların %42,9(36)'u akıllı telefonlarda VPN kullandıklarını belirtmişlerdir. Bütün katılımcılar değerlendirildiğinde ise bu oranın %36,9 olduğu görülmüştür. Bu değerler çizelge 4'de gösterilmektedir.

Çizelge 4. VPN kullanımına göre katılımcıların dağılımları

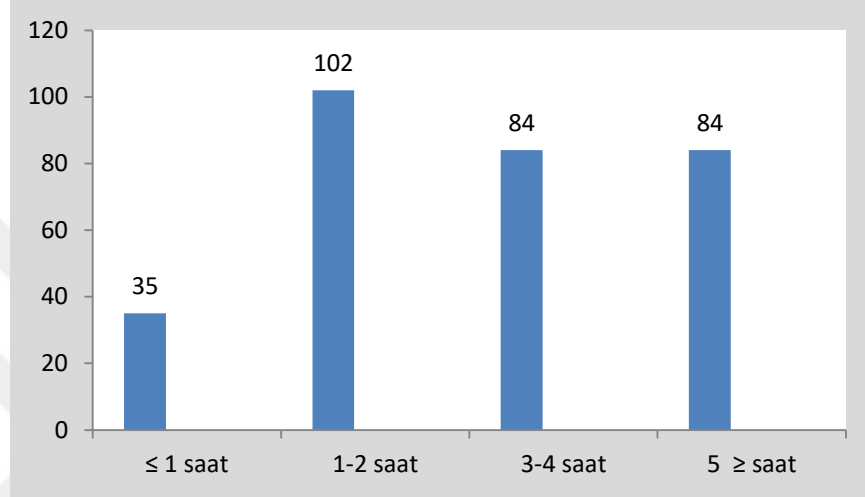
VPN (yasaklı web sitelerine erişmek için)	Cinsiyet				Toplam	
	Kadın		Erkek			
	Sayı	Yüzde	Sayı	Yüzde	Sayı	Yüzde
Evet	53	% 33,8	36	% 42,9	89	% 36,9
Hayır	104	% 66,2	48	% 57,1	152	% 63,1
Toplam	157	% 100	84	% 100	241	% 100



Şekil 10. Akıllı telefonlarda katılımcılarının VPN kullanma dağılımları

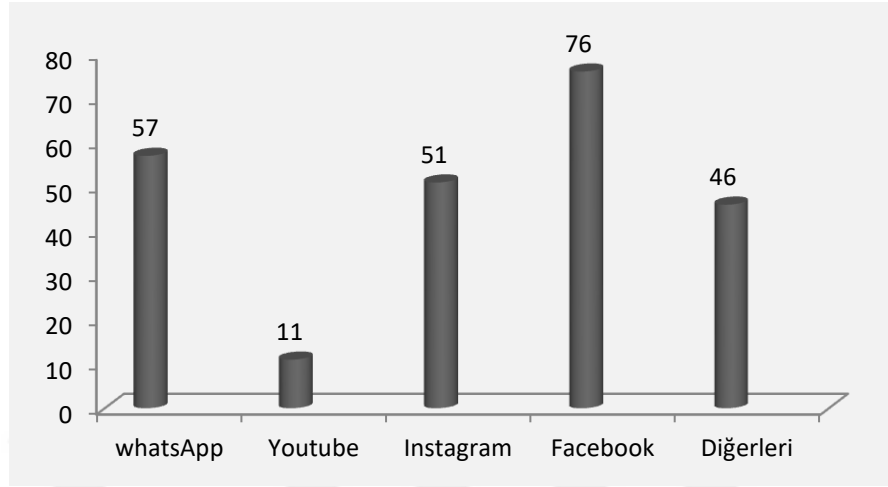
Bu çalışmada katılımcılara akıllı telefon uygulamaları (sosyal medya, mesajlaşma, oyunlar vb) kullanarak günde kaç saat zaman harcadıklarını sorulmuştur. Katılımcıların sosyal medyada günde kaç saat harcadıkları sınıflandığında, 35 kişinin 1 saatten az, 102 kişinin 1-2 saat aralığında, 84 kişinin 3-4 saat aralığında, 20 kişinin 5 saatten fazla

kullandığı görülmüştür. Şekil 10'da katılımcılar günlük internet kullanması grafiği verilmiştir.



Şekil 11. Katılımcıları günlük internet kullanma dağılımı

Bu çalışmada katılımcılara, akıllı telefonda en çok kullanılan uygulamaları yazınız diye sorulmuştur. Bu sorulara cevap veren katılımcıların Google chrom Twitter, Facebook ,Watsapp, Instagram, sozlük, yemek sepeti, banka uygulamaları, Snap-chat, e-okul gibi uygulamalar kullandıklarını belirtmişlerdir. Katılımcılardan 11'i Youtube, 76'i Facebook , 51'i Instagram , 57'i WatsApp, 11 katılımcı ise diğer uygulamaları kullandıklarını belirtmişlerdir. Şekil 11'de katılımcılar en çok kullanılan uygulamalar grafiği verilmiştir.

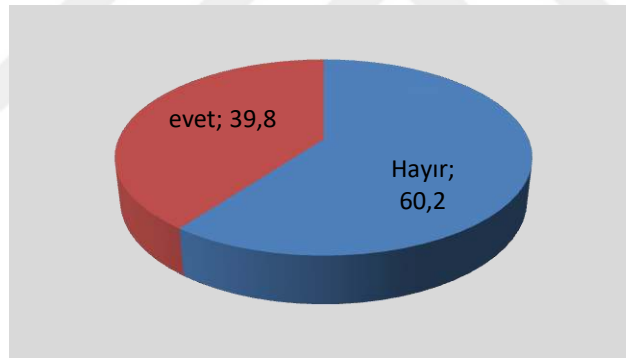


Şekil 12. Katılımcıların akıllı telefonda en çok kullandığı uygulamalar dağılımları

Bu çalışmada katılımcılara kullandığı sosyal medya uygulama hesapları oluştururken gerçek soyadı ve adı kullanıp kullanmadığı sorulmuştur Kadın katılımcıların % 10,2 (16)'si ve erkek katılımcıların % 13,1(11)'i akıllı telefonlarda gerçek adı ve soyadı kullanmadıklarını belirtmişlerdir. Bütün katılımcılar değerlendirildiğinde ise bu oranın % 11,1 olduğu görülmüştür. Bu değerler çizelge 5'te gösterilmektedir.

Çizelge 5. Katılımcılarının, sosyal medyada uygulamaları oluştururken gerçek ad ve soyadı kullanıp kullanmadıklarının dağılımları

Gerçek adı ve soyadı kullanıma	Cinsiyet				Toplam	
	Kadın		Erkek			
	Sayı	Yüzde	Sayı	Yüzde	Sayı	Yüzde
Evet	141	% 89,8	73	% 86,9	214	% 88.8
Hayır	16	% 10,2	11	% 13,1	27	% 11.2
Toplam	157	% 100	84	% 100	241	% 100

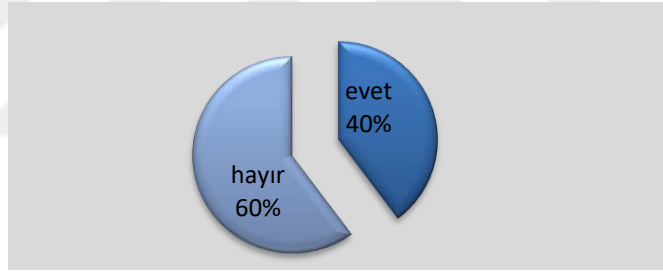


Şekil 13. Sosyal medyada uygulamaları oluştururken gerçek adı ve soyadı kullanım dağılımları

Bu çalışmada katılımcılardan kullandıkları uygulamaları, tavsiye ile kullanıp kullanmadıkları sorulmuştur. Kadın katılımcıların % 40,1 (63)'i ve erkek katılımcıların % 39,3 (33)'ü akıllı telefonda kullandıkları uygulamaları birinin tavsiyesi ile kullandıklarını belirtmişlerdir. . Bütün katılımcılar değerlendirildiğinde ise bu oranın % 39,8 olduğu bulunmuştur. Bu değerler çizelge 6'te verilmiştir.

Çizelge 6. Katılımcılara sosyal medya uygulamalarını tavsiye üzerine kullanma oranlarının dağılımları.

Tavsiye üzerine kullanım	Cinsiyet				Toplam	
	Kadın		Erkek			
	Sayı	Yüzde	Sayı	Yüzde	Sayı	Yüzde
Evet	63	% 40,1	33	% 39,3	96	% 39,8
Hayır	94	% 59,9	51	% 60,7	145	% 60,2
Toplam	157	% 100	84	% 100	241	% 100

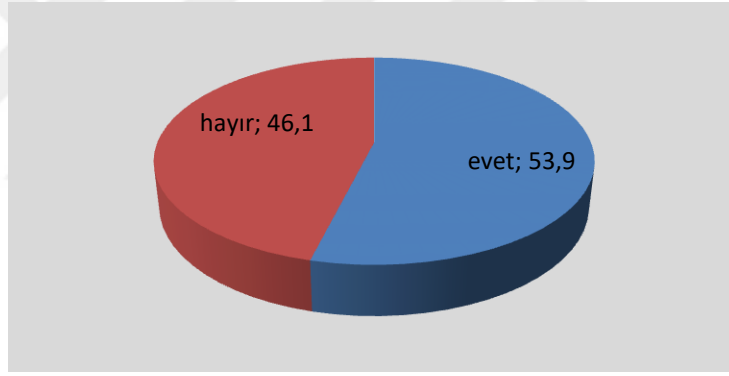


Şekil 14. Katılımcıların birisin tavsiye üzerine, sosyal medya uygulamalarının kullanımının dağılımları

Bu çalışmada katılımcılara akıllı telefonlarına uygulamaları yüklerken, indirmeden önce uygulama şartları ve koşullarını okuyup okumadıkları sorulmuştur. Erkek katılımcıların % 54,8'i, kadınların % 41,4'ü şart ve koşulları okumadıklarını belirtmişlerdir. Katılımcıların akıllı telefonlarına uygulamaları yüklerken, indirmeden önce uygulama şartları ve koşulları okuyup okumadıklarının dağılımları çizelge 7'de gösterilmiştir

Çizelge 7. Katılımcıların sosyal medya uygulamalar indirmeden şartlar ve koşullar okuma oranlarının dağılımları

Şart ve koşullar okuyorum	Cinsiyet				Toplam	
	Kadın		Erkek			
	Sayı	Yüzde	Sayı	Yüzde	Sayı	Yüzde
Evet	92	% 58,6	38	% 45,2	130	% 53,9
Hayır	65	% 41,4	46	% 54,8	111	% 46,1
Toplam	157	% 100	84	% 100	241	% 100

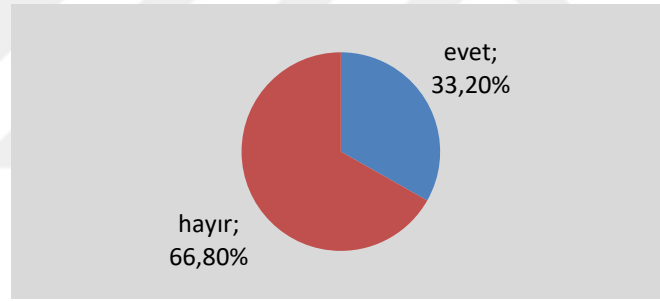


Şekil 15. Katılımcılara akıllı telefonlarına uygulamaları yüklerken, indirmeden önce uygulama şart ve koşullarını okuma dağılımları

Bu çalışmada katılımcılara sahte sosyal medya hesabı oluşturup oluşturmadıkları sorulmuştur. Kadın katılımcıların % 33,1'i, erkek katılımcıların % 33,3'u sahte hesap oluşturadığını belirtmiştir. Çizelge 8'de gösterilmiştir.

Çizelge 8. Katılımcıların sosyal medya uygulamalar sahte hesap oluşturma oranlarının dağılımları

Sahte sosyal medya hesabı oluşturma	Cinsiyet				Toplam	
	Kadın		Erkek			
	Sayı	Yüzde	Sayı	Yüzde	Sayı	Yüzde
Evet	52	% 33,1	28	% 33,3	161	% 33,2
Hayır	105	% 66,9	56	% 66,7	80	% 66,8
Toplam	157	% 100	84	% 100	241	% 100



Şekil 16. Katılımcılara sosyal medya uygulamalar sahte hesap oluşturma dağılımları

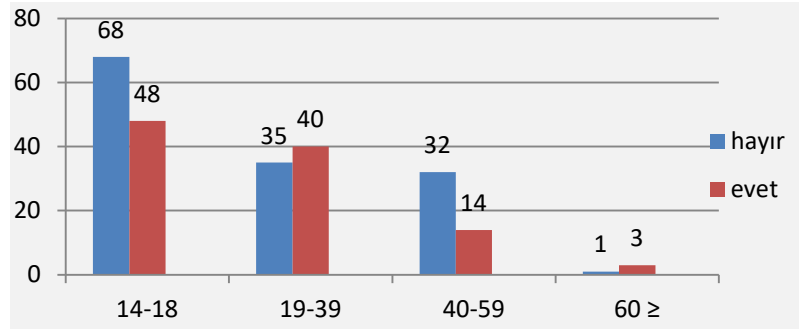
Bu çalışmada katılımcılara sahte bir Facebook hesabı kullanılarak sosyal medyadaki biri tarafından rahatsız edilip edilmedikleri soruldu. Kadın katılımcıların % 44,6'sı, erkek katılımcıların % 41,7'si rahatsız edildiğini belirtmişlerdir. Bu değerler çizelge 9'da verilmiştir.

Bu çalışmada katılımcılar yaş gruplarına göre sınıflandırıldığında, 0-19 yaş grubundaki 116 katılımcıdan 68 katılımcının Facebook üzerinden rahatsız edilmediği, 48 katılımcının ise rahatsız edildiklerini ortaya konulmuştur. 20-39 yaş grubundaki 75 katılımcıdan 35 katılımcının Facebook üzerinden rahatsız edilmediği, 40 katılımcının ise rahatsız edildiği belirtmiştir. 40-59 yaş grubu 46 katılımcılarından 32 katılımcının Facebook üzerinden rahatsız edildiği, 14 katılımcının ise rahatsız edilmediklerini

belirtmişlerdir. 60 ve üstü yaş grubundaki 4 katılımcıdan 1 katılımcının Facebook tan üzerinden rahatsız edilmediği, 3 katılımcının rahatsız edildiği tespit edilmiştir. Şekil 15 de katılımcıların Facebookta rahatsız edilme sahte bir Facebook hesabı kullanılarak yaş göre dağılımları grafiği verilmiştir.

Çizelge 9. Sahte bir Facebook hesabından sosyal medyadaki biri tarafından rahatsız edilme oranlarının dağılımları

Facebookta rahatsız edilme	Cinsiyet				Toplam	
	Kadın		Erkek			
	Sayı	Yüzde	Sayı	Yüzde	Sayı	Yüzde
Evet	70	% 44,6	35	% 41,7	105	% 43,6
Hayır	87	% 55,4	49	% 58,3	136	% 56,4
Toplam	157	% 100	84	% 100	241	% 100



Şekil 17. Kullanıcıların, sahte bir Facebook hesabından rahatsız edilmelerinin yaşa göre dağılımları

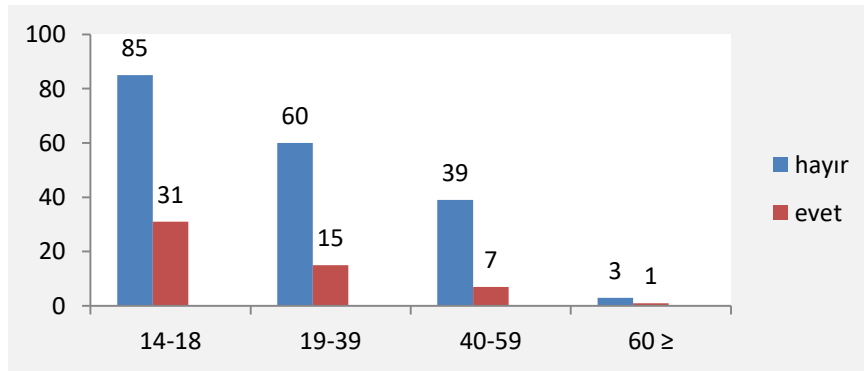
Bu çalışmada diğer bir sorunun sonucunda ise, 187 katılımcının Twitter üzerinden rahatsız edilmediğini, 54 katılımcının rahatsız edildiğini, bunların 37'sinin kadın ve 17'sinin erkek olduğu görüldü. Bu sonuçlar ve cinsiyet değerlendirildiğinde, kadın katılımcıların %

76,4'ü ve erkeklerin % 79,8'i rahatsız edilmediği belirlenmiştir Bu değerler çizelge 10'da gösterilmiştir.

Katılımcılarımız yaş grupları karşılaştığında, 0-19 grubu 116 katılımcıdan 85'inin, 20-39 yaş grubunda 75 katılımcıdan 60'ının, 40-59 yaş grubu 46 katılımcıdan 39'unun rahatsız edilmediği, 60 ve üstü yaş grubu 4 kişinin rahatsız edildiği görülmüştür. Şekil 16 da katılımcıların sahte bir Twitter hesabından rahatsız edilmelerinin yaş göre dağılımlarının grafiği verilmiştir.

Çizelge 10. Katılımcılara sahte bir Twitter hesabından sosyal medyadaki biri tarafından rahatsız edilme oranlarının dağılımları

Twitterda üzerinden rahatsız edildim	Cinsiyet				Toplam	
	Kadın		Erkek			
	Sayı	Yüzde	Sayı	Yüzde	Sayı	Yüzde
Evet	37	% 23,6	17	% 20,2	54	% 22,4
Hayır	120	% 76,4	67	% 79,8	187	% 77,6
Toplam	157	% 100	84	% 100	241	% 100



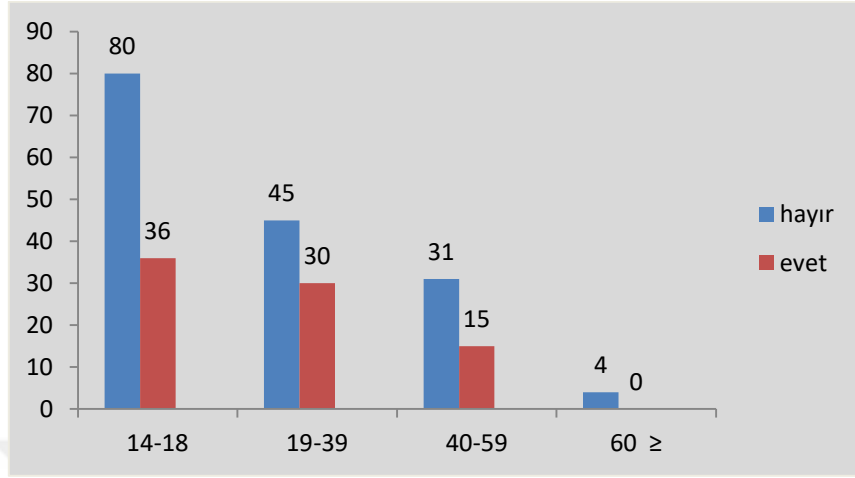
Şekil 18. Katılımcıların, sahte bir Twiter hesabından yaş göre rahatsız edilme dağılımları

Çalışmamızda katılımcıların Whatsapp uygulaması üzerinden rahatsız edilip edilmedikleri değerlendirildiğinde; kadın katılımcıların % 33,8'inin, erkeklerin ise % 33,3'ünün rahatsız edildiği tespit edilmiştir. Çizelge 11'de gösterilmiştir.

Katılımcıların Whatsapp uygulaması üzerinden rahatsız edilip edilmediğinin yaş gruplarına göre dağılımı değerlendirildiğinde; 0-19 yaş grubunda 116 katılımcıdan 36'sının rahatsız edildiği, 20-39 yaş grubu 75 katılımcıdan 30'unun rahatsız edildiği, 40-59 yaş grubu 46 katılımcıdan 15'inin rahatsız edildiği, 60 ve üstü yaş grubunda 4 katılımcıdan hiçbirinin rahatsız edilmediği anlaşılmıştır. Şekil 17. Katılımcıların sahte bir Whatsapp hesabı kullanılarak rahatsız edilenlerin yaş göre dağılımlarının grafiği verilmiştir.

Çizelge 11. Katılımcılara sahte bir Whatsapta hesabı kullanılarak sosyal medyadaki biri tarafından rahatsız edilme oranlarının dağılımları

Whatsapp üzerinden rahatsız edilme	Cinsiyet				Toplam	
	Kadın		Erkek			
	Sayı	Yüzde	Sayı	Yüzde	Sayı	Yüzde
Evet	53	% 33,8	28	% 33,3	81	% 33,6
Hayır	104	% 66,2	56	% 66,7	160	% 66,4
Toplam	157	% 100	84	% 100	241	% 100



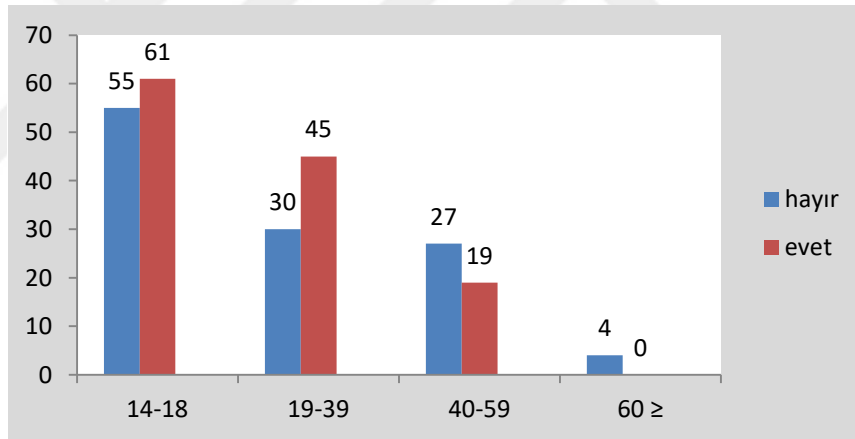
Şekil 19. Katılımcıların sahte bir hesapla Whatsapp'ta rahatsız edilmelerinin bir yaş göre dağılımları

Bu çalışmada katılımcılara Instagram üzerinden rahatsız edilip edilmediği sorgulandığında, kadın katılımcıların % 59,9'unun, erkek katılımcıların % 36,9'unun rahatsız edildiği görüldü. Çizelge 12'de gösterilmiştir.

Katılımcıların Instagram uygulaması üzerinden rahatsız edilip edilmediğinin yaş gruplarına göre dağılımı değerlendirildiğinde; 0-19 yaş grubunda 116 katılımcıdan 61'inin rahatsız edildiği, 20-39 yaş grubu 75 katılımcıdan 45'inin rahatsız edildiği, 40-59 yaş grubu 46 katılımcıdan 19'unun rahatsız edildiği, 60 ve üstü yaş grubunda 4 katılımcıdan hiçbirinin rahatsız edilmediği görüldü. Şekil 18. Katılımcıların rahatsız edilme sahte bir Instagram hesabından yaş guruplarına göre dağılımlarının grafiği verilmiştir.

Çizelge 12. Katılımcılara sahte bir Instagramda hesabı kullanılarak sosyal medyadaki biri tarafından rahatsız edilme oranlarının dağılımları

Instagram üzerinden rahatsız edilme	Cinsiyet				Toplam	
	Kadın		Erkek			
	Sayı	Yüzde	Sayı	Yüzde	Sayı	Yüzde
Evet	94	% 59,9	31	% 36,9	125	% 48,4
Hayır	63	% 40,1	53	% 63,1	116	% 51,6
Toplam	157	% 100	84	% 100	241	% 100

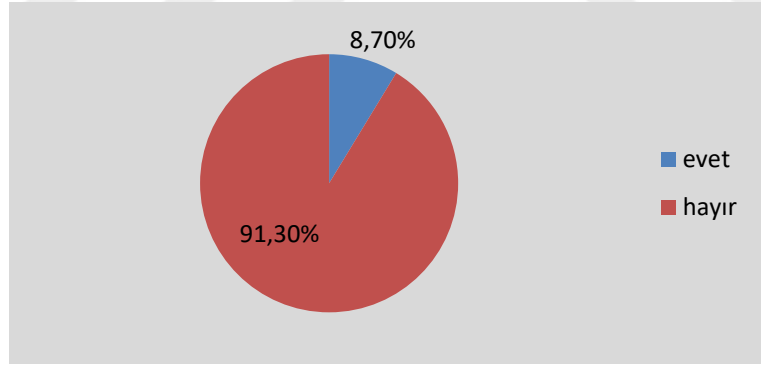


Şekil 20. Katılımcıların Instagramda sahte bir hesap kullanılarak rahatsız edilmelerinin yaşa göre dağılımları

Bu çalışmada katılımcılara diğer sosyal medya uygulamalar (Snapchat vs) üzerinden rahatsız edilip edilmediği sorgulandığında, kadın katılımcıların % 7,6'sının, erkek katılımcıların % 10,7'sinin rahatsız edildiği görülmüştür. Bu oranlar çizelge 13'te gösterilmiştir.

Çizelge 13. Katılımcılara diğer sosyal medya uygulamalara sahte hesabı kullanılarak sosyal medyadaki biri tarafından rahatsız edilme oranlarının dağılımları

Diğer sosyal medya uygulamaları üzerinden rahatsız edilme	Cinsiyet				Toplam	
	Kadın		Erkek			
	Sayı	Yüzde	Sayı	Yüzde	Sayı	Yüzde
Evet	12	% 7,6	9	% 10,7	21	% 8,7
Hayır	145	% 92,4	75	% 89,3	220	% 91,3
Toplam	157	% 100	84	% 100	241	% 100

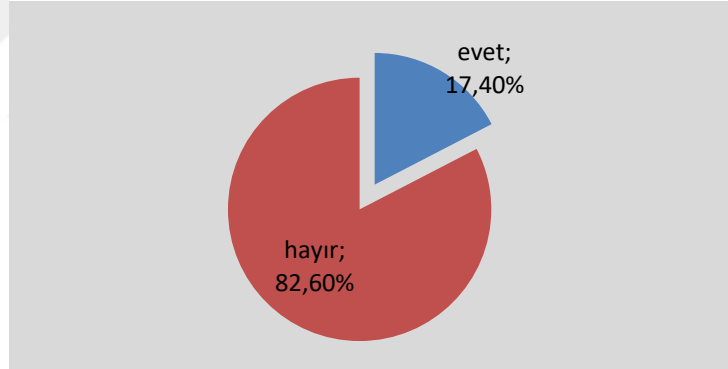


Şekil 21. Katılımcıların rahatsız edilme diğer sosyal medya uygulamalar sahte hesabı kullanılarak yaş göre dağılımları

Bu çalışmada katılımcılara sosyal medyada siber takip veya zorbalığa maruz kalıp kalmadığı sorgulandığında; kadın katılımcıların % 17,8'inin erkek katılımcıların ise % 16,7'sinin siber takip veya zorbalığa maruz kaldığı görülmüştür. Bu oranlar çizelge 14'dü gösterilmiştir.

Çizelge 14. Katılımcıların sosyal medyada sosyal medyada siber takip veya zorbalığı muhatap olan oranlarının dağılımları

Sosyal medyada siber takip veya zorbalığı muhatap olma	Cinsiyet				Toplam	
	Kadın		Erkek			
	Sayı	Yüzde	Sayı	Yüzde	Sayı	Yüzde
Evet	28	% 17,8	14	% 16,7	42	% 17,4
Hayır	129	% 82,2	70	% 83,3	199	% 82,6
Toplam	157	% 100	84	% 100	241	% 100

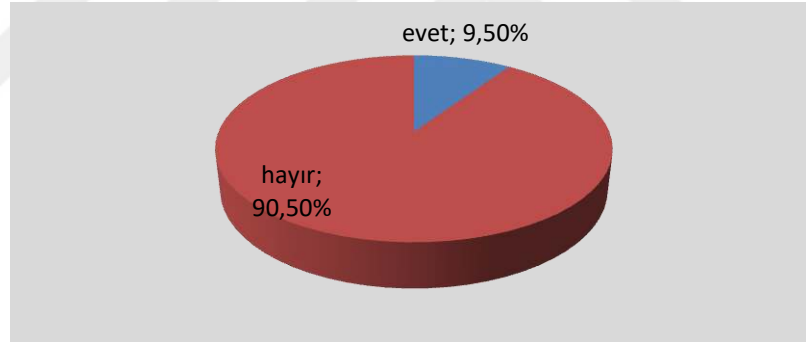


Şekil 22. Katılımcıların akıllı telefonlarda sosyal medyada siber takip veya zorbalığı muhatap olan dağılımları

Bu çalışmada katılımcılara konum bildiren uygulamaları kullanan birisi tarafından takip edilip edilmediği sorgulandığında; kadın katılımcıların % 8,9'unun, erkek katılımcıların ise % 10,7'unun takip edildiği anlaşılmıştır. Tablo 15'te bu oranlar verilmiştir.

Çizelge 15. Katılımcıların akıllı telefonlarda konu bildiren uygulamalar tarafından takip edilme oranlarının dağılımları

Konu bildiren uygulamalar tarafından takip edilme	Cinsiyet				Toplam	
	Kadın		Erkek			
	Sayı	Yüzde	Sayı	Yüzde	Sayı	Yüzde
Evet	14	% 8,9	9	% 10,7	23	% 9,5
Hayır	143	% 91,1	75	% 89,3	218	% 90,5
Toplam	157	% 100	84	% 100	241	% 100

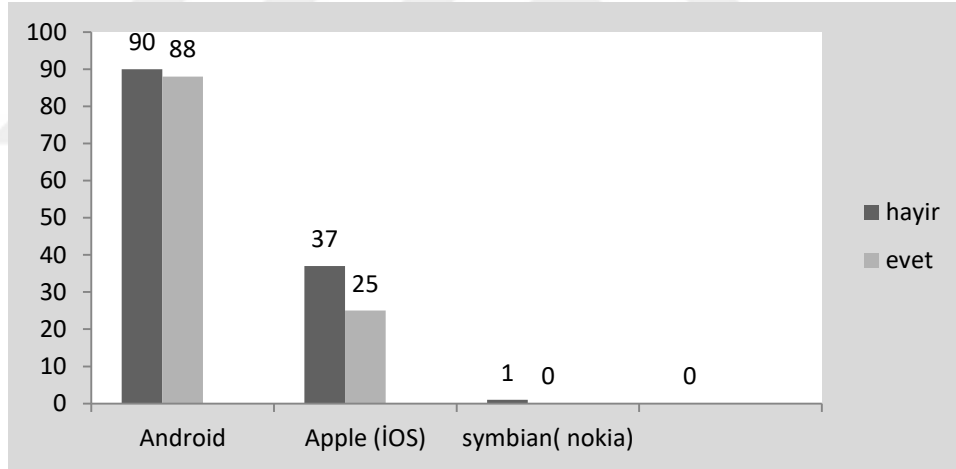


Şekil 23. Katılımcıların konu bildiren uygulamalar tarafından takip edilme dağılımları

Çalışmamızda katılımcıların telefonlarının bir bağlantı yoluyla paylaşılan virüslerden etkilenip etkilenmediği değerlendirildiğinde, erkek katılımcıların % 51,2'sinin, kadınların %44,6'sının telefonlarının olumsuz etkilendiği görülmüştür. Bu değişimler çizelge 16'da gösterilmiştir. Telefonların işletim sistemleri karşılaştırıldığında Android işletim sistemine sahip telefon kullanan 178 kişiden 88'inin, IOS işletim sistemine sahip telefon kullanan 62 kişiden 25'inin telefonlarının olumsuz etkilendiği belirlenmiştir. Şekil 21 de bir bağlantı (Wi-Fi, Bluetooth) yoluyla bulaşan virüslerden katılımcıların telefon işletim sistem olumsuz etkileme oranlarının dağılımlarının grafiği verilmiştir.

Çizelge 16. Bir bağlantı yoluyla paylaşılan virüslerden katılımcıların telefonlarının olumsuz etkilenme oranlarının dağılımları

Virüslerden telefonum olumsuz etkilendi	Cinsiyet				Toplam	
	Kadın		Erkek			
	Sayı	Yüzde	Sayı	Yüzde	Sayı	Yüzde
Evet	70	% 44,6	43	% 51.2	113	% 46,9
Hayır	87	% 55,4	41	% 48.8	128	% 53,1
Toplam	157	% 100	84	% 100	241	% 100

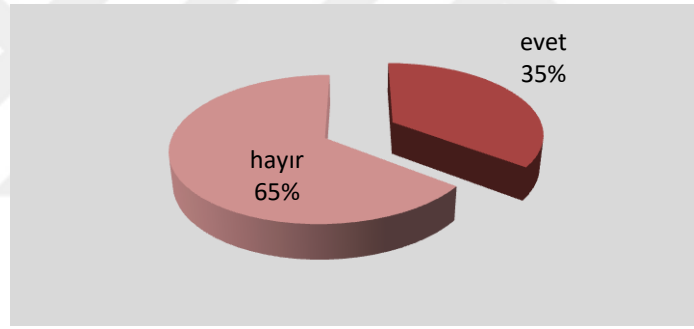


Şekil 24. Bir bağlantısı yoluyla paylaşılan virüslerden katılımcılarının telefon işletim sistem olumsuz etkilenme oranlarının dağılımları

Bu çalışmada katılımcılara ikinci el akıllı telefon kullanıp kullanmadıkları sorulmuş. Kadınların % 31,8'i ve % erkeklerin % 41,7'i ikinci el akıllı telefon kullandıkları anlaşılmıştır ve değerler çizelge 17'de gösterilmiştir.

Çizelge 17. Katılımcıların ikinci el akıllı telefon kullanma oranlarının dağılımları

İkinci el akıllı telefon Kullanma	Cinsiyet				Toplam	
	Kadın		Erkek			
	Sayı	Yüzde	Sayı	Yüzde	Sayı	Yüzde
Evet	50	% 31,8	35	% 41,7	85	% 35,3
Hayır	107	% 68,2	49	% 58,3	156	% 64,7
Toplam	157	% 100	84	% 100	241	% 100

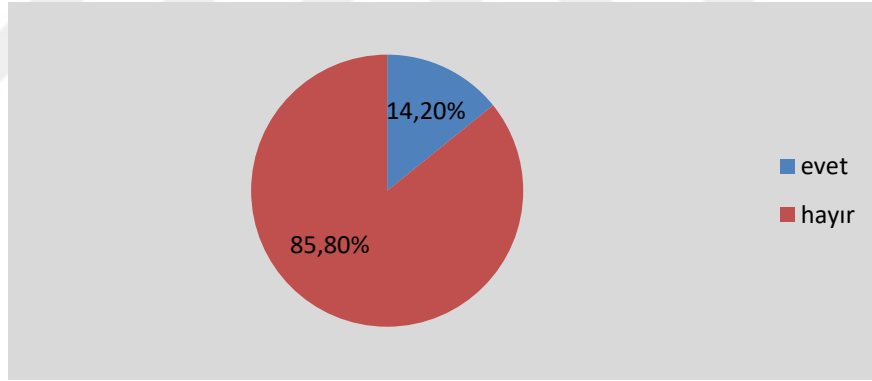


Şekil 25. Katılımcıların ikinci el akıllı telefonlar kullanma oranlarının dağılımları

Bu çalışmada katılımcılara; bilmeden kullandıkları ikinci el telefon yüzünden herhangi bir sorunla karşılaşp karşılaşmadıkları sorulmuştur. Sorunun cevabı sonucunda, kadınların % 7,0'ı ve erkeklerin % 21,4'ü ikinci el akıllı telefon kullandıklarında sorun yaşadıklarını belirtmişlerdir ve değerler çizelge 18'de gösterilmiştir.

Çizelge 18. İkinci el akıllı telefon kullanırken katılımcıların sorun yaşama oranlarının dağılımları

İkinci el akıllı telefon kullanırken sorun yaşayanlar	Cinsiyet				Toplam	
	Kadın		Erkek			
	Sayı	Yüzde	Sayı	Yüzde	Sayı	Yüzde
Evet	11	% 7	18	% 21,4	29	% 14,2
Hayır	146	% 93	66	% 78,6	212	% 85,8
Toplam	157	% 100	84	% 100	241	% 100

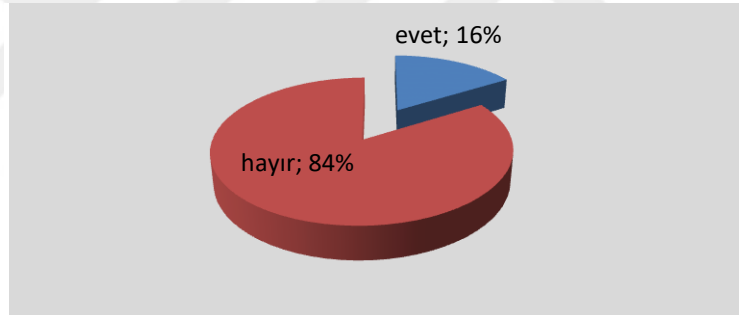


Şekil 26. İkinci el akıllı telefon kullanırken katılımcıların sorun yaşama oranlarının dağılımları

Bu çalışmada katılımcılara hiç izin almadan başkasının IMEI (yurt dışında gelen telefonlar) numarasını kendi telefonlarında kullanıp kullanmadıkları sorulmuştur. Kadınların % 12,1'i ve erkeklerin % 23,8'i herhangi bir izin almadan başkasının IMEI numarasını kullandıklarını belirtmiştir. Bu dağılım çizelge 19'da gösterilmiştir.

Çizelge 19. Katılımcıların izin almadan başkasının İMEİ numarasını kullanma oranlarının dağılımları

İzin almadan başkasının İMEİ numarasını kullananlar	Cinsiyet				Toplam	
	Kadın		Erkek			
	Sayı	Yüzde	Sayı	Yüzde	Sayı	Yüzde
Evet	19	% 12,1	20	% 23,8	39	% 16,2
Hayır	138	% 87,9	64	% 76,2	202	% 83,8
Toplam	157	100%	84	% 100	241	% 100

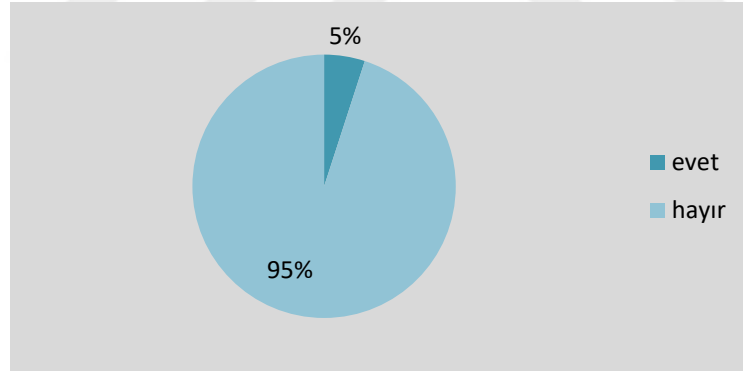


Şekil 27. Katılımcılar izin almadan başkasına ait IMEI numarasını kullanma oranlarının dağılımları

Bu çalışmada katılımcılara başkasının İMEİ'ne kayıtlı herhangi bir akıllı telefon kullanırken yasal sorunlara yol açan herhangi bir problemle karşılaşp karşılaşmadıkları soruldu. Kadınların % 4,5'i, erkeklerin % 6'ı polisle yasal bir problemle karşılaştığını belirtmiş ve dağılım çizelge 20'de gösterilmiştir.

Çizelge 20. Katılımcılar başkasının IMEI numarasını kullanırken yasal sorun yaşama oranlarının dağılımları

Başkasının IMEI numarasını kullanırken yasal sorun yaşama durumu	Cinsiyet				Toplam	
	Kadın		Erkek			
	Sayı	Yüzde	Sayı	Yüzde	Sayı	Yüzde
Evet	7	% 4,5	5	% 6	12	% 5
Hayır	150	% 95,5	79	% 94	229	% 95
Toplam	157	% 100	84	% 100	241	% 100

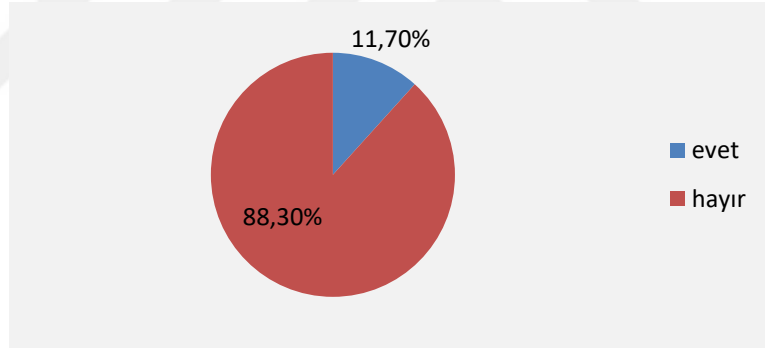


Şekil 28. Katılımcılar başkasına ait IMEI numarası olan bir telefon kullanma oranları

Bu çalışmada katılımcılara akıllı telefonlarının çalınıp çalınmadığı sorulmuştur. Kadınların %11,5'i ve erkeklerin %12,0'ı akıllı telefonlarının çalındığını belirtmiştir. Tablo 21'de gösterilmiştir.

Çizelge 21. Katılımcıların akıllı telefonlarının çalınma oranlarının dağılımları

Akıllı telefonun çalınma durumu	Cinsiyet				Toplam.	
	Kadın		Erkek			
	Sayı	Yüzde	Sayı	Yüzde	Sayı	Yüzde
Evet	18	% 11,5	10	% 12	28	% 11,7
Hayır	139	% 88,5	73	% 88	212	% 88,3
Toplam	157	% 100	84	100%	241	% 100

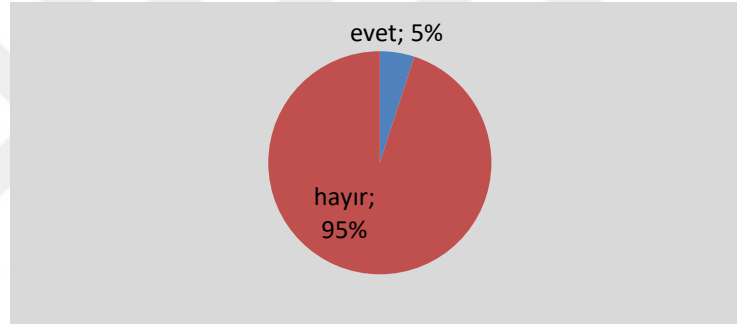


Şekil 29. Katılımcıların akıllı telefonlarının çalınma oranları

Bu çalışmada katılımcılara telefonların çalınması ile kişisel bilgilerinin tehlikeye atılıp atılmadığı soruldu. Kadınların % 5,1'i ve erkeklerin % 4,8'i kişisel bilgilerinin tehlikeye atıldığını belirtmişler ve değerler çizelge 22'de gösterilmiştir.

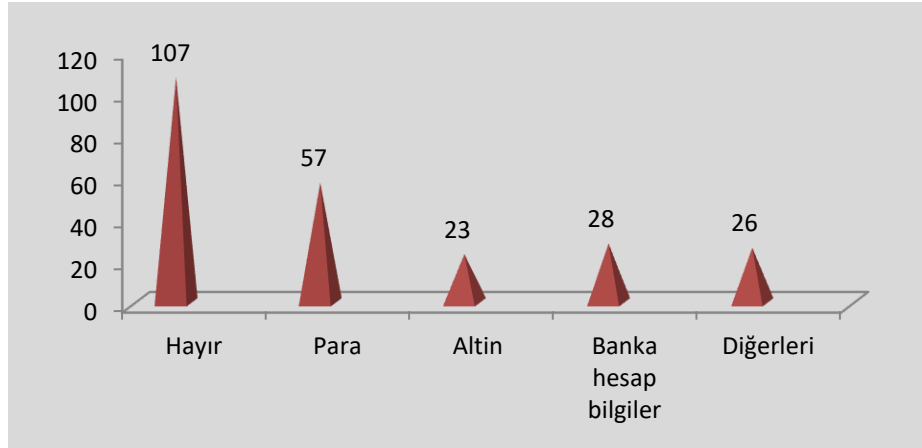
Çizelge 22. Katılımcılarının akıllı telefonda bulunan kişisel bilgilerinin tehlikeye atılma oranları

Kişisel bilgilerin çalışınma durumu	Cinsiyet				Toplam.	
	Kadın		Erkek			
	Sayı	Yüzde	Sayı	Yüzde	Sayı	Yüzde
Evet	8	% 5,1	4	% 4,8	12	% 5
Hayır	149	% 94,9	80	% 95,2	229	% 95
Toplam	157	% 100	84	% 100	241	% 100



Şekil 30. Katılımcılarının akıllı telefon kişisel bilgileri tehlikeye atılma oranları

Katılımcılarımıza dolandırıcılardan bir telefon veya mesaj alıp almadıkları sorulmuş. 107 katılımcıya mesaj ya da bir telefon araması gelmediğini, fakat 134 katılımcıdan para, altın, banka hesap bilgileri vb. istendiğini belirtmişlerdir. Bu kişiler arasında 57 kişiden para, 23 kişiden altın, 28 kişiden banka hesap bilgileri, 26 kişiden başka şeyler talep edilmiştir. Şekil 27’de dolandırıcılardan telefonla aranma ya da SMS yoluyla talepte bulunulanların oranlarının grafiği verilmiştir.

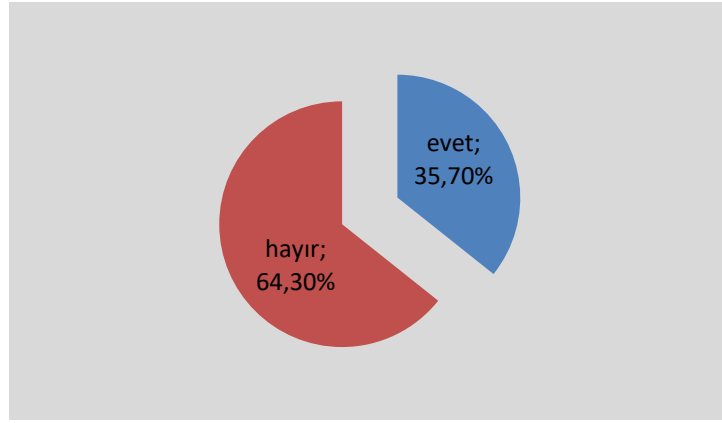


Şekil 31. Dolandırıcılardan telefonla aranma ya da mesaj alınma ve talepte bulunulanların oranları

Bu çalışmada katılımcılara E-dolandırıcılık (e-mail gibi gönderilen linkler ile kişisel bilgilerin (banka hesap bilgileri vs.) çalınması yaşayıp yaşamadıkları sorulmuş. Kadınların %35'i ve erkeklerin % 36,9'u e-dolandırıcılıkla karşılaştığını belirtmiştir. Bu dağılım çizelge 23'te gösterilmiştir.

Çizelge 23. Katılımcılarının E-dolandırıcılık yaşama oranlarının dağılımları

Katılımcılarımız E-dolandırıcılık yaşadılar mı?	Cinsiyet				Toplam	
	Kadın		Erkek			
	Sayı	Yüzde	Sayı	Yüzde	Sayı	Yüzde
Evet	55	% 35	31	% 36,9	86	% 35,7
Hayır	102	% 65	53	% 63,1	155	% 64,3
Toplam	157	% 100	84	% 100	241	% 100

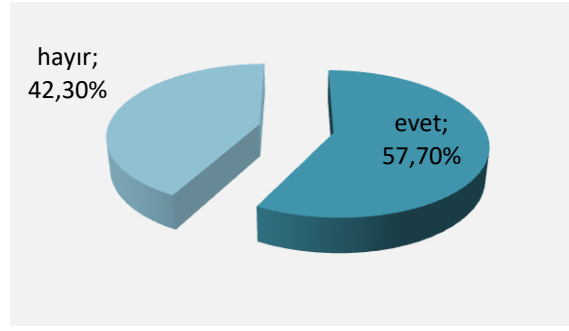


Şekil 32. Katılımcıların E-dolandırıcılık yaşama oranları

Bu çalışmada katılımcılara kredi kartıyla telefonda alışveriş yapıp yapmadıkları sorulmuştur. Kadınların % 60,5'i ve erkeklerin % 52,4'ü kredi kartıyla telefonda alışveriş yaptıklarını belirtmiştir. Bu dağılım tablo 21 ve çizelge 24'te gösterilmiştir.

Çizelge 24. Kredi kartlarıyla akıllı telefonlarında alışveriş yapanlar oranlarının dağılımları

Kredi kartlarıyla akıllı telefonlarında alışveriş yaptılar mı?	Cinsiyet				Toplam	
	Kadın		Erkek			
	Sayı	Yüzde	Sayı	Yüzde	Sayı	Yüzde
Evet	95	% 60,5	44	% 52,4	139	% 57,7
Hayır	62	% 39,5	40	% 47,6	102	% 42,3
Toplam	157	% 100	84	% 100	241	% 100

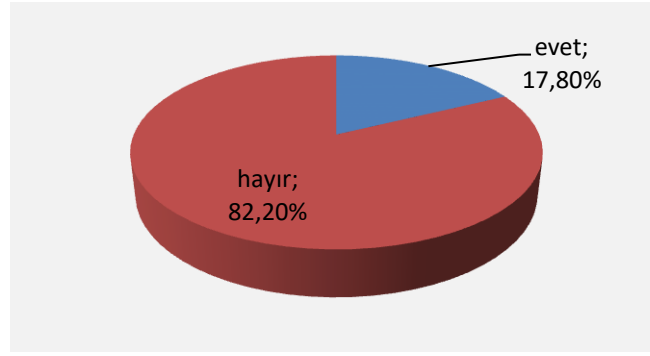


Şekil 33. Katılımcılar akıllı telefonlar ile kredi kartıyla alışveriş yapma dağılımları

Bu çalışmada katılımcılara; kredi kartlarıyla alışveriş yaparken herhangi bir sorunla karşılaşp karşılaşmadıkları sorusu yöneltildiğinde, (sanal web gibi ya da yanlış ürün veya sahte ürün aldılar mı?) kadınların % 15,9'u ve erkeklerin % 21,4'ü sorunlar ile karşılaştıklarını belirtmiştir. Bu dağılım tablo 25'te gösterilmiştir.

Çizelge 25. Akıllı telefonlarda kredi kartıyla alışveriş yaparken sorun yaşayanların oranlarının dağılımları

Akıllı telefonlarda alışveriş yaparken sorun yaşayanlar	Cinsiyet				Toplam	
	Kadın		Erkek			
	Sayı	Yüzde	Sa yı	Yüzde	Sayı	Yüzde
Evet	25	% 15,9	18	% 21,4	43	% 17,8
Hayır	132	% 84,1	66	% 78,6	198	% 82,2
Toplam	157	% 100	84	% 100	241	% 100

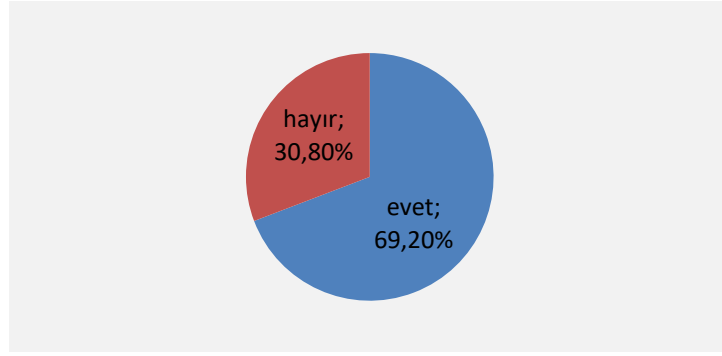


Şekil 34. Akıllı telefonlarda kredi kartıyla alışveriş yaparken sorun yaşayanların oranları

Bu çalışmada katılımcılara banka uygulamalarını (İş Cep, Ziraat Mobil vb) kullanıp kullanmadıkları sorulmuştur. Kadınların % 77,7'si ve erkeklerin % 60,7'si akıllı telefondan banka uygulamaları kullandıklarını belirtmiştir. Bu dağılım çizelge 26'da gösterilmiştir.

Çizelge 26. Akıllı telefonlarda banka uygulamalar kullanma oran

Akıllı telefonlarda Banka uygulamalar kullananlar.	Cinsiyet				Toplam	
	Kadın		Erkek			
	Sayı	Yüzde	Sa yı	Yüzde	Sayı	Yüzde
Evet	122	% 77,7	51	% 60,7	173	% 69,2
Hayır	35	% 22,3	33	% 39,3	68	% 30,8
Toplam	157	% 100	84	% 100	241	% 100

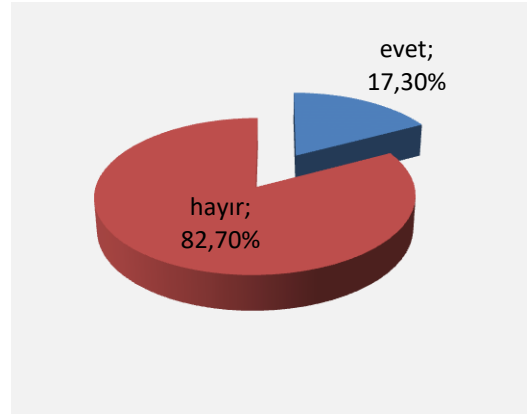


Şekil 35. Akıllı telefonlarda banka uygulamalar kullanma dağılımları

Bu çalışmada katılımcılara banka uygulamalarını kullanırken herhangi bir sorun yaşayıp yaşamadıkları (pinin çalması, mobil internet bankacılığı uygulamasının hacklenmesi, mobil bankacılık uygulamasını kullanarak Banka hesabınızdan para çalmak.) sorulmuştur. Kadınların % 16,6'sı ve erkeklerin % 17,9'u banka uygulamalarını akıllı telefondan kullandıklarında sorunlarla karşılaştıklarını belirtmiştir. Bu dağılım çizelge 27'de gösterilmiştir.

Çizelge 27. Akıllı telefonlarda Banka uygulamalar kullanırken yaşayan sorunlar oranlarının

Akıllı telefonlarda Banka uygulamalar kullanırken sorun yaşanlar	Cinsiyet				Toplam	
	Kadın		Erkek			
	Sayı	Yüzde	Sayı	Yüzde	Sayı	Yüzde
Evet	26	%16,6	15	%17,9	41	%17,3
Hayır	131	%83,4	69	%82,1	200	%82,7
Toplam	157	%100	84	%100	241	%100.0



Şekil 36. Akıllı telefonlarda banka uygulamalar kullanırken yaşanan sorunlar dağılımları

4.1. Değerlendirme

Adana örneklemini için yapılan anket çalışmasında, akıllı telefon kullanıcılarının yukarıda verilen sonuçlarının kısa bir özeti yapılacak olursa 241 katılımcının % 65.1 ni kadınlar, %39.1 ni ise erkekler oluşturmaktadır. Ankete katılan kullanıcılardan yaş gruplarına göre dağılımlarının %79,2 si 0-39 yaş grubunu, %20.8 ise 40 yaş ve üzerini oluşturmaktadır. Bunu anlamı ise telefonu kullanan katılımcıların genç denilebilecek grubu oluşturmaktadır. Yine katılımcıların 169 üniversite öğrencisi ve mezunu 27 si lise mezunu, 45 i ise ortaokul ve ilkokul mezununu oluşturmaktadır. Yaş gruplarına göre dağılım (%79,2) ile okul mezuniyetine göre dağılım (196/241 %81) paralellik göstermektedir. Kullanıcıların büyük çoğunluğu genelde akıllı telefonlarını 132 hem iş hem de kişisel amaç için kullandıklarını belirtmişlerdir.

Kullanıcıların büyük çoğunluğu Android telefon işletim sistemine sahip olduklarını belirtmişlerdir. Yine katılımcıların hemen hemen tümü akıllı telefonlarında internet kullandıklarını belirtmişlerdir. İnternet kullanımının dağılımı ise 175 kişi sosyal medya ve oyun için, 55 kişi ise eğitim amaçlı olduğunu belirtmişlerdir. Akıllı telefonla harcanan zaman ise çarpıcı sonuçlar vermiştir.

Akıllı telefonlarda 5 saatten fazla zaman harcayanların sayısı 20 kişi iken, 186 kişi ise 1-4 saat arası zaman harcadıkları sonucuna ulaşılmıştır. Sosyal medya sıralaması ise Facebook ve WhatsApp oluşturmaktadır.

Sosyal medyada kimlik gizleyenlerin sayısı 27 kiři olmuřtur geri kalan ise kimliklerini gizlememektedirler. Bu ise kullanıcıların doęru yolda olduklarının bir göstergesi olarak kabul edilebilir. Yine sosyal medyada sahte hesap oluřturanların sayısı da %33 civarındadır. Bu ise azımsanmayacak bir yüzdelik dilimidir.

0-39 yař grubundaki katılımcıların 88'i facebooktan rahatsız edildiklerini, 40 > üzeri yař grubunu ise 15 kiři rahatsız edildiklerini belirtmiřlerdir. Buna göre facebooktan rahatsız edilenlerin yüzdesi % 43.6 olmuřtur.

Twitter den rahatsız edilenlerin sayısı ise 54 (%22) ile sınırlıdır. WhatsApp tan rahatsız edilenlerin sayısı ise 81 kiřidir. İnstagram dan rahatsız edilenlerin sayısı dięer sosyal medya uygulamaları içinde en fazla olanıdır. Kullanıcıların %48,2'si rahatsız edildiklerini belirtmiřlerdir.

Buradan řu sonuçlara ulařılabilir. Sosyal medyadan rahatsız edilenlerin sayısı yaklaşık olarak katılımcıların %30 ile %50 sini oluřturmaktadır. Kullanıcılar en çok instagram dan en az ise twitter den rahatsız edilmiřlerdir.

Siber zorbalıęa maruz kalanların sayısı 42 olarak tespit edilmiřtir. Bu az bir sayı olarak görünse de kullanıcılar üzerindeki etkisi çok büyük olmaktadır.

Akıllı telefonların virüsten etkilenme durumları ise epeyce dikkat çekmektedir. Katılımcıların hemen hemen yarısı (%46,9) virüsten akıllı telefonlarının etkilendiklerini belirtmiřlerdir.

İkinci el telefon kullananların sayısı yaklaşık olarak katılımcıların %30 nu yani 1/3 nü oluřturmaktadır. İkinci ele kullananların ise %14 ü sorun yařadıklarını belirtmiřlerdir.

Dolandırıcılık açısından ise katılımcıların 134 ü etkilenmiřtir. Bu sayının fazla olması (%55) telefon dolandırıcılıęının etkili olduęu görölmektedir.

Telefon üzerinden kredi kartıyla alıř veriř yapanların sayısı ise azımsanmayacak kadar fazladır ve % 57 kullanıcı alıřveriř yaptıklarını belirtmiřlerdir. Bu alıř b-veriřte sorula karřılařanların yüzdesi %17,8 olmakla birlikte sahtekârlık açısından son derece önemli bir miktardır.

5. TARTIŞMA

5.1. Elektronik Cihazlarda VPN Kullanımı

Son yıllarda teknoloji alanında çok büyük bir değişim meydana gelmiştir. Bu, insanların internet üzerinden haklarını korumaya devam edebilmesi hakkında gerekli bir soruyu gündeme getirmektedir. Son yirmi yılda, farklı ülkelerin hükümetleri sosyal medyadaki bilgileri kontrol etme ve kısıtlama çabalarını arttırmıştır. Çevrimiçi içeriğin manipülasyonu, genel internet özgürlüğünün azalmasına neden olmuştur. Günümüzde sahte haberler, bilgisayar korsanlığı ve çevrimiçi hırsızlık çok popüler hale gelmiş, siber güvenlik dünyasında gerçek bir tehdit unsuruna dönüşmüştür. Bu nedenlerden dolayı bazı ülkeler VPN (Sanal Özel Ağ) kullanımına yeni kısıtlamalar getirmiştir (38).

Global Web Index tarafından 2017 yılında dünya genelinde VPN kullanımı üzerine yapılan ankete göre, o yıl internet kullanıcılarının %25'inin VPN'yi elektronik cihazlarında, bilgisayarlarda %17, mobil cihazlarda %15 ve tabletlerde %7 kullandığı saptanmıştır. Bu ankette, Endonezya ve Hindistan elektronik cihazlarda en yüksek VPN kullanım oranına sahipken Türkiye üçüncü sırada yer almaktadır. Bu çalışmaya göre, erkeklerin % 62'sinin ve kadınların % 38'inin elektronik cihazlarında VPN kullandığı bildirilmiştir (39).

VPN kullanımı bazı ülkelerde yasal olmakla birlikte, örneğin Çin, İran, Türkiye, UAE ve Rusya gibi ülkelerde yalnızca hükümet onaylı VPN'lere izin verilmektedir, diğerleri yasadışıdır. Irak ve Kuzey Kore gibi ülkeler ise, VPN'nin elektronik cihazlarda kullanımını tamamen yasaklamıştır. Amerika, Avrupa ve diğer ülkelerde VPN kullanımı yasallaştırılmıştır (40).

Türkiye'de, hükümet ve özel kuruluşlar tarafından yasaklan web sitelerinden bilgiye erişmek için elektronik cihazlarda VPN kullanımının anayasaya göre net bir kanun cezası yoktur. Ancak, hükümet ve özel kuruluşlar tarafından yasaklan web sitelerinden müzik,

kitap, film ve pornografi gibi bilgileri, özellikle de çocuk pornografisi vb. indirmek ve yüklemek için VPN kullanımını kanunen cezalandırılabilir (41).

Hükümetler, VPN'in akıllı telefonlar gibi elektronik cihazlarda kullanılmasına genellikle karşı değilken hacking, çevrimiçi hırsızlık, korsanlık gibi VPN'in yasadışı kullanımının engellenmesi mücadelesini vermektedirler (38).

5.2. Sahte Sosyal Medya Hesapları

Twitter, Facebook, Instagram gibi sosyal medya platformları, kayıt olurken kişilerin kimliğini doğrulamaz. Bu yüzden de bazı insanlar ve siber suçlular gerçek kimliklerini çok daha kolay gizleyebilir ve dolandırıcılık, çevrimiçi siber taciz, yanlış haberler ve pornografik materyaller gibi uygunsuz, kötü amaçlı etkinlikleri yürütebilirler (63).

2013-2014 yılları arasında Facebook tarafından yayımlanan yıllık raporda, dünya çapında aylık aktif Facebook kullanıcılarının %5,5- %11,2'sinin sahte hesaplar kullandığı ve bu hesabın tanımlanamayan kimliklere kayıtlı olduğu bildirilmiştir (42).

Bilkent Üniversitesi ve Orta Doğu Teknik Üniversitesi tarafından Instagramda sahte ve otomatik hesap kullanımı tespiti konusunda bir araştırma yayınlandı. Suç işlemek için kullanılan sahte hesapları tespit etmek amacıyla 2013 yılı Instagram hesaplarının incelenmesi sonucu 201 Instagram hesabının sahte ve tanımlanmamış kimliklere sahip olduğu, farklı suçları işlemek için kullanıldığı gözlemlendi (43).

Adana-Türkiye'de akıllı telefon kullanarak işlenen suçlarla ilgili olarak yaptığımız ankete göre, katılımcıların %20'sinin kimliği belirsiz kimliklere sahip sahte sosyal medya hesapları olduğu ve %80 katılımcının da gerçek soyadlarını ve adlarını bu sosyal medya platformlarında kullanmadığı gözlenmiştir.

İnsanlar bu sosyal medya platformlarına kayıt olurken gerçek adlarını ve soyadlarını kullanmak zorunda değiller, çünkü bu sosyal platformlar veya anayasada kişinin bu sosyal medya platformlarında sahte isimler kullanmasına dair bir yasaklama yok. Ancak bir kişi, bir sosyal medya hesabı oluşturmak için başka bir kişinin kimliğini kullanarak bu hesapla aktiviteler yürütürse, bu, dünyanın her ülkesinde suçtur ve yasalar tarafından da açıkça belirtilmiştir. Diğer bir deyişle buna, dünyanın her yerinde ciddi suç olan kimliğe bürünme

denir. Sahte hesabın çevrimiçi siber taciz, siber takip, hackleme, yanlış haber ve erotik videoların paylaşılması gibi kötü amaçlı aktiviteler için kullanılması yasalara aykırıdır ve bu tür faaliyetler hapis cezası ile cezalandırılabilir.

TCK madde 268'ye (44) göre kişinin izni olmadan kimlik bilgilerinin kullanması, kimliğine bürünme ve kişi hakkında yanlış bilgi yayınlamak bir suçtur ve 4 yıla kadar hapis cezası ile cezalandırılabilir.

5.3. Sosyal Medya ve Suç

Facebook, Twitter, Snapchat ve Instagram gibi sosyal medya platformlarının popüleritesi arttıkça suç ve mağduriyet de arttığı belirlenmiştir.

Önceden insanların suçla ilgili fikirlerinin medyada gördüklerine veya okuduklarına göre oluşturdıkları düşünülüyordu. Ancak sosyal medyayı BCC, CNN, TRT World gibi haber kaynaklarına tercih ettiğimiz düşünülürse, bu yeni platformlar suç anlayışımızı nasıl etkiliyor?

Sosyal medya da suçun kendisi ile ilgili yeni endişeler yaratmıştır. Sosyal medya platformları mağduriyeti nadir değildir ve günümüzde insanların karşılaştığı temel sorunlardan biridir (45).

Ancak, bunların hepsi kötü haber değildir. Sosyal medya, diğer şeylerin yanı sıra, polis ve ordu gibi ceza adaleti kurumlarının suçları çözmesi için yeni fırsatlar yaratmıştır. İnsanlar, polis ekiplerinden önce suç mahallinin canlı videolarını çekip yayınlamak için Facebook, Instagram, Twitter gibi akıllı telefon sosyal medya uygulamalarını kullanmaya başlamıştır. Bu deliller de, mahkemede suçu çözmek için kullanılabilirler. Dolayısıyla, iletişim teknolojisindeki diğer birçok gelişme gibi, sosyal medyanın ceza adaleti ve hukukla ilişkisi söz konusu olduğunda iyi, kötü ve çirkin yanları mevcuttur (45).

- **İyi Yanları**

Sosyal medyanın bazı ceza adalet kurumları için yararlı olduğuna şüphe yoktur.

Polis için, sosyal medya onlara eşi görülmemiş bir şekilde halka erişim sağlamıştır ve bunun tersi de geçerlidir. Facebook ve Twitter aracılığıyla, polis ve halk olaylar

hakkında gerçek zamanlı iletişim kurabilirler. Günümüzde polis, ordu ve diğer adalet ajanslarının Facebook ve Twitter gibi sosyal medya hesapları bulunmaktadır. Böylece halk ile doğrudan bağlantı kurabilirler ya da insanlar direkt olarak sosyal medya hesaplarından belli bir suça ait bilgileri ya da videoları gönderebiliyorlar. Bu bilgiler hukuk mahkemesinde de oldukça önemli olabilir (45).

Sosyal medya, polis soruşturmasında da önemli bir araç haline gelmiştir. Örneğin, Melbourne kadını Jill Meagher'in son anlarının görüntülerinin Facebook ve YouTube'dan CCTV yayınlanması, katilini yakalamaya yardımcı olmuştur. Bu kadın, 22 Eylül 2012'nin erken saatlerinde Melbourne, Victoria'nın bir iç banliyösü Brunswick'teki bir bardan eve yürürken tecavüze uğramış ve öldürülmüştü. Youtube'da yayınlanan CCTV'nin görüntüleri, halkın katili tanımamasına ve polise bildirmesine yardımcı olmuştur (45).

Ayrıca, sosyal medya yayını, ceza yargılamalarına fazladan bir şeffaflık katmıştır. İnsanlar artık mahkeme duruşmalarını izlemek ve dinlemek için mahkemelere gitmiyorlar, çünkü Facebook, Twitter vb. sosyal medya yargılamaları sosyal medya hesaplarından veya akıllı telefonlar gibi mobil cihazlardan canlı izleyebiliyorlar.

- Kötü Yanları

Sosyal medya, başta gençler olmak üzere birçok kullanıcı için risk oluşturmakla suçlanmaktadır.

Sosyal medya, siber zorbalık ve pornografik materyallerin gönderilmesi gibi yeni suçları kolaylaştırmak için kullanılmıştır. Bu da daha sert cezaların uygulanmasıyla sonuçlanmıştır (45).

Ayrıca, Suçluların potansiyel mağdurları ve mallarını takip etmek için sosyal medya platformlarını kullanma becerisi gelişmiştir. İnsanlar bulundukları ve ziyaret ettikleri yerleri göstermek için sosyal medya hesaplarını kullanmaktadırlar. Ayrıca günümüzde insanlar ev, saat, para gibi eşyalarının fotoğraflarını sosyal medyada paylaşmaktadırlar. Bu bilgiler yüzünden insanlar veya evleri soyulmaktadır.

Ayrıca taciz ve tehdit gibi eski suçların yanı sıra sahtekârlık ve kimlik hırsızlığı da sosyal medya yoluyla yeni şekillerde yürütülmektedir. Günümüzde suçlular sahte sosyal

hesapları oluşturmakta ve zorlanmadan birinin kimliğini kullanabilmektedir (45). Bu da, bu tür suçların artmasına neden olmaktadır.

Sosyal medya, suç sonrası insan davranışlarının doğasını da değiştirmektedir. Suçluların çevrimiçi olarak arkadaşlarına ve takipçilerine yönelik suç davranışları ile övündükleri performans suçları giderek yaygınlaşmaktadır.

Adana-Türkiye'de akıllı telefon kullanarak işlenen suçlarla ilgili yaptığımız ankette, Facebook kullanan 105 katılımcı, Twitter kullanan 54 katılımcı, Whatsapp kullanan 84 katılımcı, Instagram kullanan 125 katılımcı ve diğer sosyal medya ağlarını (Snapchat vb.) kullanan 21 katılımcı olduğu saptanmıştır. Bu katılımcılar, sahtekârlık, şantaj, virüs bağlantı mesajlar ve reklamlar yoluyla sahte sosyal medya hesapları kullanılarak kullanıcılar mağdur edilmişlerdir. Bu araştırma aynı zamanda 42 katılımcının kullandıkları sosyal medya ağlarında siber zorbalığa uğradığını da ortaya koymuştur. Bu araştırmaya göre, Instagram ve Facebook kullanıcılarının mağduriyetinin çok daha yüksek olduğu görülmüştür. Çünkü bunlar dünyada en çok kullanılan sosyal medya uygulamalarıdır.

- Olumsuz Yanları

Sosyal medya nedeniyle yargılama, ceza adalet sisteminde çalışanlar için giderek daha fazla endişe kaynağı haline gelmiştir, çünkü teknoloji hızla gelişip karmaşıklaşırken bu alanda çalışacak uzman sayısı azdır.

Facebook ve Twitter'daki faaliyetler, iddianameden önce sanıkların fotoğraflarının paylaşılması, nefret gruplarının oluşturulması gibi uygulamalar yoluyla kovuşturmalara ve adil yargılanma hakkına tehdit oluşturabilir. Yargılanan bir suçla ilgili fotoğraf ve bilgi paylaşmak, mahkeme tarafından cezalandırılabilir. Yukarıda tartışılan Meagher davasında, Avustralya'daki Victoria Polisi, Facebook sayfasını, halkı bu tür ihlallerin sonuçları konusunda eğitmek için kullandı (45).

Sosyal medya, Paris'teki Kardashian soygunundan sonra olduğu gibi kurbanı suçlamak için bir araç olarak da kullanılabilir. Olayın hemen ardından, bazı Facebook ve Twitter kullanıcıları Kardasian'ların “hak ettiği şeyi” aldığını ve “belki şimdi kendini toparlayacağını” iddia etmiştir (45). Sosyal medya, suç mağdurlarının arkadaşlarının ve ailelerinin ikincil mağduriyete maruz kaldıkları bir araç olarak da kullanılabilir.

- Gelecek

Platformlar geliştikçe ve yeni meseleler ortaya çıktıkça sosyal medya, ceza adaleti yetkilileri için zorluklar ve fırsatlar sunmaya devam edecek, ayrıca halkın suç ve mağduriyet konularını algılama ve bunlara katılma şeklini değiştirmeye devam edecektir (45). Ancak, yasak çağrıları ve sosyal medyaya getirilen kısıtlamaların sonuç vermesi olası değildir.

Görünen o ki, sosyal medya, hayatımızda sürekli bir ihtiyaç olacaktır. Bu fenomeni anlamak, faydalarından yararlanmak, suç ve ceza adalet sistemi ile ilgili olumsuz etkilerini önlemek veya en aza indirmek istiyorsak, bakış açımızı genişletmemiz gerekmektedir.

5.4. Akıllı Telefonlarda Kötü Amaçlı Yazılımlar

Mobil Kötü Amaçlı Yazılımlar Akıllı Telefonunuza Nasıl Girebilir?

Akıllı telefonların hızla büyüyen satışları, neredeyse sürekli çevrimiçi varlıklarıyla birlikte, bu cihazları mobil kötü amaçlı yazılımların yeni hedefleri haline getiriyor (46). Akıllı telefonların, bir bağlantı mesajı şeklinde gönderilen virüslere karşı savunmasız kalmasını sağlayan bir Bluetooth bağlantıları ve veri özellikleri vardır. Bu virüsler öncelikle üç şekilde yayılır:

- İnternette indirmeler

Virüs, geleneksel bir bilgisayar virüsüyle aynı şekilde yayılır. Kullanıcı, virüslü bir dosyayı bir PC veya telefonun kendi internet bağlantısı yoluyla telefona indirir. Bu, dosya paylaşım indirmelerini, eklenti sitelerinden (zil sesleri veya oyunlar gibi) elde edilebilen uygulamaları ve Symbian Web sitesinde yayınlanan yanlış güvenlik yamalarını içerebilir (48).

- Bluetooth kablosuz bağlantısı

Virüs, Bluetooth bağlantıları aracılığıyla telefonlar arasında yayılır. Telefon keşfedilebilir modadayken kullanıcı Bluetooth üzerinden bir virüs alır, bu da diğer Bluetooth özellikli telefonlar tarafından görülebileceği anlamına gelir (47).

- Mltimedya mesaj servisi

Virs, MMS metin mesajının bir ekidir. E-posta eki olarak gelen bilgisayar virslerinde olduėu gibi, virsn telefona bulařabilmesi iin kullanıcının eki aıp yklemesi gerekir. Genellikle, MMS yoluyla yayılan virs, telefonun kiři listesine girer ve orada mevcut her telefon numarasına kendisini gnderir (47).

Telefon kt amalı yazılımları, akıllı telefonlar gibi insanların akıllı telefonlar gibi mobil cihazlarının performansını olumsuz etkilemekle kalmaz, aynı zamanda banka gibi iřletmeleri ve dolayısıyla ekonomiyi de etkileyen kresel bir sorundur. Teknolojideki ilerlemeden dolayı, evrimii para iřlemleri ve mobil bankacılık uygulamalarının varlıėı, banka hesap numaraları ve řifreler gibi bankacılık bilgilerini alan telefon yazılımlarının bilgisayar korsanlarının ve su etelerinin dikkatini ekmesine neden oldu. Fidyeye almak amalı kullanılan kt amalı yazılımlar nedeniyle oėunluėu nl olan insanlar ve byk řirketler hackerler tarafından maėdur edilmiřtir (48). nk fotoėraf ve videolar gibi kiřisel bilgilerinin alınması sonrası byk miktarda para talepleriyle ya da bu bilgiyi yayınlama tehdidi ile řantaja maruz kalmıřlardır.

Malwarebyte laboratuvarlarına gre, 2020 řubat ayında dnyadaki kt amalı yazılımların durumu hakkında yayınlanan yıllık rapor, insanların %73'nn mobil cihazlarında bankalar iin kt amalı yazılımlar bulunduėunu ortaya koymuřtur. Bu raporda ayrıca, Amerika (%72) ve İngiltere gibi geliřmiř lkelerde, kt amalı yazılım saldırılarının en yksek yzdelere sahip olduėu tespit edilmiřtir (48).

Adana-Trkiye'de akıllı telefonlarla iřlenen sularla ilgili olarak yaptığımız anket, 113 katılımcının akıllı telefonunun baėlantı mesajı biimindeki kt amalı yazılımlardan olumsuz etkilendiėini ortaya koymuřtur. Arařtırmamıza gre, 88 Android ve 25 İOS akıllı telefonlar, en ok etkilenenler olmuřtur. Bu da, Android akıllı telefonlarının, farklı iřletim sistemlerine sahip diėer akıllı telefonlara kıyasla mobil kt amalı yazılım saldırılarına karřı daha savunmasız olduėunu ortaya koymaktadır.

Baėlantı kt amalı yazılım mesajlarının MMS biiminde, insanların mobil cihazlarına zarar vermek amacıyla yayılması bir sutur, nk birisinin mlknn tahrip edilmesi her lkede yasalarca cezalandırılabilir.

5.5. Akıllı Telefon Hırsızlığı

Akıllı telefon hırsızlığı, taşınabilirliği nedeniyle kalıcı ve yaygın bir sorundur. Suçlular akıllı telefonları kalabalık sokaklardan, restoranların içinde, hatta metrolarda bile kolayca çalabilmektedir. Bu çalıntı telefonlar daha sonra ikinci el telefon satan elektronik mağazalar gibi web sitelerinde satılmaktadır. Graham Farrell çalışmaya göre; Telefon hırsızlığını ve soygununu önleme: hükümetin harekete geçme ihtiyacı ve uluslararası koordinasyon, büyük şehirlerde meydana gelen soygunların %30 ila %40'ının cep telefonu hırsızlığını da içerdiğini öne sürmektedir (69).

Adalet Yardımı Bürosu tarafından yayınlanan raporlara göre, ABD Adalet Bakanlıkları, kalabalık eyaletlerin daha fazla mobil hırsızlık vakasına barındırmaktadır. İngiltere ve Hindistan gibi birçok ülkede hükümetler, telefonun sahibi polise rapor verdikten sonra çalıntı telefonları takip eden bir veri tabanı oluşturarak cep telefonu hırsızlığını azaltmaya çalışmış ve polis departmanı çalınan telefonu IMEI numarasını kullanarak kara listeye almıştır. Böylece cep telefonu GPS kullanarak konumunu izleyebilmektedir. Ama günümüzde çoğu insan, telefonu çalındıktan sonra telefonun seri numarasını kullanarak telefonu almaya karar vermekte ve böylece kullanmak isteyenleri engellemektedir. Bu, son yıllarda cep telefonu hırsızlığının nedeninin düştüğünü açıklamaktadır, çünkü herhangi bir telefonun izlenmesini kolaylaştıran GPS sistemi ve seri numaraları vardır. Yine de bu durum, cep telefonu hırsızlığı davalarıyla ilgili davaların çözüldüğü anlamına gelmemektedir (13).

Adana-Türkiye'de akıllı telefon kullanarak işlenen suçlarla ilgili yaptığımız ankette, 28 katılımcının akıllı telefonunun çalındığını ve 8 katılımcının akıllı telefondan kişisel bilgilerinin soyguncular tarafından kullanıldığı saptanmıştır.

5.6. Akıllı Telefon Dolandırıcılığı ve Sahtekârlık

Akıllı telefonlar, hayatımızın büyük bir parçası haline gelmiş ve son yıllarda hızla gelişerek çok çeşitli işlevler sunan cihazlar haline getirilmiştir. Ancak, maalesef dolandırıcılar da bu yeni teknolojiyi sevmiş, sunduğu fırsatlardan yararlanmaya çalışmaya başlamışlardır. Bu dolandırıcılıkların çoğu internet üzerinden, dolayısıyla da mağdurun

kimliği fark etmeksizin gerçekleşir. Dolandırıcılık ve sahtekârlık davalarının polis tarafından araştırılması genellikle çok zordur çünkü çoğu insanı (hem mağdurlar hem de şüpheliler) içerir. Araştırmak için çok fazla kaynak mevcuttur ve sahtekârlık ile keskin uygulama arasında var olan tarafsız bölge nedeniyle mahkemeler gerçek suçluyu bulup ceza vermekte zorlanabilir (50).

Dolandırıcılık, her yaştan ve her gelir düzeyinden insanları hedef alırlar, yani ayrımcılık yapılmaz. Kısa mesaj dolandırıcılıkları, sahte piyangolar, yatırım sahtekârlıkları ve romantizm dolandırıcılıkları, siber güvenliğin günümüzde karşılaştığı temel sorunlardan biridir. Bu tür dolandırıcılıkta her zaman yeni bir tür sahtekârlıkla karşılaşılabilir.

2012 yılında Metropoliten Polis Servisi (İngiltere) tarafından yayınlanan rapora göre, İngiliz halkı her yıl çevrimiçi, posta yoluyla, kapıdan kapıya veya telefon dolandırıcılığıyla defalarca kandırılmış, milyarlarca İngiliz sterlini harcanmıştır. İngiltere'de ve yurtdışındaki birçok insan sürpriz bir kazanım heyecanı ile çekilişlere katılmakta, sahte ödülleri kazanabilmek için büyük miktarlarda para kaybetmektedirler. Özellikle çoğunluğu yaşlı ve savunmasız olan çok sayıda kurban mail aracılığıyla Kitle Pazarı dolandırıcılığına yakalanmışlardır (51).

Teknoloji ilerledikçe dolandırıcılık faaliyetleri insanlar arasında daha popüler hale gelmiştir. Günümüzde akıllı telefonlar, bilgisayarlarda kullanılan ucuz ve sahte elektronik birçok web sitesi bulunmaktadır. Akıllı telefonlar aslında mini bilgisayarlar gibidir, bu nedenle birçok dolandırıcı ve sahtekâr bilgisayar kullanmaz. ECC-Net tarafından sahtekârlık hakkında yayınlanan rapora göre, dolandırıcılar, web siteleri oluşturmak, kısa mesaj gönderme gibi kötü amaçlı etkinliklerini gerçekleştirmek için akıllı telefonlar kullanırlar. Avrupa genelinde 2017 yılında sınır ötesi e-ticarete, siber dolandırıcılığın, Eylem Sahtekârlığı ajansına bildirilen tüm suçların % 41'ini temsil ettiği ve ortalama bireysel kaybın £ 3689 olduğu belirtilmiştir (52).

FBI'nın İnternet Suç Raporu'na göre, İnternet Suç Şikâyet Merkezi 2017 yılı içerisinde yaklaşık 300.000 şikâyet almıştır ve mağdurlar, çevrimiçi dolandırıcılıkta 1,4 milyar doların üzerinde para kaybetmiştir. Stratejik ve Uluslararası Araştırmalar Merkezi (CSIS) ve McAfee tarafından yürütülen bir araştırmaya göre, siber suçlar küresel ekonomiye 600 milyar dolara mal olmakta ve bu da toplam küresel GSYİH'nın % 0,8'ine

dönüşmektedir (53). Çevrimiçi dolandırıcılık birçok şekilde ortaya çıkar. E-posta spam'ından çevrimiçi aldatmacalara kadar değişebilmektedir. İnternet sahtekârlığı, çoğunlukla veya tamamen internet kullanımına dayalı olsa bile meydana gelebilir.

Türkiye'de dolandırıcılık, sahtekârlık ve sahte web sitelerini kullanarak ucuz sahte elektronik ürünleri satmak, metin dolandırıcılığı mesajları göndermek gibi günlük olarak polis, ordu gibi adalet kurumlarının karşılaştığı temel sorunlardır. Türkiye'deki polis teşkilatı genellikle dolandırıcılık ve hilekârlıklarla ilgili uyarı metinleri göndererek sahtekârlık ve dolandırıcılık konusunda halkı uyarır ve ayrıca polis her zaman halka bu tür kötü niyetli faaliyetlere karışan kişilerin ihbar edilmesini söyler. 2018'de Türkiye'nin popüler gazetelerinden Milliyet, cezaların yetersiz olduğunu ve teknolojinin hızlı bir şekilde gelişmesinin dolandırıcıların sayısını artırdığını bildirmiştir. 2017 yılı gözaltı evleri raporuna göre, Türkiye'de yedi binden fazla kişi hapsedilmiş ve sahtekârlıktan hüküm giymiştir (54).

Adana-Türkiye'de akıllı telefon kullanarak işlenen suçlarla ilgili yaptığımız ankette, katılımcıların dolandırıcılar veya sahtekârlar tarafından arandıklarını ve onlara para, altın, banka hesap bilgileri ve diğer kişisel bilgileri sorarak mesajlaştıklarını ortaya çıkmıştır. Dolandırıcılar tarafından, 57 katılımcıya para, 23 katılımcıya altın, 28 katılımcıya banka bilgileri ve 26 kullandıkları elektronik cihaz gibi sorular yöneltilmiştir. Aynı araştırmadan 86 katılımcının da, kredi kartı bilgileri veya sosyal güvenlik numarası (T.C) gibi kişisel bilgilere erişmek için akıllı telefonlarının hacklenmesi gibi elektronik dolandırıcılıkla karşılaştığı ortaya konmuştur.

Utanç, dolandırıcılık ve sahtekârlık yaşandığında hissedilen yaygın tepkilerden biri olabilse de, aslında bu şekilde hissetmeye gerek yoktur. Çünkü en dikkatli insanlar bile dolandırıcılık mağduru olabilirler ve bazen de dolandırıcılara bir suç işlemek için ev adresi, e-posta veya telefon numarası gibi en küçük bilgiler bile yetebilmektedir. Bazı insanlar sahtekârlığa kurban olduktan sonra kendilerini suçlamaktadırlar, ancak unutulmamalıdır ki bu suçtan sadece suçlu sorumludur.

5.7. Uluslararası Mobil Ekipman Kimliği

Uluslararası Mobil Cihaz Kimliği (IMEI), 3GPP ve iDEN cep telefonlarının yanı sıra bazı uydu telefonlarını tanımlamak için benzersiz bir sayıdır. Genellikle telefonun pil bölmesinde veya telefonun arkasına yazdırılır ve Iphone gibi bazı telefonlarda basılı olarak bulunur. Ayrıca tuş takımında *#06# tuşlanarak veya akıllı telefon işletim sistemlerindeki ayarlar menüsünde diğer sistem bilgilerine ek olarak çoğu telefonun ekranında görüntülenebilir (63).

GSM şebekeleri, cihazların geçerli veya sahte olup olmadığını tanımlamak için IMEI numarasını kullanır ve ayrıca çalınan bir telefonun şebekeye erişimini durdurmak için de kullanılabilir. Örneğin, akıllı telefon gibi bir cihaz çalınırsa, telefonu kara listeye almak için cihaz sahibinin şebeke sağlayıcısının IMEI numarasını kullanmasını sağlayabilir. Hırsız telefonun SIM (Abone Kimlik Modülü) kartını değiştirse bile bu, telefonun kendinde mevcut veya diğer ağlardaki internete erişemeyeceği anlamına gelir (64).

SIM kart yuvası olmayan cihazlarda genellikle IMEI kodu yoktur. Ancak, IMEI yalnızca cihazı tanımlar ve abone ile belirli bir ilişkisi yoktur. Telefon, teorik olarak herhangi bir el cihazına aktarılabilen bir SIM kartta sakladığı Uluslararası Mobil Abone Kimliği (IMSI) numarasını ileterek aboneyi tanımlar. Ancak, ağın bir abonenin gündemini bilme yeteneği, bireysel cihazın birçok ağ ve güvenlik özelliğini sağlar (65).

❖ IMEI ve Yasa

Çoğu ülke, günümüzde ciddi bir sorun haline gelen cep telefonu hırsızlığı sorununu önlemek için IMEI kullanımını kabul etmiştir. Örneğin, Birleşik Krallıkta, Cep Telefonları Yasası (Yeniden Programlama) uyarınca, bir telefonun IMEI' sini değiştirmek veya değiştirebilecek donanıma sahip olmak, bazı durumlarda bir suç olarak kabul edilmektedir (66).

Türk hukuk sistemine göre, ithal edilen tüm cep telefonları için Türkiye'ye IMEI telefon numaralarının kaydedilmesi gerekmektedir. Bu sosyal düzenleme, cep telefonlarının güvenliğini sağlamayı amaçlamaktadır. Aslında, cep telefonlarının cep telefonlarının Mobil Cihaz Kayıt Sistemi'ne (MERS) kaydedilmesi Türkiye içinde telekomünikasyon hizmeti alabilmesi için yasal bir zorunluluktur. Sonuç olarak, bu nedenle kayıt dışı cep telefonları

ne kaybolmasına ne de çalınmasına rağmen işe yaramaz olma riski taşır. Ancak, bugünlerde ithal edilen cep telefonlarının bir kısmının IMEI numaralarının kaydı, telefon teknisyenleri tarafından yasadışı olarak kaydedilmektedir. Örneğin, Adana'da Çakmak Plaza isimli iş merkezinde, telefon teknisyenleri ithal edilen bir telefonu daha az ücret karşılığında yasadışı yoldan kaydedebilmektedirler. Başka bir telefona kaydolmak için birinin telefon IMEI numarasını kullanmak, Türkiye'de kanunen yasaktır ve cezalandırılır (67).

Adana-Türkiye'de akıllı telefon kullanarak işlenen suçlarla ilgili yaptığımız anket çalışmasında, katılımcıların 36'sının akıllı telefonlarını başka bir IMEI numarası kullanmak suretiyle yasadışı olarak kaydettiğini ve 12 katılımcının da mahkeme tarafından IMEI numaralarının yasadışı kullanımı nedeniyle cezalandırıldığını tespit ettik.

❖ Kolluk ve İstihbarat Kullanımı

Kolluk kuvvetleri ve istihbarat servisleri, birkaç metre hassasiyetle bir cep telefonu bulabilen izleme cihazları için bir IMEI numarasını kullanabilmektedirler. Suudi Arabistan hükümet kurumlarının, diğer ülkelerdeki Suudi Arabistan ataerkil toplumundan kaçan kadınları bulmak ve gözaltına almak için cep telefonu ambalajından alınan IMEI numaralarını kullandıkları bildirilmiştir (68).

6. SONUÇLAR VE ÖNERİLER

6.1. Sonuçlar

Akıllı telefonlarla işlenen suçlarla ilgili Adana-Türkiye’de yaptığımız ankete 241 kişi katıldı. 157 katılımcı kadın, 84 katılımcı erkekti. 169 katılımcı üniversite mezunu (123 kadın ve 46 erkek), 27 katılımcı lise mezunu (13 kadın ve 14 erkek), 41 katılımcı ortaokul mezunu (18 kadın ve 23 erkek) idi. Kadınların erkeklerden daha eğitilmiş olduğu görülmüştür.

Tüm katılımcıların akıllı telefon kullanımı mevcut idi. 65 katılımcı Iphone, 104 katılımcı Samsung, 11 katılımcı HTC, 14 katılımcı LG ve 47 katılımcı da başka türlerde akıllı telefon kullanmakta idi. Telefonların işletim sistemleri arasında diğer işletim sistemlerine kıyasla daha fazla kişinin Android telefon (178 katılımcı) kullandığı görüldü.

132 katılımcı akıllı telefonlarını hem kişisel kullanım hem de iş amaçlı, 108 katılımcı kişisel kullanım için ve bir katılımcı da iş için kullanmaktaydı. Daha fazla sayıda insanın telefonlarını hem iş hem de kişisel kullanım için kullandığı görülmüştür.

239 katılımcının akıllı telefonlarında internet kullandığı ve 2 katılımcının kullanmadığı görüldü. 175 katılımcının interneti çoğunlukla sosyal medya ve oyunlar için, 55 katılımcının eğitim amaçlı ve 14 katılımcının iş amaçlı kullandığı saptandı. Katılımcıların çoğunun sosyal medya ve oyunlar için interneti kullandığı görülmüştür.

En çok kullanılan akıllı telefon uygulamaları ve sosyal medya uygulamaları örneğin Instagram, Facebook, Whatsapp, Youtube ve Google gibi gruplandırıldı. 76 katılımcının akıllı telefonlarından daha çok Facebook, 51 katılımcının daha çok Instagram, 57 katılımcının daha çok Whatsapp kullandığı; 11 katılımcının akıllı telefonlarında daha çok Youtube, 46 katılımcının diğerlerinin yanı sıra Google Chrome gibi telefon uygulamalarını da kullandığı saptandı. Facebook ve Whatsapp'ın diğer uygulamalardan daha fazla kullandığı görülmüştür.

89 katılımcının (53 (%33,8) kadın katılımcı ve 36 (%42,9) erkek katılımcı), hükümetler ve özel kuruluş tarafından engellenen web sitelerine akıllı telefonlarında erişmek için VPN kullandığı, engellenen web sitelerine erkek katılımcıların kadın katılımcılardan daha fazla eriştiği gözlenmiştir.

27 katılımcının (16 (%10,2) kadın katılımcı ve 11 (%13,1) erkek katılımcı), sosyal medya ve akıllı telefon uygulamalarını oluştururken gerçek adlarını ve soyadlarını kullanmadığı görüldü. Tüm katılımcılar değerlendirilirse, bu oranın %11,1 olduğu ve erkeklerin sosyal medyada kadınlardan daha fazla sahte isim kullandığı görülmüştür.

96 katılımcının (63 (%40,1) kadın katılımcı ve 33 (%39,3) erkek katılımcı), birinin tavsiyesi üzerine sosyal medya uygulamalarını kullandığı, tüm katılımcılar değerlendirilirse, bu oranın %39,8 olduğu görülmüştür.

111 katılımcının (65 (%41,1) kadın katılımcı ve 46 (% 54,8) erkek katılımcı), bu sosyal medya uygulamalarını ve akıllı telefon uygulamalarını indirirken şartları okumadığı, tüm sonuçlar değerlendirilirse, bu oranın %53,9 olduğu ve ayrıca daha fazla kadın katılımcının, diğer katılımcılara kıyasla kullanım şartlarını daha fazla okuduğu görülmüştür.

80 katılımcının (52 (%33,1) kadın katılımcı ve 28 (%33,3) erkek katılımcı), sahte sosyal medya hesapları oluşturduğu, tüm katılımcıların sonuçları değerlendirilirse, bu oranın %33,2 olduğu görülmektedir.

105 katılımcının (70 (%44,6) kadın katılımcı ve 35 (%41,7) erkek katılımcı) sahte Facebook hesabı kullanan biri tarafından taciz edildiği ve rahatsız edildiği, kadınların erkeklere göre daha fazla kadın tacize maruz kaldığı ve rahatsız edildiği görülmektedir.

54 katılımcının (37 (%23,6) kadın katılımcı ve 17 (%20,2) katılımcı), sahte Twitter hesabı kullanan biri tarafından taciz edildiği görüldü. Sahte Twitter hesaplarını kullanan kişiler tarafından kadınların erkeklere kıyasla daha fazla rahatsız edildiği görülmektedir.

81 katılımcının (53 (%33,8) kadın katılımcı ve 28 (%33,3) erkek katılımcı) sahte bir Whatsapp hesabı kullanan biri tarafından taciz edildiği görüldü. Sahte Whatsapp hesaplarını kullanan kişiler tarafından kadınların erkeklere kıyasla daha fazla rahatsız edildiği görülmektedir.

125 katılımcı, 94 (% 59,9) kadın katılımcı ve 31 (% 36,9) erkek katılımcı sahte bir Instagram hesabı kullanan biri tarafından rahatsız edildi ve taciz edildi. Sahte Instagram hesaplarını kullanan kişiler tarafından Instagramda daha fazla kadınlar rahatsız edildiğini ve daha fazla rahatsız edildiğini gözlemektedir.

21 katılımcının (12 (%7,6) kadın katılımcı ve 9 (%10,7) erkek katılımcı) Snapchat, Tumblr gibi diğer sahte sosyal medya hesaplarını kullanan biri tarafından rahatsız ve taciz edildiği gözlenmektedir.

42 katılımcının (28 (%17,8) kadın katılımcı ve 14 (%16,7) erkek katılımcı) kullandıkları sosyal medya platformlarında siber zorbalık ve siber tacizlere maruz kaldığı, sosyal medya platformlarında kadınların erkeklere göre daha fazla siber zorbalığa maruz kaldığı görülmüştür.

23 katılımcının (14 (%8,9) kadın katılımcı ve 9 (%10,9) erkek katılımcı), katılımcının yerini gösteren akıllı telefon uygulaması kullanan biri tarafından takip edildiği, sonuçlardan daha fazla erkek katılımcının takip edildiği gözlenmiştir.

113 katılımcının (70 (%44,6) kadın katılımcı ve 43 (%51,2) erkek katılımcı) akıllı telefonlarının bağlantı mesaj şeklinde sosyal sosyal medya platformlarında paylaşılan virüslerin performansından olumsuz etkilendiği saptandı. Akıllı telefonların çalışmasına göre, 88 Android telefon ve 25 İOS telefonun, bağlantı mesajları şeklinde sosyal medya platformlarında paylaşılan virüsten olumsuz etkilendiği, sosyal medya platformlarında paylaşılan mesajlar şeklinde paylaşılan virüsler tarafından daha fazla Android akıllı telefonun saldırıya uğradığı gözlemlendi.

85 katılımcının (35 (%41,7) erkek katılımcı ve 50 (%31,8) kadın katılımcı) ikinci el akıllı telefon kullandığı, fakat 11 (%7) kadın katılımcı ve 18 (%21,4) erkek katılımcının ikinci el akıllı telefon kullanırken yasal sorunlarla karşılaştığı saptanmıştır.

39 katılımcının (19 (%12,1) kadın katılımcı ve 20 (%23,8) erkek katılımcı), akıllı telefonlarını başkasının akıllı telefon IMEI numarasını kullanarak kayıt yaptırdığı, ancak 7 (%4,2) kadın katılımcı ve 5 (%6) erkek katılımcının akıllı telefonlarını başka bir IMEI numarası ile kayıt yaptırması nedeni sonra yasal sorunlarla karşılaştığı görülmüştür.

28 katılımcının (18 (%11,5) kadın katılımcı ve 10 (%12) erkek katılımcı) akıllı telefonlarının çalındığı görülmüştür. Akıllı telefonlardaki kişisel bilgilerin, akıllı telefonlarını çalan hırsızlar tarafından kullanıldığı tespit edilmiştir.

134 katılımcının, para, banka hesap bilgileri, altın vb. isteyen dolandırıcılar ile mesajlaştığı ve/veya konuştuğu, 57 katılımcıdan para, 23 katılımcıdan altın, 28 katılımcıdan banka hesap bilgileri ve 26 katılımcıdan bilgisayar, telefon vb. istenmiştir.

86 katılımcı (55 (%35) kadın katılımcı ve 31 (%36,9) erkek katılımcı), e-dolandırıcılıkla (e-mail gibi gönderilen linkler ile kişisel bilgilerin çalınması) karşılaştığını belirtmiştir.

139 katılımcının (95 (%60,5) kadın katılımcı ve 44 (%52,4) erkek katılımcı) akıllı telefonlarını kullanarak internette alışveriş yapmak için kredi kartını kullandığı, 25 (%15,9) kadın katılımcı ve 18 %21,4 erkek katılımcının internet alışverişi yaparken sahte ürünler satın almak gibi sorunlarla karşılaştığı saptanmıştır.

173 katılımcının (122 (%77,7) kadın katılımcı ve 51 (%60,7) erkek katılımcı) akıllı telefonlarında İŞ Cep gibi mobil bankacılık uygulamalarını kullandığı, ancak 26 (%16,6) kadın katılımcı ve 15 (%17,9) erkek katılımcının bankacılık uygulamalarını kullanırken hesaplarının hacklenmesi ve mobil PIN numaralarının çalınması vb sorunlar gibi karşılaştığı görüldü.

Yukarıdaki sonuçlardan, akıllı telefonların insanların yaşamları üzerinde nispeten olumsuz bir etkisi olduğu ve yine bazı insanların suç işlemek için akıllı telefonları kullandıkları gözlenmiştir.

6.2. Öneriler

İnsanlar, endişelenmeleri gereken tek siber suç biçiminin, bilgisayar korsanlarının finansal bilgilerini çalmak olduğunu düşünebilirler. Ancak bu o kadar basit olmayabilir. Temel finansal endişelerden çok daha fazla endişe mevcuttur (55).

Siber suçlar gelişmeye devam etmekte ve bu da her yıl yeni tehditler ortaya çıkarmaktadır. Belki bazı kullanıcılar siber suçların çeşitliliğini öğrendiğinde, akıllı telefonu kullanmayı bırakabilir. Fakat çözüm olarak, kullanıcıların, verilerini korumaya

yardımcı olmanın ilk adımı olarak, siber suçların ne olduğunu ve nasıl başa çıkabileceğini öğrenmesi iyi bir fikirdir. Bazı temel önlemleri almak ve çevrimiçi suç işlemlerinde başkalarını gördüğünüzde kiminle iletişime geçeceğinizi bilmek de önemli adımlardır.

Siber suç nedir? Sorusunun cevabı için Kullanıcılar Siber suç, güvenlik ihlallerinden kimlik hırsızlığı konusunda eğitilebilirler.

Ülkeler, Bilişim Suçları ile ilgili yasal düzenlemeler yaparken; mobil telefonlar, bilgisayarlar, kablolu ya da kablosuz ağdan işlenen suçlar vs. gibi durumlar dikkate alınarak dijital ortamda işlenen suçların niteliğine göre yasalar çıkarılmalıdır.

Üniversite, lise ve ortaokul gibi kurumların siber suçlar konusunda duyarlı hale getirmeleri için eğitim-öğretim programlarına eklenmesi önemlidir.

Bilişim suçları ile ilgili temel bilgiler konusunda halkın bilinçlendirilmesi gerekmektedir.

Bir bilişim suçundan, kimlik hırsızlığından ve/veya ticari bir dolandırıcılıktan şüphelenildiğinde, vakit geçirilmeden hukuki işlem başlatılmalıdır (55, 56).

Birçok kişinin gerçek kimliklerini kullanmadığı gerekçesi ile gelecekte mümkünse Twitter, LinkedIn, Facebook gibi sosyal medya kurumlarında, hesaplar oluşturulmadan önce, kullanıcıların kimlikleri yetkililer tarafından sorgulamalı ve doğrulanmalıdır.

Evlerde/İşyerlerinde Wi-Fi (kablosuz) ağlar, düzgün bir şekilde güvenli hale getirilmediklerinde izinsiz girişlere karşı savunmasızdır. Mevcut ayarlar gözden geçirilmeli ve güvenlik önlemleri artırılmalıdır.

Bilgisayarlar ve diğer elektronik sayısal cihazlar, bakım veya yazılım kurulumu konusunda yardıma ihtiyaç duyulduğunda, servis sağlayıcısına veya sertifikalı bir telefon servisine danışılması güvenlik açısından önemlidir. Alışverişler, güvenli sitelerden yapılmalı, hiç kimseye kimlik ve banka bilgileri paylaşılmamalı, banka ile ilgili gereken işlemler bireyler tarafından ilgili bankası ile yüz yüze görüşülerek gerçekleştirilmelidir (57).

Halka açık Wi-Fi alanlarında, diğer bir deyişle risk oluşturabilecek alanlarda cihazlar korunmasız olabildiği için dikkatli olunması gerekmektedir (58). İşletmeler, günlük işlerini yürütmek için mobil teknolojiyi daha fazla kullanmakta ve giderek güvenmektedirler. Ancak mobil cihazlar ve işletmelerin sistemleri zayıf bağlantısı olabilir.

Şunlardan emin olunmalıdır: şifre korumasını açılmalı, mobil uygulamalar ve işletim sistemleri mobil cihazlar için güncel tutulmalı ve bilinmeyen kablosuz erişim noktalarını kullanmamalıdır (56).

Sosyal medya uygulamaları ve özellikleri hakkında bilgi sahip olunmalı ve bilinçli kullanılmalıdır. Akıllı telefon, tablet vb. gibi mobil cihazların virüs ve diğer zararlı yazılımlara karşı güvence altına alınabilmesi için bilinen ve yaygın olan uygulamalar kullanılmalı ve güvenilir sitelerden akıllı telefonlara yüklenmelidir (59, 60).

Güçlü parolalar kullanılmalı. Farklı hesaplar için farklı kullanıcı kimliği/şifre kombinasyonları (rakam, harf, noktalama işaretleri vs.) kullanılmalı ve bunlar dijital ortama kaydedilmemelidir. Harfler, sayılar, özel karakterler (toplamda en az 10 karakter) birleştirilerek şifreler daha karmaşık hale getirilmeli ve düzenli aralıklarla değiştirilmelidir (61).

KAYNAKLAR

1. **Habermas J.** (1962 trans 1989) The Structural Transformation of the Public Sphere: An Inquiry into a category of Bourgeois Society, Eriřim: <https://v3.arkitera.com/h21487-kamusal-alan-nedir-kamusal-mekan-nedir.html>. Eriřim Tarihi 11.12.2019.
2. **Çalışkan O.** Kamusal Alan Bağlamında Ağ Toplumu ve Yeni Kamusal Alan Arayışı. Maltepe Üniversitesi, **2014**.
3. **Ağ toplumu kavram nedir?** Eriřim: <https://tarihibilgi.org/manuel-castells-kimdir-ag-toplumu-kavrami-nedir/>. **2009** Eriřim Tarihi 22.12.2019.
4. **Binark M.**, Yeni Medya Çalışmaları. Dipnot Yayınları / Ankara, **2007**; 1.
5. **Mittal S, Mattela V.** A Survey of Techniques for Improving Efficiency of Mobile Web Browsing. Concurrency Computat, **2016**:1–42.
6. **Reisinger D.** Worldwide smartphone user base hits 1 billion. Eriřim: (<https://www.cnet.com/news/worldwide-smartphone-user-base-hits-1-billion>). 2012. Eriřim Tarihi: 11.12.2019.
7. **Sahay S ve Kumar MJ.** Junctionless field-effect transistors: design, modeling, and simulation. John Wiley & Sons, **2019**; 4(1);222-234.
8. **Asif, S.** 5g mobile communications: Concepts and technologies. CRC Press; **2018**; 128–134.
9. **Aghatise J.** Cyber crime definition, Eriřim: (<https://www.researchgate.net/publication>) **2014**. Eriřim Tarihi 09.12.2019
10. **Rather, MK ve RAther SA.** Impact of Smartphones on Young Generation. Library Philosophy and Practice. **2019**; 1:1-9.
11. **Bishop M.** What is computer security?. IEEE Security & Privacy, **2003**; 1(1):67-9.
12. **Bureau of Justice Assistance. Smartphone Thefts and Robberies Growing Trends and Promising Practices:** U.S Department of Justice report on smartphone theft and robberies. Washington, D.C., United States.
13. **Glisson WB, Storer T, Mayall G, Moug I ve Grispos G.** Electronic retention: what does your mobile phone reveal about you?. International Journal of Information Security. **2011**; 10(6):337.
14. **Kumar S ve Mohd J J.** Social media's impact on teenagers and women. Eriřim: (<https://www.researchgate.net/publication>). **2012**. Eriřim Tarihi: 02.01.2020.

15. **Barmpatsalou K, Damopoulos D, Kambourakis G ve Katos V.** A critical review of 7 years of Mobile Device Forensics. *Digital Investigation*. **2013**; 10(4):323-49.
16. **Willassen S.** Forensics and the GSM mobile telephone system. *International Journal of Digital Evidence*. **2003**; 2(1):1-7.
17. **Singh NP.** Online frauds in banks with phishing. *The Journal of Internet Banking and Commerce*. **1970**; 12(2):1-27.
18. **Hamm M S.** Crimes Committed by Terrorist Groups. Eriřim: (<https://www.ncjrs.gov/pdffiles1/nij/grants/211203.pdf>). **2005**. Eriřim Tarihi: 03.24.2020
19. **Pearson EF.** *Criminalistics: An introduction to forensic science: By Richard Saferstein*. Prentice-Hall Inc, Englewood Cliffs, New Jersey, USA, **1982**:287-288.
20. **Lane ND, Miluzzo E, Lu H, Peebles D Choudhury T ve Campbell AT.** A survey of mobile phone sensing. *IEEE Communications magazine*, **2010**; 48(9):140-150.
21. **Curran K, Maynes V ve Harkin D.** Mobile device security. *International Journal of Information and Computer Security*, **2015**; 7(1):1-13.
22. **Casey E.** *Digital evidence and computer crime: Forensic science, computers, and the internet*. Academic press. **2011**; 223-246.
23. **Cynthia M.** Cellular Phone Evidence Data Extraction and Documentation. Eriřim: (<http://www.mobileforensicscentral.com.pdf>). **2014**. Eriřim Tarihi: 02.20.2020
24. **Fiorillo S.** Theory and practice of flash memory mobile forensics. Eriřim: (<https://ro.ecu.edu.au/adf/67/>). **2009**. Eriřim Tarihi: 01.19.2020.
25. **Casadei F, Savoldi A ve Gubian, P.,** Forensics and SIM cards: an Overview. *International Journal of Digital Evidence*, **2006**; 5(1):1-21.
26. **Srivastava A ve Vatsal P.** Forensic importance of SIM cards as a digital evidence. *J Forensic* **2016**; 7(322):1-34.
27. **Mohankumar M, Banuroopa K, Sreevidhya K.** survey on mobile device cyber crime: *International Journal of Research in Electronics and Engineering*, **2018**; 6:2348-2281
28. **Bergman N, Stanfield M, Rouse J ve Scambray J.** *Hacking Exposed: Mobile Security Secrets & Solutions*. Eriřim: (<https://www.academia.edu/>) **2016**. Eriřim Tarihi: 12.28.2019.
29. **Asari K.** Cyber Defamation: A Comparative Analysis of the Legal Position in Malaysia and the United Kingdom. Eriřim: (<https://www.researchgate.net/publication>). **2014**. Eriřim Tarihi: 01.19.2020.
30. **Quadara A, El-Murr A ve Latham J.** The effects of pornography on children and young people. *Australian Institute of Family Studies* Eriřim: (<https://www.safersurfing.org/>). **2017**. Eriřim Tarihi: 12.28.2019.
31. **Newman GR ve McNally MM.** Identity theft literature review, **2005**, 11-23
32. **Lowry BJ, Zhang J, Wang C, Wu T ve Siponen M.** Understanding and Predicting Cyberstalking in Social Media: Integrating Theoretical Perspectives on Shame, Neutralization, SelfControl, Rational

- Choice, and Social Learning. Eriřim: (<https://www.researchgate.net/publication>) **2013**. Eriřim Tarihi: 02.14.2020.
33. **Qijun G ve Peng L.** Denial of Service Attacks,. Eriřim (<https://s2.ist.psu.edu/ist.pdf>.) **2017**. Eriřim Tarihi: 03.03.2020.
34. **Felt AP, Finifter M, Chin E, Hanna S ve Wagner D.** A Survey of Mobile Malware in the Wild. Eriřim: (<https://mfinifter.github.io/papers/mobilemalware>). **2011**. Eriřim Tarihi: 01.14.2020.
35. **Hornik D.** combating software piracy: the softling problem. Harvard Journal of Law & Technology, **1994**; 7(1): 88-94
36. **Levi M ve Burrows J.** Measuring the impact of fraud in the UK. A conceptual and empirical journey. The British Journal of Criminology, **2008**; 48(3):293-318.
37. **Belal A.** Phishing Techniques in Mobile Devices. Journal of Computer and Communications pdf , **2018**; 27-35.
38. **Khan K, Mehmood A, Khan S, Khan MA, Iqbal Z ve Mashwani WK.** A survey on intrusion detection and prevention in wireless ad-hoc networks. Journal of Systems Architecture. **2020** 1;105:101701.
39. **Global Index Web.** VPN Usage Around the World Report. Eriřim: (www.globalwebindex.net). **2017**. Eriřim Tarihi: 03.27.2020.
40. **Bhattarai S.** Virtual Private Network. Eriřim: (<https://www.researchgate.net/publication/pdf>). **2017**. Eriřim Tarihi: 03.15.2020
41. **Yesil B, Kerem Sözeri E, Khazraee E.** Turkey's Internet policy after the coup attempt: The emergence of a distributed network of online suppression and surveillance. Eriřim: (<https://repository.upenn.edu/internetpolicyobservatory/22/>). **2017**. Eriřim Tarihi: 02.17.2020.
42. **Romanov A, Semenov A, Veijalainen J.** Revealing Fake Profiles in Social Networks by Longitudinal Data Analysis. InInternational Conference on Web Information Systems and Technologies, **2017**; 2:51-58.
43. **Akyon FC, Kalfaoglu ME.** Instagram Fake and Automated Account Detection. In2019 Innovations in Intelligent Systems and Applications Conference (ASYU), **2019**; 1-7.
44. **Türkiye Cumhuriyeti Anayasası.** Başkasına ait kimlik bilgilerinin kullanılması TCK 268. **12.10.2004** tarihi ve 25611 sayılı Resmî Gazete'de yayımlanmıştır.
45. **McGovern A ve Milivojevic S.** Social Media and Crime. La Trobe University websites Eriřim: (<https://www.latrobe.edu.au>.), **2017**. Eriřim Tarihi: 03/23 /2020
46. **Peng S, Yu S, Yang A.** Smartphone malware and its propagation modeling: A survey. IEEE Communications Surveys & Tutorials. **2013**; 16(2):25-41.
47. **Layton J.** How Mobile Malware Can Enter Your Smartphone. Housestuffworks websites. Eriřim: (<https://electronics.howstuffworks.com/cell-phone-virus2.htm>.) Eriřim Tarihi: 03,23, 2020
48. **Suarez-Tangil G, Tapiador JE, Peris-Lopez P, Ribagorda A.** Evolution, detection and analysis of malware for smart devices. IEEE Communications Surveys & Tutorials, **2013**; 16(2):961-987.

45. **Malwarebyteslabs 2020.** State of Malware Report, Eriřim: (<https://resources.malwarebytes.com/pdf>). 2020. Eriřim Tarihi: 03.24.2020.
50. **Button M, Lewis C ve Tapley J.** Fraud typologies and the victims of fraud: Literature review. Eriřim: (<https://researchportal.port.ac.uk/pdf>).2016). Eriřim Tarihi: 03/27 /2020.
51. **Gloria Huniford.** The little book of Big Scam. Metropolitan Police U.K (Book), 5:68-84.
52. **ECC.** Net (European Consumer Centres Network) Fraud in Cross-Boarder. E-commerce. European union report on fraud, **2017**, 09-24
53. **Federal Bureau of Investigation FBI 2017** Internet Crime Report. Eriřim: (fbi.gov/pdf). **2018**. Eriřim Tarihi: 03/29 /2020.
54. **Zengin F.** Dolandırıcıların gözdesi İstanbul. Eriřim: ([https://www.milliyet.com.tr\(website\)](https://www.milliyet.com.tr(website))). **2018**. Eriřim Tarihi: 03/29 /2020.
55. **Jahankhani H, Al-Nemrat A, Hosseinian-Far A.** Cybercrime classification and characteristics. InCyber Crime and Cyber Terrorism Investigator's Handbook **2014**; 149-164Syngress, 2014;149-164.
56. **Quade MH, Leimstoll U.** Mobile Business with Smartphones and Tablets: Effects of Mobile Devices in SMEs. InBled eConference, **2015**;1-12
57. National Identity Management Commission. National id specs. Eriřim: ([https://www.nimc.gov.ng/docs/biometrics standards specs/pdf](https://www.nimc.gov.ng/docs/biometrics_standards_specs/pdf)). **2018**. Eriřim Tarihi: 03.30.2020.
58. **Megan G.** Why-Fi or Wiffy? How Americans Pronounce Common Tech Terms, **2014**; 111-119.
59. **Dawson M, Wright J, Omar M.** Mobile devices: The case for cyber security hardened systems. In New Threats and Countermeasures in Digital Crime and Cyber Terrorism, **2015**; 8-29.
60. **Aldhafferi N, Watson C, Sajeev AS.** Personal information privacy settings of online social networks and their suitability for mobile internet devices. International Journal of Security, Privacy and Trust Management. **2013**; 2:1305-2770
61. **Franchi E, Poggi A, Tomaiuolo M.** Information Attacks on Online Social Networks. Journal of Information Technology Research (JITR). **2014**; 7(3):54-71.
62. **Krombholz K, Merkl D ve Weippl E.** Fake identities in social media: A case study on the sustainability of the facebook business model. Journal of Service Science Research. **2012**; 4(2):175-212.
63. **Network EU.** 3rd generation partnership project; technical specification group services and system aspects; general packet radio service (GPRS) enhancements for evolved universal terrestrial radio access network (E-UTRAN) access. EUTRA Network. **2011**; 9(0):1-8.
64. **Europe GS.** GSME proposal regarding mobile theft and IMEI security. Eriřim: ([http://www. gsmeurope. org/documents/positions/gsme_proposals_mobile_thefts_imei_security](http://www.gsmeurope.org/documents/positions/gsme_proposals_mobile_thefts_imei_security). Pdf). **2003**. Eriřim Tarihi: 10.30.2019.
65. **Chen CL.** A secure and traceable E-DRM system based on mobile device. Expert Systems with Applications. **2008**; 35(3):878-886.

66. **Mobile Telephones (Re-programming) Act 2002.** Eriřim: (Legislation.gov.uk.) 2013. Eriřim Tarihi: 01.20.2020.
67. **Ozkan AF.** An Economic Analysis of the “Mobile Equipment Registration System” in Turkish Telecommunications Law. *Computer and Telecommunications Law Review*, **2015**; 21(5):123-129.
68. **The Saudi government is hunting down women who flee the country by tracking the IMEI number on their cellphones.** Eriřim: (<https://www.businessinsider.com/saudi-arabia-imei-track-runaways>). **2019.** Eriřim Tarihi: 11.12.2019.
69. **Farrell G.** Preventing phone theft and robbery: the need for government action and international coordination. *Crime science*, **2015**; 4(1):4.



EKLER

EK 1. ANKET FORMU

Bu anket Çukurova Üniversitesi Bağımlılık ve Adli Bilimler Enstitüde yüksek lisans öğrenci Charles Sserutte' in Araştırma tezi için yapılmaktadır. Anketin amacı **Bilişim Suç Aracı Olarak Mobil/Akıllı Telefon Kullanımı: Adana Örneği** yaşanan sorunlarla ilgilidir. Araştırma bilimsel bir nitelik taşıdığından derlenen kişi ve aile bilgileri gizli tutulacaktır. Sorulara objektif ve samimi cevaplar vereceğinize inanıyorum. Katkılarınız için şimdiden teşekkür ederim.

Lütfen soruları tam olarak okuduktan sonra kendinize en uygun olan cevabı işaretleyiniz.

Adı Soyadı:

Cinsiyet: Erkek ☐ Kadın ☐

Yaş: A).0-19 ☐ C).20-39 ☐ D).40-59 ☐ E). 60 ≥ ☐

Eğitim seviyesi: A).İlkokul ☐ B).Ortaokul ☐ C). Lise ☐ D).Üniversite ☐

1). Kaç kişilik ailesiniz?.....

2). Büyüklerin telefon var mı ?

A). Evet ☐ D).Hayır ☐

3). Sizden küçüklerin telefon var mı ?

A). Evet ☐ D).Hayır ☐

4). Ailen birin telefon kullanımı ile ilgili bir sorun yaşadı mı ? Evetse yazınız

.....

5). Akıllı telefonunuz var mı?

A). Evet ☐ D).Hayır ☐

6). Telefonunun markası ne?

A).Apple ☐ B).Samsung ☐ C).HTC ☐ D).LG ☐ E). Diğerleri (belirtin)

7). Telefonunuzu iş veya kişisel kullanım için kullanıyor musunuz?

A) kişisel kullanım ☐ B).İş ☐ C) her ikisi de ☐

- 8). Hangi operatörü kullanıyorsunuz?
- A).Vodafone ☐ B).Türkcell ☐ C) Türk Telekom ☐
- 9). Operatörü ne sıklıkla değiştirirsiniz? Kutucuğa rakam yazınız.
- A). Genellikle ☐ B). Sık sık ☐ C). Bazen ☐ D). Nadiren ☐ E).Asla ☐
- 10). Akıllı telefonunuzun işletim sistemini ne kadar iyi biliyorsunuz?
- A).10% ☐ B)30% ☐ C)50% ☐ D).70% ☐ E).100% ☐
- 11) Telefonunuzda kullanmakta olduğunuz mevcut işletim sisteminiz nedir?
- A). Android ☐ B). Apple(İOS) ☐ C) Symbian(nokia) ☐ D).Diğer ☐
- 12). İnternet kullanıyor musun?
- A). Evet ☐ D).Hayır ☐
- 13). İnterneti çoğunlukla ne için kullanıyorsunuz? (1 ile 3 arasında bir sayı)
- A). Eğitim amacı ☐ B). Sosyal medya ve oyunlar ☐ C). İş amacı ☐
- 14). VPN' genellikle yayıncıya açık olmayan web sitelerine veya bazı ülkelerde erişmek için kullanıyor musunuz? (wikipedia gibi siteleri)
- A.Evet ☐ B). Hayır ☐
- 15). Akıllı telefon uygulamalarınızı (sosyal medya, mesajlaşma, oyunlar) kullanarak günde yaklaşık kaç saat harcıyorsunuz?
- A). 1 saatten az ☐ B)1-2 saat ☐ C).3-4 saat ☐ D).5 saatten fazla ☐
- 16). Telefonunuzda en çok kullanılan uygulamalar hangileridir?
-
- 17). Bu sosyal medya uygulama hesaplarını oluştururken gerçek soyadınızı ve adınızı mi kullanıyorsunuz??
- A). Evet ☐ B). Hayır ☐
- 18). Uygulamaları birisinin tavsiye üzerine kullanıyor musun ?
- A). Evet ☐ B). Hayır ☐
- 19). Mobil uygulamaları yüklerken, indirmeden önce bu uygulamaların şartlarını ve koşullarını okur musunuz?
- A). Evet ☐ B) Hayır ☐
- 20). Hiç sahte sosyal medya hesabı oluşturduunuz mu?
- A).Evet ☐ B). Hayır ☐

21). Sahte bir hesap kullanarak sosyal medyadaki biri tarafından hiç rahatsız ettiniz mi veya rahatsız oldunuz mu?

Evet

Hayır

Facebook		
Twitter		
Whatsapp		
Istangram		
Diğerler (Snapchat gibi)		

22). Sosyal medyada hiç siber takip veya zorbalığı muhatap oldunuz mu?

A) Evet ☐ B). Hayır ☐

23). Konum bildiren uygulamaları kullanan birisi tarafından takip edildiniz mi ?

A). Evet ☐ B). Hayır ☐

24). Telefonunuz bir bağlantısı yoluyla paylaşılan virüslerden etkilendi mi ve bu durum telefonunuzun performansını olumsuz etkiledi mi?

A) Evet ☐ B) Hayır ☐

25). . Hiç ikinci el telefon kullandın mı?

A). Evet ☐ B). Hayır ☐

26). Bilmeden kullandığınız ikinci el telefon yüzden kullanırken herhangi bir sorunla karşılaştınız mı?

A). Evet ☐ B). Hayır ☐

27) Hiç başkasının İMEİ (yurt dışında gelen telefonlar) adresine kayıtlı bir akıllı telefon kullandınız mı?

A). Evet ☐ B). Hayır ☐

28). Böyle bir telefonu kullanırken polisle yasal sorunlara yol açan herhangi bir problemle karşılaştınız mı?

A). Evet ☐ B) Hayır. ☐

29). Akıllı telefonunuzu hiç çalındı mı?

A). Evet ☐ B). Hayır ☐

30). Telefonunuzun çalınmasından dolayı kişisel bilgileriniz tehlikeye atıldı mı?

A). Evet ☐ B). Hayır ☐

31). Sahtekârlardan (dolandırıcı) bir telefon veya test mesajı aldınız mı?

A). Hayır. ☐

B). Evet. ☐ Ne istediler?

A). Para. ☐ B). Altın ☐ C). Banka hesabı bilgileri. ☐ C). Diğerleri. ☐

31). E-dolandırıcılık (e mail gibi gönderen linkler kişisel sorgulayan bilgiler TC veya banka hesap bilgileri) hiç yaşadınız mı?

A). Evet ☐ B). Hayır ☐

32). Kredi kartlarıyla telefon alışveriş yapıyor musun?

A). Evet ☐ B) Hayır ☐

33). Hiç sorunla karşılaştınız mı? (sanal web gibi ya da yanlış ürün veya sahte aldınız mı?)

A)Evet ☐ B)Hayır ☐

34). Banka uygulamalar (İŞ Cep, Ziraat Mobil vb) kullanıyor musun?

A). Evet ☐ B). Hayır ☐

35). Banka uygulamaları kullanırken hiç sorun yaşadınız mı?

A). Evet ☐ B) Hayır ☐

ÖZGEÇMİŞ

Charles Sserutte, 1992 yılında Kampala/Uganda’da doğdu. İlkokul, ortaokul ve lise eğitim Uganda’da tamamladı. 2012 yılında Çukurova Üniversitesi Fen Edebiyat Fakültesi Matematik Bölümünü kazandı, 2016 yılında mezun oldu. 2018’de Çukurova Üniversitesi Bağımlılık ve Adli Bilimler Enstitüsü Bağımlılık Anabilim Dalında Tezli Yüksek Lisans programına başladı. Çok iyi derecede Luganda, İngilizce ve Türkçe bilmektedir.

