

**TÜRKİYE CUMHURİYETİ
ÇUKUROVA ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
İLETİŞİM ÇALIŞMALARI ANA BİLİM DALI**

**KİŞİSEL VERİ GİZLİLİĞİ VE DİJİTAL ÇAĞDA MAHREMİYET: SESLİ
SANAL ASİSTANLAR**

Elçin KÖKSALAN

YÜKSEK LİSANS TEZİ

ADANA / 2022

TÜRKİYE CUMHURİYETİ
ÇUKUROVA ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
İLETİŞİM ÇALIŞMALARI ANA BİLİM DALI

KİŞİSEL VERİ GİZLİLİĞİ VE DİJİTAL ÇAĞDA MAHREMİYET: SESLİ
SANAL ASİSTANLAR

Elçin KÖKSALAN

Danışman: Dr. Öğr. Üyesi Sevdâ ÜNAL

Jüri Üyesi: Dr. Öğr. Üyesi Çiğdem Yasemin ÜNLÜ

Jüri Üyesi: Dr. Öğr. Üyesi Fatma YASA

YÜKSEK LİSANS TEZİ

ADANA / 2022

Çukurova Üniversitesi Sosyal Bilimler Enstitüsü Müdürlüğüne;

Bu çalışma, jürimiz tarafından Ana Bilim/Ana Sanat Dalında
YÜKSEK LİSANS TEZİ olarak kabul edilmiştir.

Başkan: Ünvanı, Adı Soyadı
(Danışman)

Üye: Ünvanı, Adı Soyadı

Üye: Ünvanı, Adı Soyadı

ONAY

Yukarıdaki imzaların, adı geçen öğretim elemanlarına ait olduklarını onaylarım.

.../.../20...

Prof. Dr. Serap ÇABUK

Enstitü Müdürü

NOT: Bu tezde kullanılan ve başka kaynaktan yapılan bildirişlerin, çizelge, şekil ve fotoğrafların kaynak gösterilmeden kullanımı, 5846 sayılı Fikir ve Sanat Eserleri Kanunu'ndaki hükümlere tabidir.

ETİK BEYANI

Çukurova Üniversitesi Sosyal 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 ve ahlak kurallarına uygun olarak sunduğumu,
 - Tez çalışmada yararlandığım eserlerin tümüne uygun atıfta bulunarak kaynak gösterdiğimi,
 - Kullanılan verilerde ve ortaya çıkan sonuçlarda herhangi bir değişiklik yapmadığımı,
 - Bu tezde sunduğum çalışmanın özgün olduğunu,
- bildirir, aksi bir durumda aleyhime doğabilecek tüm hak kayıplarını kabullendiğimi beyan ederim. / / 20....

İMZA

Elçin KÖKSALAN

ÖZET

KİŞİSEL VERİ GİZLİLİĞİ VE DİJİTAL ÇAĞDA MAHREMİYET: SESLİ SANAL ASİSTANLAR

Elçin KÖKSALAN

Yüksek Lisans Tezi, İletişim Çalışmaları Ana Bilim Dalı

Danışman: Dr.Öğr. Üyesi Sevda ÜNAL

Mayıs 2022, 112 sayfa

Dijitalleşen dünyada kişisel verilerin gizliliği ve korunabilirliği, insan hakları konusunun en öncelikli güncel problemlerinden biri haline gelmiştir. Bireyin gündelik yaşantısının her anında kullanmasının artık zorunlu hale geldiği dijital teknolojiler, olumlu yanlarının yanı sıra bireyin mahremiyetine yönelik tehditler de oluşturmaktadır. Bu teknolojilerden biri olan sesli sanal asistanlar, ses tanıma ve doğal dil işleme gibi yapay zekâ destekli çalışma sistemleriyle kullanıcılarının sesli komutlarını algılayabilen ve yanıtlayabilen yazılımlardır. Cep telefonları ve ev tipi hoparlörler aracılığıyla hizmet sunabilen sesli sanal asistanlar, bu sayede kullanıcıların daima yanlarında bulundurdıkları araçlar haline gelmişlerdir. Bu araçlar ihtiyaç çeşitliliğine bağlı olarak her gün daha fazla geliştirilmektedir ve bunun için kullanıcı verilerine ihtiyaç duymaktadır.

Bu çalışmada, sesli sanal asistanlar kişisel veri gizliliği yönünden incelenerek, bu teknolojinin kullanımı sırasında yaşanabilecek risklere vurgu yapılmıştır. Kişisel veriye yönelik riskler karşısında kullanıcıların bilinçlenmelerinin öneminden dolayı, çalışma kapsamında İletişim Fakültesi öğrencilerinin sesli sanal asistanlar ve kişisel veri gizliliğiyle ilgili algı, tutum ve farkındalıklarını ortaya koymayı amaçlayan görüşmeler yapılmıştır. Görüşmelerde elde edilen bulgular MAXQDA nitel veri analizi programı ile analiz edilerek kodlara ayrılmıştır. Çalışmanın sonucunda kullanıcıların veri gizliliğine dair bilgisi ile mahremiyet endişelerinin her zaman doğru orantılı olmadığı, kullanıcıların bilgileri olsa da mahremiyet ihlallerini kabul eden, akıllı teknolojileri benimseyen ve kullanmaya devam eden bir tutum benimsedikleri görülmüştür.

Anahtar kelimeler: Kişisel veri gizliliği, dijital mahremiyet, sesli sanal asistanlar

ABSTRACT**PERSONAL DATA PRIVACY AND PRIVACY IN THE DIGITAL AGE:
VIRTUAL VOICE ASSISTANTS****Elçin KÖKSALAN****Master Thesis, Department of Communication Studies****Supervisor: Dr. Sevda ÜNAL****May 2022, 112 pages**

In the digitalized world, the confidentiality and protection of personal data has become one of the most prioritized current problems of human rights. Digital technologies, which have become mandatory for individuals to use at every moment of their daily life, pose threats to the privacy of the individual, as well as having obvious positive aspects. Voice virtual assistants, one of these technologies, is software that can detect and respond to the voice commands of their users with artificial intelligence supported working systems, such as voice recognition and natural language processing. Voice virtual assistants can provide services through mobile phones and home speakers, having thus become tools that users always have with them. It is being developed exponentially every day depending on a wide variety of needs and it requires user data for this.

In this study, voice virtual assistants are examined in terms of personal data privacy and the risks that can be experienced during the use of this technology are emphasized. Due to the importance of users' awareness of risks to personal data, interviews were conducted within the scope of the study, aiming to reveal the perception, attitude, and awareness levels of the students of the Faculty of Communication regarding voice virtual assistants and personal data privacy. The findings obtained from the interviews were analyzed with the MAXQDA qualitative data analysis program. As a result of the study, it has been seen that the users' knowledge of data privacy and privacy concerns are not always directly proportional, and that users adopt an attitude that accepts privacy violations even if they have information. They adopts this fact and continues to use smart technologies.

Keywords: Personal data, digital privacy, voice virtual assistants

ÖN SÖZ

Tez çalışmam boyunca büyük bir özveri ve sabırla bana destek olan, yalnızca akademik tecrübelerini değil; fikrine ihtiyaç duyduğum her konuda bilgisini ve şefkatini benimle paylaşan saygıdeğer danışmanım Dr. Öğr. Üyesi Sevda ÜNAL'a teşekkürlerimi sunarım.

Tez jürimde bulunarak beni onurlandıran kıymetli hocalarım Dr. Öğr. Üyesi Çiğdem Yasemin ÜNLÜ'ye ve Dr.Öğr. Üyesi Fatma YASA'ya teşekkürlerimi sunarım.

Eğitim hayatım boyunca bilgilerinden faydalandığım ve öğrettikleriyle beni düşünmeye sevk eden, daha iyi bir insan olmamı sağlayan tüm hocalarıma teşekkürlerimi sunarım.

İlk öğretmenim, her zaman en büyük destekçim olan canım annem Naciye CAN'a, aynı aileyi paylaştığım için daima çok şanslı hissettiğim kız kardeşlerim Burçin KÖKSALAN'a, Neslican KÖKSALAN'a ve teyzem Nurcan GELMEZ'e teşekkürlerimi sunarım.

Hayatımın en güzel zamanlarını paylaştığım dostum Gözde EBELER'e ve cesaretimi desteğiyle hep diri tutan Omar VALENCIA'ya teşekkürlerimi sunarım.

İÇİNDEKİLER

ÖZET	iv
ABSTRACT	v
ÖN SÖZ	vi
KISALTMALAR	x
TABLolar LİSTESİ	xi
ŞEKİLLER LİSTESİ	xii
RESİMLER LİSTESİ	xiii
EKLER LİSTESİ	xiv

BÖLÜM I

GİRİŞ

1.1. Araştırmanın Problemi ve Amacı	3
1.2. Araştırmanın Önemi	5
1.3. Araştırmanın Sınırlılıkları.....	5

BÖLÜM II

DİJİTAL MAHREMİYET VE KİŞİSEL VERİ GİZLİLİĞİ

2.1. Mahremiyet Tartışmaları	10
2.2. Dijital Mahremiyet ve Veri Gizliliği	11
2.3. Dijital Çağda Kişisel Veri.....	12
2.4. Kişisel Verilerin İşlenmesinde Genel İlkeler	14
2.4.1. Türkiye’de Kişisel Verilerin Korunması.....	15
2.5. Kişisel Veriler Neden ve Nasıl İşlenir?	17
2.6. Dijital Çağda Kişisel Verilerin Gizliliği, Güvenliği ve Korunması.....	19

BÖLÜM III

SESLİ SANAL ASİSTANLAR

3.1. Yapay Zekâ Teknolojilerinin Doğuşu.....	22
3.2. Sesli Sanal Asistanlar.....	24

3.2.1. Sohbet Botları	26
3.2.2. Sesli Sanal Asistanların Çalışma İlkeleri	27
3.2.2.1. Makine Öğrenimi – Derin Öğrenme	28
3.2.2.2. Doğal Dil İşleme	29
3.3. Sesli Sanal Asistanlar ve Kişisel Veri Gizliliği	30
3.3.1. Sesli Sanal Asistanlar ve Güvenlik	33
3.3.2. Sesli Sanal Asistanların Kullanım Alanları ve Veri Gizliliği Politikaları	34
3.3.2.1. Siri	35
3.3.2.2. Google Asistan	36
3.3.2.3. Alexa	38
3.3.2.4. Bixby	39
3.3.2.5. Cortana	41

BÖLÜM IV

KUŞAK KAVRAMI

4.1. Dijital Yerliler ve Dijital Göçmenler	46
4.1.1. Dijital Yerliler	47
4.1.2. Dijital Göçmenler	48
4.2. Kuşakların Mahremiyet Algısı	49
4.2.1. Y ve Z Kuşağının Mahremiyet Algısı	50
4.2.2. X Kuşağının Mahremiyet Algısı	51

BÖLÜM V

YÖNTEM VE BULGULAR

5.1. Araştırmanın Yöntemi ve Kapsamı	53
5.2. Araştırmanın Bulguları	56
5.2.1. Sesli Sanal Asistanları Tanımlamak	62
5.2.2. Kullanılan Sesli Sanal Asistanlar	64
5.2.3. Sesli Sanal Asistanların Kullanım Amaçları	67
5.2.4. Sesli Sanal Asistanların Kullanıldığı Mecralar	69
5.2.5. Sesli Sanal Asistanların Sağladığı Avantajlar	70
5.2.6. Veri Gizliliği ve Güvenliğine Dair Kullanıcı Farkındalığı	72

5.2.7. Veri Gizliliđi ve Güvenliđine Dair Bilginin Kaynakları.....	77
5.2.8. Sesli Sanal Asistanların Gizlilik Yönünden Dezavantajları	78
5.2.9. Kullanıcıların Gizlilik Politikaları Konusunda Bilgilendirilmesi	80
5.2.10. SSA’ların Veri İhlaline İlişkin Katılımcıların Kullanıcı Tecrübesi	83
5.2.11. Kullanıcıların Aldıđı Kişisel Önlemler	85
SONUÇ	87
KAYNAKÇA	93
EKLER	110
ÖZGEÇMİŞ	112



KISALTMALAR

SSA	: Sesli Sanal Asistan
KVKK	: Kişisel Verilerin Korunması Kanunu
GDPR	: Genel Veri Koruma Tüzüğü
IBM	: International Business Machines Corporation
IoT	: Internet of Things



TABLÖLAR LİSTESİ

Tablo 1. <i>Kodların ve Alt Kodların Frekans Analizi</i>	58
Tablo 2. <i>Katılımcıların Gizlilik Bilgileri ve Bilgilendirme Metinlerini Okuma Oranları Arasındaki İlişki</i>	81
Tablo 3. <i>Katılımcıların Gizlilik Bilgileri ve Bilgilendirme Metinlerini Okuma Oranları Arasındaki İlişki 2</i>	81



ŞEKİLLER LİSTESİ

Şekil 1. Katılımcıların yaş dağılımları.....	56
Şekil 2. Katılımcıların cinsiyet dağılımları.....	56
Şekil 3. Alt kodların kelime grubu	60
Şekil 4. “Gizlilik” kelimesiyle oluşturulan etkileşimli kelime ağacı.....	61
Şekil 5. SSA’ları tanımlamış ve tanımlamamış katılımcılar	62
Şekil 6. Katılımcılar arasında en sık kullanılan SSA’lar	64
Şekil 7. SSA’ların kullanım amaçları	67
Şekil 8. SSA’ların kullanıldığı mecralar.....	69
Şekil 9. SSA’ların kullanıcılara sağladığı avantajlar.....	70
Şekil 10. Veri gizliliği ve güvenliğine dair farkındalıklar.....	72
Şekil 11. Veri gizliliği ve güvenliğine ilişkin bilgi kaynakları.....	77
Şekil 12. SSA’ların gizlilik yönünden dezavantajları	78
Şekil 13. Gizlilik politikalarına dair bilgilendirilme durumları.....	80
Şekil 14. SSA’ların veri ihlaline ilişkin katılımcıların tecrübeleri	83
Şekil 15. Katılımcıların aldığı kişisel önlemler	85

RESİMLER LİSTESİ

Resim 1. Etkinleştirilmiş mobil sesli sanal asistanlar	27
Resim 2. Konuşma tanıma işlemi süreci	29
Resim 3. Siri'nin orta tuş ile aktifleşmesi	35
Resim 4. Google asistanın arayüzü	37
Resim 5. Alexa'nın aktif haldeki görüntüsü.....	38
Resim 6. Bixby'nin arayüzü	40
Resim 7. Cortana'nın arayüzü	41



EKLER LİSTESİ

Ek. 1. Araştırma Gönüllü Katılım Formu.....	110
Ek. 2. Görüşme Soruları	111



BÖLÜM I

GİRİŞ

İnsanlık tarihinin son yarım asrında teknolojinin büyük ataklar yapmasıyla birlikte, her geçen gün daha da dijitalleşen dünyada insan-makine ilişkisi yeni bir boyut kazanmaya başlamıştır. Yaşamın da en az teknolojik gelişmeler kadar hızlanmasıyla birlikte insanlar bir günlerine yapabileceklerinden çok daha fazlasını sığdırmaya mecbur hissetmeye başlamışlardır ve bu zorunluluk yeni ihtiyaçlar yaratmıştır. Bunun sonucu olarak günümüzde dijital teknolojiye duyulan ihtiyaç yapay zekâ fikrinin doğduğu 1950’lerde bile tahmin edilemeyeceği ölçülerdedir. Bu yapay zekâ teknolojilerinden sesli sanal asistanlar (SSA) henüz yeni bir teknoloji sayılmasına rağmen 2021 yılı itibarıyla kullanıcı sayısı 132 milyon kişiye ulaşmıştır (Statista, 2022). SSA’lar evlerde, mobil cihazlarda, kişisel araçlarda, iş yerlerinde ve okullarda yaygınlaşırken aynı zamanda diğer internet tabanlı cihazlara entegre olarak daha fazla akıllı teknoloji aracılığıyla etkinliğini artırmaktadır. Bu derece hızlı yaygınlaşan bir teknolojinin faydalarının konuşulduğu kadar, olası zararlarının da düşünülmesi ve gereken önlemlerin alınması şarttır. SSA’lar özelinde kişisel veri gizliliği ve dijital mahremiyet konularının tartışıldığı bu çalışmanın içeriği, internet bağlantılı tüm ev tipi ve mobil cihazların kullanımı sırasında yaşanabilmesi mümkün olan mahremiyet ihlallerine karşı örnek kabul edilebilir. Dünyada internet tabanlı akıllı cihazların özelliklerinin ve gizlilik politikalarının tartışıldığı birçok çalışma yapılmışsa da konu Türkiye’de hala yenidir ve literatürdeki çalışmalar kısıtlıdır.

Türkiye’deki çalışmalara dair alanyazın incelenirken göz önünde bulundurulacak birincil etmen çalışmaların özellikle “dijital asistan, sesli sanal asistan, akıllı asistan” ifadelerine benzer şekilde SSA sınıfına giren akıllı teknolojiler üzerine yapılan çalışmalar olmasıdır. Zira alanyazında akıllı teknolojiler, dijital mahremiyet ve sesli asistanlar üzerine ayrı ayrı çalışmaları bulunsa da bu çalışmada olduğu gibi bu konuların analizi olan benzer bir çalışmaya ulaşılmamıştır. Aramalar sonucunda “mobil asistan” aramasına karşılık üç yüksek lisans tezine ulaşılmıştır fakat bunlar bilgisayar mühendisliği alanında yapılmış çalışmalardır. YÖK Ulusal Tez Merkezi üzerinden ulaşılabilen SSA’larla ilgili en eski çalışma Gökhan Çelikkaya’nın (2015) “Doğal Dil İşleme Teknikleri Kullanılarak Türkçe Mobil Asistan Yazılımı Geliştirilmesi” başlıklı yüksek lisans tezidir. Bununla birlikte yakın zamanda yapılmış diğer çalışmalar, Ayça

Atabey'in (2019) "Is Google at Odds With the GDPR? Evaluation of Google's Personal Data Collection on Mobile Operating Systems in Light of the Principles of Data Minimisation, Purpose Limitation, and Accountability" başlıklı yüksek lisans tezi, Sümeyya Olcay'ın (2019) "Sosyal İhtiyaçların Karşılansında Yeni Medya Uygulama Örneği Olarak Dijital Asistanlar" başlıklı yüksek lisans tezi, Deniz Gül Özcan'ın (2020) "Doğal Dil İşleme Tekniklerinin İncelenmesi ve Seyahat-Turizm Sesli Asistanı için Türkçe Varlık İsmi Tanıma Aracı Geliştirilmesi" başlıklı yüksek lisans tezi, Hakan Özler'in (2021) "Apple Siri ve Google Assistant Çoklu Medya Bildirimlerinde Akıllı Mobil Asistan Deneyiminin Geliştirilmesi" başlıklı yüksek lisans tezidir. Nil-Göksel Canbek ve Mehmet Emin Mutlu'nun (2016) "Sayısal gelecekte yeni adım: akıllı kişisel yardımcılar" başlıklı makalesi de yine Türkiye'de alanyazındaki en eski çalışmalardan bir tanesidir.

Uluslararası literatürde SSA'larla ilgili çalışmaları incelemek amacıyla OATD (Open Access Theses and Dissertations) üzerinden "voice assistant" ifadesine dair arama yapılmış ve konuya ilişkin yapılan en eski çalışmaların 2003 yılında yayınlandığı görülmüştür. En fazla çalışma ise SSA kullanımının yaygınlaşması ile doğru orantılı olarak 2018-2022 yılları arasında (128 çalışma) yayınlanmıştır. Arama "voice assistant, privacy (sesli asistan, mahremiyet)" olarak daraltıldığında ise SSA ve mahremiyet konularının ele alındığı 17 çalışmaya ulaşılmaktadır. Bunlardan en eski olanı 2014 yılında Easwara Moorthy ve Kim-Phuong L. Vu'nun yazmış olduğu "Privacy Concerns for Use of Voice Activated Personal Assistant in the Public Space (Kamusal Alanda Sesle Etkinleştirilen Kişisel Asistanın Kullanımına İlişkin Gizlilik Endişeleri)" başlıklı çalışmadır. 2013 yılına kadar olan çalışmalar kablosuz erişim, ses tanıma teknolojisi, makine öğrenimi, akıllı yazılımlar, insan-bilgisayar etkileşimi gibi SSA'nın da temelinde yer alan teknolojilere yönelik konuları ele almıştır.

Sesli sanal asistanların ele alındığı bu çalışma beş bölümden oluşmaktadır. Çalışmanın amacı, kapsamı, önemi ve sınırlılıklarının ele alındığı birinci bölümden sonra ikinci bölümde "mahremiyet" ve "dijital mahremiyet" kavramlarının tanımı yapılmış, mahremiyet kavramı kültürle ilişkilendirilerek açıklanmıştır. Mahremiyet anlayışının kültürden kültüre, çağdan çağa hangi boyutlarda farklılıklar gösterebileceği dijital teknolojiler, dijital çağ ve kuşaklar gibi kavramlar üzerinden incelenmiştir. Mahremiyet kavramı ile vurgulanmak istenen "kişisel verinin mahremiyeti" olsa da çalışmanın gidişatı itibarıyla mahremiyetin toplumsal gerekçeleri ve sonuçları da ele alınmıştır. Alanyazındaki mahremiyet tartışmalarının temellerine ve dijitalleşmenin bu

tartışmaları nasıl şekillendirdiğine değinilmiştir. Ardından kişisel veri, kişisel verilerin neden ve nasıl işlendiği ve yakın tarihte Türkiye’deki anayasal düzenlemelerle kişisel verinin korunması ve işlenmesi konusunda ne gibi gelişmeler yaşandığı açıklanmıştır. Kişisel verinin nasıl finansal bir değer haline geldiği ve büyük şirketler için veri saklamanın ve veriler üzerinden kazanç sağlamanın ne gibi avantajları olduğu ele alınmıştır. Bu bölümde kişisel veri ifadesinin nelere kapsadığı, bu verilerin korunması için hukuksal altyapının güçlü olmasının ve şirketlerin düzenlemekle yükümlü olduğu politikaların şeffaflığının önemi ele alınmıştır.

Üçüncü bölümde yapay zekâ teknolojisinin düşünceden hayata geçirilmesine, yapay zekâ araştırmaları ve SSA’ların geliştirilmesine kadar olan dönem incelenmiştir. SSA’ların tanımı yapılmış, güncel SSA’lar ve geliştirici şirketlerin gizlilik politikaları açıklanmıştır. SSA’ların kısa fakat hızlı ilerleyen tarihsel sürecine, SSA’lara benzer teknolojiler olan fakat bariz farklılıklar içeren sohbet botlarına, SSA’ların teknik özellikleriyle birlikte genel olarak SSA teknolojisine değinilmiştir.

Dördüncü bölümde kuşaklar incelenmiş, X, Y ve Z kuşaklarının farklı bir bakış açısından tanımı olan “dijital yerli” ve “dijital göçmen” kavramlar ele alınmıştır. Ardından mahremiyet anlayışına ilişkin kuşaklar arasındaki farklılıklar incelenmiştir. Toplumsal değişimin sonucu olarak kuşak farklılığı ve beraberinde değişen mahremiyet algısı beraber ele alınmıştır. Böylece tezin araştırma konusu da olan, çoğunlukla Y ve Z kuşağının oluşturduğu “üniversite öğrencilerinin kişisel veri gizliliğine dair algıları” konusuna zemin hazırlanmıştır. Çalışmanın beşinci ve son bölümüyle, Çukurova Üniversitesi İletişim Fakültesi öğrencileri ile yapılan görüşmelerden derlenen verilerle yürütülmüş olan araştırmanın detayları ve bulguları değerlendirilmiştir.

1.1. Araştırmanın Problemi ve Amacı

Teknolojik gelişmelerle birlikte gündelik yaşamın önemli bir parçası haline gelen SSA’ların kullanıcı sayıları hızla artmaktadır. Alman araştırma şirketi Statista tarafından yayımlanan “2019’dan 2024’e Kadar Dünya Çapında Kullanılan Dijital Sesli Asistan Sayısı (milyar olarak)” başlıklı istatistiğe göre 2020 yılı için tüm dünyada kullanılan SSA sayısı 4,2 milyar olarak açıklanırken, bu sayının 2024 yılında 8,4 milyar olmasının beklendiği belirtilmektedir (Laricchia, 2022). 2021 yılında ABD’de SSA’ların kullanımına ilişkin araştırmaya göre 55 yaş üstü katılımcıların yaklaşık yüzde

40'ı Amazon'a ait ev tipi SSA olan Alexa'ya kullanırken, 18-24 yaş arası katılımcıların yüzde 60'ı Apple'a ait SSA olan Siri'yi kullanmaktadır (Statista Research Department, 2022).

Kullanıcıların bilgiyi arama ve erişim pratiklerinde önemli değişikliklere yol açan SSA'lar, ayrıca öğrencilerin “özerk öğrenimini geliştirmek için geniş bir öğretim potansiyeli sunmaktadır” (Al Shamsi, Al-Emran ve Shaalan, 2022, s.3).

Sunduğu fırsatlar kadar veri gizliliği ve mahremiyet açısından taşıdığı risk ve tehditler SSA'ların kullanımında soru işaretlerine neden olmaktadır. İnsan odaklı teknolojiler olarak niteleyebileceğimiz SSA, insanların günlük yaşamındaki her alanda işlerini kolaylaştırdığı ve bilgiye erişimi hızlı ve kolay kıldığı gibi, bu kişilerin verilerine üçüncü kişilerin izinsiz erişimini mümkün kılmakta, dahası kullanıcı rolündeki kişilerin bilinçli bir tercihle bu verileri paylaşması yönünde teşvik edici olmaktadır. Burada önemli olan kişilerin, verilerinin ne amaçla ve hangi kapsamda paylaşacağına dair bilgisinin olmasıdır (Erdinç, 2017). SSA kullanıcıları uygulamaları kullanmak için aktifleştirdiklerinde uygulamanın hizmet şartlarını ve gizlilik politikalarını da kabul etmiş olurlar. Gizlilik politikaları bu tür uygulamalar ve web sitelerinde yer alan ve içeriğindeki maddelerle ilgili kullanıcıların rızasını alma amacı taşıyan feragatnamelerdir, yani kişinin haklarından vazgeçtiğinin kanıtı niteliği taşımaktadırlar (Electronic Privacy Information Center, 2022). Telefonlarda bulunan SSA'lar kamera, mikrofon, takvim, kişiler, konum, çağrı kayıtları, metin mesajları, bluetooth gibi birçok özelliğe direkt erişim hakkı ister ve kullanıcı tarafından ayarları değiştirilmediği sürece bu erişimi sağlar (Google Support – Apple/Privacy). Akıllı hoparlör formundaki SSA'lar da benzer özelliklere erişim sağlar ve diğer akıllı ev cihazlarıyla etkileşebilir (Abdi, Ramokapane ve Such, 2019). Bütün bunların kullanıcıya açıklandığı metinler şirketlerin gizlilik politikasını yansıtan bilgilendirme metinleridir. Ancak bu bilgilendirme metinleri genellikle sayfalarca süren, hukuki terimlerle dolu metinler oldukları ve çoğunlukla okunmadıkları için kullanıcılar, sağlanan hizmet karşılığında neleri kabul ettiklerini ve bunun sonuçlarını bilmemekte; servis sağlayıcının onların kişisel verileri üzerinde ne kadar kontrol sahibi olduğunu, bilgilerine ne ölçüde erişildiğini ve bilgilerinin ne amaçla kullanıldığını fark edememektedirler. Bu tez çalışmasının amacı, İletişim fakültesi öğrencilerinin SSA'ların gizlilik politikaları, bu politikaların kişisel veri gizliliği, kullanıcı hakları ve mahremiyetle ilişkisi konusundaki tutumlarını, algılarını ve farkındalıklarını ortaya çıkarmaktır.

Araştırma kapsamında şu sorulara yanıt aranmıştır:

S1: İletişim fakültesi öğrencilerinin SSA'ların gizlilik politikaları konusunda ilgili algıları nelerdir?

S2: İletişim fakültesi öğrencileri SSA'lar hakkında neler bilmektedir?

S3: İletişim fakültesi öğrencileri SSA kullanırken onlara mahremiyetlerinin ihlal edildiğini düşündüren tecrübeler yaşadılar mı?

1.2. Araştırmanın Önemi

Bilişim çağında kişisel verilerin nasıl korunacağını ve güvenlik ihlallerinin ne boyutta tehlikeler yaratacağını bilmek hayati bir önem kazanmıştır. SSA'ların Türkiye'deki kullanımı da gittikçe yaygınlaşmakta olup özellikle COVID-19 salgını sonrası bu oran daha da artmıştır (İçözü, 2020). SSA'lar ve ev tipi akıllı asistanlara dair alanda benzer farkındalık ölçme çalışmaları yapılmış olsa da güncel verilerin çoğu "chatbot" olarak adlandırılan sohbet botlarını ele almaktadır. Araştırmanın önemi, kullanımı gittikçe artan bu teknolojilerin dijital mahremiyet ve veri gizliliği açısından büyük bir güvenlik riski yaratıyor olmasından dolayı, bu teknolojileri kullanan kişilerin kişisel verilerin korunması konusunda bir farkındalığa sahip olması gerekliliğinden ileri gelmektedir. Aynı zamanda SSA'ların bu teknolojinin içine doğan ve dijital yerli olarak adlandırılan Y ve Z kuşağının kullanım pratikleri, veri gizliliği ve mahremiyet konusundaki farkındalıklarını sorgulamaya yönelik bir çalışma bulunmamaktadır. Bu tez çalışmasının bu uygulamaların yaygın kullanımı göz önüne alındığında bundan sonraki çalışmalara katkı sağlayacağı değerlendirilmektedir.

1.3. Araştırmanın Sınırlılıkları

SSA'lar çok farklı yönleriyle incelenebilecek geniş kapsamlı bir konu olmakla birlikte, derinlemesine bir inceleme ve sorgulama yapabilmek için bazı sınırlamalar gerekmektedir. Bu kapsamda araştırmanın veri toplama tekniği araştırmanın amacı doğrultusunda, yarı yapılandırılmış görüşme ile sınırlandırılmıştır. Görüşme yapılacak öğrenciler amaçlı örnekleme çerçevesinde Adana ili Çukurova Üniversitesi İletişim Fakültesi öğrencileriyle sınırlandırılmıştır. İletişim Fakültesi öğrencilerinin seçilmesindeki temel motivasyonlardan birisi aldıkları eğitim doğrultusunda veri gizliliği ve güvenliği konusunda farkındalık geliştirip geliştiremediklerini sorgulayabilmektir. Görüşmeler pandemi koşulları nedeniyle Microsoft Teams

uygulaması üzerinden çevrimiçi olarak gerçekleştirilmiştir. Görüşmelerin yüz yüze gerçekleştirilmesi özellikle açık uçlu soruların yer aldığı ve görüşmenin durumuna göre yeni sorularla görüşmenin zenginleştirildiği derinlemesine görüşmeler açısından önemlidir. Çalışmanın bir diğer sınırlılığı da örneklemin Adana ili ile ve devlet üniversitesi ile sınırlandırılmasıdır. Bu alanda yapılacak daha sonraki çalışmalarda hem özel hem de devlet üniversitelerinin yer aldığı, karşılaştırmaya olanak sağlayacak şekilde örneklem genişletilebilir.



BÖLÜM II

DİJİTAL MAHREMİYET VE KİŞİSEL VERİ GİZLİLİĞİ

Mahremiyet kavramı nesilden nesile hem anlam hem de hayata geçirilme yönünden sürekli değişime uğramıştır. Bu değişim ise kendi içinde kültürel, hukuksal, dinsel ve bireysel anlamda farklılıklar barındırmaktadır. Eski dönemlerde mahremiyet anlayışı çoğunlukla bireyin bedenine ve mülküne yönelikken, bugün bilgi güvenliği ile ilgili bir sorun haline gelmiştir. Çağımızda mahremiyetin korunması gerekliliği birçok ülkede yasalarla ve anayasal haklarla desteklenmektedir. Dünyanın her yerinde, farklı ülkelerin anayasa hukukunda mahremiyet, temel bir hak olarak yer almaktadır (Solove, 2008).

Mahremiyetin zamanla bir norm haline gelmesinde önce şehirleşmenin, yakın tarihte ise teknolojinin etkisi büyüktür. Mahremiyet hakkının hem devlet düzeyinde hem de bireysel düzeyde gelişmeye başlaması sanayileşme sonrası yükselişe geçmiştir. 21.yy'da bilgi toplumunun doğuşuyla bilgisayar, internet ve sosyal medyayla birlikte aktarılan bir düşünce, bireylerin dijital ortamdaki bilgileri de mülkiyet haline gelmiştir (Dinler ve Çalışkan, 2019). Köylerde mahremiyet şehir hayatına göre daha azken, büyük şehirlerde bireysel mahremiyet daha yüksek seviyelerdedir. Aslında gelişen teknolojinin yaşamı tekrar küçük bir köy yaşantısında olduğu gibi mahremiyet sınırlarının daha dar olduğu bir dünyaya taşıdığını söylemek mümkündür (Jagadish, 2016). Bireylerin hayat tarzları, benimsedikleri doğruları, davranış kalıpları gibi mahremiyet algısı da kültüre bağlı oluşur. Kültür, yaşayış biçimini şekillendiren en büyük etkenlerden biridir ve kişinin doğumundan ölümüne kadar etkisini göstermeye devam eder. Özel hayat ve özel hayata dair mahremiyet haklarının meydana geliş sürecinde, birey ve devlet ilişkisi kadar birey ve kültür ilişkisi de büyük önem taşır ve bu ilişkinin etkileri genellikle daha ciddidir, kabul edilmiş bir gerçeği değiştirmek yasal olan bir gerçeği değiştirmekten zordur (Knopp, 2019). Mahremiyet toplum düşüncesinde henüz kavramsallaşmamışken bile, eylem olarak ortaya konmuştur. Din ve kültürün etkileşimi ile ortaya çıkan katı inanç sistemi, mahremiyeti çoğunlukla olumsuz yönde etkilemiştir. İnsanlık tarihi göstermektedir ki, pratikte hayatta kalma ihtiyacı genellikle mahremiyet ihtiyacını gölgede bırakmıştır. Örneğin, köklü bir gelenek olarak modern Kuzey Amerika Eskimo aileleri arasında yalnızlığı tercih eden bireyler toplumdan dışlanmaktadır. Bir gün için bile grubu terk edenler yalnızlık

arzularının bedelini temelli yalnız kalarak ödemektedir (Ferenstein, 2015). Antik Yunan döneminde özel hayat bazen anti-sosyal bir davranış olarak görülse de emeklilik sonrası dönemde kişilerin daha kendilerine dönük bir hayat tarzını benimsemeleri normal kabul edilmiştir (Holvast, 2009). İnzivanın toplumdan uzaklaşmanın makul bir gerekçesi olarak kabul edildiği bir başka topluluk Hristiyan geleneğini benimsemiş topluluklardır. İbadet odaklı bir hayat sürmek isteyen ilk Hristiyan azizler modern mahremiyet kavramına öncülük etmişlerdir (Ferenstein, 2015). Bunların yanında, mahremiyetten yoksun kalmanın daha çekici olduğu toplumlar da olmuştur. Roma halkından zenginlerin evlerinin bahçeleri birer buluşma noktası olarak hizmet etmiş ve bu bir zenginlik göstergesi olarak değerlendirilmiştir (Trueman, 2015).

Mahremiyet tanımının nelere karşılık geldiği kültürden kültüre farklılaşır, hatta aynı kültür içinde farklı anlamlar ifade edebilir. Güney Asya'da düşük gelirli aileler arasında yaygın olarak benimsenen görüş, mahremiyetin yalnızca üst sınıf aileler için var olabileceği, kişisel ve sosyal çevre içindeki sınırların kabul edilebilir olduğudur (Knopp, 2019). Bu toplumlarda sınıfsal farklılıklar, mahremiyetin bir hak mı yoksa bir lüks mü olduğunu belirler.

Bireysellik anlayışının yüksek olduğu ülkelerde bir bireyin mahremiyetinin korunma hakkı sosyal normların bir parçasıdır ve olağandır; aynı zamanda bireyin mahremiyet endişesi daha yüksektir (Thomson, Yuki, Ito, 2015). Buna karşılık, çoğunluğun tercihlerinin, bireyin kişisel haklarından daha değerli görüldüğü toplumlar da vardır. Afrika toplumlarının bazılarının benimsediği Ubuntu felsefesi buna örnek gösterilebilir. Ubuntu, grubun refahının gruptaki tek bir bireyin refahından daha yüksek olduğu bir toplumsal anlayıştır (Mboy, 2019). Böyle bir sosyal anlayış etrafında şekillenmiş bir toplumda veri gizliliğine ihtiyaç duyulmayacağı için, veri gizliliği yasası taslağı hazırlanırken, potansiyel bir gerilim ve çelişki ortaya çıkması söz konusu olabilir (Olinger, Britz, Olivier, 2007). Çünkü bu kültür için bireysel mahremiyet, Batılı mahremiyet anlayışına kıyasla daha az önemli görünmektedir.

Kültürel değerlerin mahremiyet endişeleriyle ilişkilendirildiği birçok güncel çalışma çevrimiçi mahremiyete odaklanmaktadır. Bu durum, günümüzün mahremiyet anlayışının dijitalleşmiş olmasından ve gündelik hayatın kaygılarından çok sosyal medya ortamlarından, e-ticaret alışkanlıklarından doğabilecek tehlikelere karşı duyulan kaygının ön plana çıkmasından kaynaklanmaktadır.

Mahremiyet düşünce özgürlüğü, bireyin bedensel ve kişisel bilgileri üzerindeki kontrolü, kişisel alanındaki hakları, gözetimin dışında kalabilme özgürlüğü, itibarının

korunması gibi birçok durumu içine alan kapsamlı bir kavramdır (Solove, 2008). Mahremiyet kişinin kendini, nesneleri, alanları, bilgileri ve davranışları kontrol edebilme becerisidir (Laufer ve Wolfe, 1977). Bu tanımların vurguladığı ifadeler “özel olan” ve bu özeli olması gerektiği gibi gizli tutmayı sağlayan “kontrol gücü”dür. Mahremiyet, ihlal edilmemiş bir yaşam alanı içinde bireylerin özel hayatlarını yaşayabilme hakkıdır. Kişilerin ya da grupların mahremiyet sınırlarının birinci derece yaratıcıları kendileridir. Bunun yanında bu özgür alan hukukla toplumun geri kalanı tarafından işgal edilmeyecek şekilde korunabilmelidir. Mahremiyet bireyin hak ve özgürlüklere ne kadar oranda sahip olduğuyla doğrudan ilgilidir. James Rachels “Why Privacy is Important (Gizlilik Neden Önemlidir)” adlı makalesinde (1975) bireysel mahremiyet alanının tam olarak neyi kapsadığını ifade ederken, bu alanın sadece belli başlı birkaç özel durumda değil, aynı zamanda gündelik hayatta birçok yaygın ve dikkate değer olmayan küçük eylemlerde dahi korunmaya ihtiyacı olduğunu belirtir. Rachels, bir kişinin patronu ya da ailesi ile kurduğu ilişkinin yanında, birkaç özel kişiyle paylaştığı ya da kimseyle paylaşmak istemediği bütün durumların eşit derecede kişinin kendi rızası ile şekillenebileceğini dile getirir. Mahremiyet kişinin paylaşmaktan çekindiği ya da paylaşmanın ona dezavantaj yaratabileceği bilgileri de içerir fakat bundan çok daha fazlasıdır. Rachels (1975) “Birisi bizim doktorumuzsa, sağlığımızı takip etmek onun görevidir; birisi bizim işverenimiz ise, bize ne kadar maaş ödendiğini bilmek onun işidir. Genel olarak kendimizle ilgili bir gerçek, aramızda onları bilmeye hakkı olan biri varsa, böyle bir sosyal ilişki dahilinde ilgili kişiye sorunsuzca ulaşabilmelidir. Kişiler bu tür ilişkilere girip girmemeyi seçmekte özgürdür ya da olabildiğince fazla mahremiyet sağlamak istiyorlarsa bu ilişkilere isteksizce gireceklerdir.” diyerek mahremiyeti “bize kimin erişebileceğini ve bizim hakkımızda kimin neyi bildiğini kontrol etme yeteneğimiz” olarak tanımlar (s. 3).

Mahremiyetin yoksunluğu gibi, mutlak bir mahremiyet de mümkün değildir. Dolayısıyla mahremiyet sorununu ele alırken, “mahremiyet tehdit edildiğinde neyin tehlikede olduğunu ve bu sorunları çözmek için yasanın tam olarak ne yapması gerektiğini” (Solove, 2008, s. 2) açık ve kesin bir şekilde ifade edebilmek önemlidir. Thomson (1975)’un mahremiyetin sınırlarının nasıl belirlenebileceğini görselleştirmek için sunduğu örnek şöyle özetlenebilir: evinizde biriyle yüksek sesle kavga ettiğinizi düşünün ve bu olurken camlarınız açık, dışarıda ise sizi dinleyen biri var. Bu kişi sizin hakkınızı ihlal etmiyor, davranışını en fazla kınayabilirsiniz. Şimdi bir de bu kavga olurken pencerelerin kapalı olduğunu ve sessiz bir kavga olduğunu varsayın. Fakat

caddenin karşısındaki biri bir aparat yardımıyla evinizi dinliyor, bu sistemi sadece evinizi dinlemek için kullanıyor. Thomson her iki durumun da mahremiyet hakkının ihlali olduğunu dile getirir, ancak bu iki durum aynı yaptırımı hak etmez. Bu örnek bireyin kendi mahremiyeti için önlem almasının ne derece fark yaratabileceğini ifade etmektedir.

2.1. Mahremiyet Tartışmaları

Mahremiyet üzerine ilk kavramsal ve hukuksal anlamda tartışmalar ABD’de II. Dünya Savaşı’ndan bir süre önce başlamıştır (Holvast, 2009). Bu dönemde birçok yayın mahremiyetin ne ifade ettiğini tanımlamaya çalışmış ve mahremiyetin ihlalinin nedenlerini saptamaya yönelik araştırmalar sunmuştur. Bu araştırmaların odak noktasında kullanımı yaygınlaşan bilgisayar teknolojisi yer almaktadır. Mahremiyet tartışmaları, bilgi teknolojisinin yeni bir boyuta taşıdığı özel hayatın ve kişisel verinin gizliliği sorununa bir cevap arayışı olarak doğmuştur. Bu nedenle, 20. yüzyıldan bugüne gizlilik ve veri koruma üzerine süregelen tartışmaları bilgisayarlardan, internetten ve özel bilgilerin toplanması, kullanılması ve paylaşılmasına yönelik birçok diğer teknolojik araçtan ayrı düşünmek imkansızlaşmıştır.

Mahremiyet hakkı üzerine alandaki en eski ve ilk kapsamlı makalelerden biri, Samuel Warren ve Louis Brandeis tarafından 1890 yılında Harvard Law Review dergisinde yayınlanmış olan “Mahremiyet Hakkı (The Right to Privacy)” dır. Makalenin yazılma ihtiyacı, Amerikalıları fotoğrafın ve basının müdahaleciliğinden korumaya yönelik endişeleriden sonra doğmuştur (Lavagnino, 2013). “Basın, her yönden uygunluk ve ahlak sınırlarını aşıyor.” diyen Warren ve Brandeis (1890, s. 196), 1884’te Kodak tarafından geliştirilen şipşak fotoğraf makinelerinin taşınabilir olması ve halka açık alanlarda bile fotoğraf çekebilmeyi sağlamasından dolayı, basının bu teknoloji ile özel hayatın gizliliğini işgal edeceğini öne sürmüşlerdir (Holvast, 2009). Buradaki temel sorun, bu tehditlere karşı alınacak önlemleri içeren ve davranışları düzenlemeye yönelik, başka bir ifadeyle nasıl davranılacağını göstermesi gereken mevcut düzenlemelerin mahremiyeti yasal olarak koruyacak içeriğe sahip olmamasıdır (Holvast, 2009). Warren ve Brandeis, hukukun mahremiyetin korunması için kolaylıkla bir çözüm geliştirebileceğini savunmuşlardır: “Hukuk, her bireyin düşüncelerini ve duygularını başkalarına ne ölçüde iletebileceğini kendisinin belirleme hakkını güvence altına alır.” (Solove, 2006, s. 482).

Mahremiyetin korunmasında hukukun önemini dile getiren bir diğer isim mahremiyet hukuku alanının temelini atan kişi (Holvast, 2009) olarak da kabul edilen Alan Westin'dir. George Washington Üniversitesi Hukuk profesörü Jeffrey Rosen, Westin'i "Louis Brandeis'ten sonra en önemli mahremiyet bilgini" olarak tanımlamıştır (Fox, 2013). Westin, 1967'de yayınladığı "Mahremiyet ve Özgürlük (Privacy and Freedom)" adlı kitabında mahremiyeti şu şekilde tanımlamıştır: "'Mahremiyet bireylerin, grupların veya kurumların kendileri hakkındaki bilgilerin başkalarına ne zaman, nasıl ve ne ölçüde iletileceğini kendileri belirleme iddiasıdır.'" (Westin, 1967, s. 7). Westin, kişilerin kendi bilgilerinin üzerindeki kontrolünün gerekliliğini vurgulayarak, bu bilgilerin ne zaman, kimler tarafından, ne amaçla kullanılacağını ve nasıl korunacağını da yasalarla belirlenmesi ve korunması gerektiğini savunmuştur. Westin, 1972'de yayınlanan "Databanks in a Free Society (Özgür Bir Toplumda Veri Bankaları)" adlı kitabında ise şirketler, çeşitli kuruluşlar ve bizzat hükümet tarafından, kişisel kayıtların dijital ortamda depolanmaya başlanmasını ele almıştır. Ancak verilerin dijitalleşmesini endişe duyulması gereken ve mahremiyeti tehdit eden bir yenilik olarak görmeyerek, yalnızca bu sürecin hukuksal destekle şekillenmesi gerektiğinin altını çizmiştir (Rollenhagen, 2021).

2.2. Dijital Mahremiyet ve Veri Gizliliği

Dijital mahremiyet, bilgi mahremiyeti ile ilişkili olup, bireylerin dijital ortama yansıyan kimliklerinin ve kişisel her türlü bilgilerinin gizliliğini ifade eder. Çevrimiçi ortamlardaki mahremiyet üzerine yapılan tartışmaların önemli bir boyutu, kullanıcıların erişilebilirliği ve anonim kalabilmesi arasında bir denge sağlamak için gizlilik sınırlarının nasıl yönetildiğiyle ilgilidir (Baruh, Cemalcılar ve Seçinti, 2017). Tıpkı toplumla birey arasında yaşanan, belirlenmesi ve uyulması gereken diğer mahremiyet boyutları gibi dijital ortamlardaki mahremiyet endişeleri de bireyin kendi izin verdiği ölçüde görünür olabilmesi, gizliliğinin sınırlarını kendisinin belirleyebilmesi ve bu özgürlüğünün yasalarca desteklenmesi ile ilgilidir. Sharriff, Green ve Jettinghoff'a göre (2021) insanın mahremiyet algısını bozan ve kaygısını besleyen temel sebep, mahremiyetin alanının son otuz yılda, daha önce hiçbir çağda görülmediği kadar hızlı bir çevresel değişim yaşamış olmasıdır. Dijitalleşme, insanın yüzyıllardır kendi sosyal alanında kurmuş olduğu mahremiyet dengesini bozmuştur. Dolayısıyla insanlık hala dijital mahremiyet psikolojisine adapte olma sürecindedir. Diğer yandan bireylerin

kişisel bilgilerinin güvenliğinin ne derece suistimal edileceği kâr amacı güden şirketler, hükümetler ve teknolojiyi kontrol edebilme becerisi daha yüksek bir kesimin insafına kalmıştır. Fakat önemli olan bireylerin mahremiyetlerini koruma içgüdüsünün çevrimdışı hayatta olduğu gibi çevrimiçi dünya içinde de aynı oranda keskinleşmesi ve güvenliğinin bu ihlallere ne derece maruz kaldığının farkında olabilmesidir. Bilgi toplumunun bir parçası olmak, dijital dünyada daha da kıymetlenen bilginin ve kişisel verilerin korunmasını sağlamayı gerekli kılar. Bu güvenliği sağlama konusunda bireyin çabası ancak doğru ve etkili yasal düzenlemelerle sonuç verebilir. İçinde bulunduğumuz dijital çağ ise kişisel mahremiyet ve verilerin korunması konusunda yeni zorlukları beraberinde getirmiştir (Shariff, Green ve Jettinghoff, 2021).

Genel bir tanımla kişisel verilerin korunması, kişiye özel verilerin veri sorumluları ve bu verileri işleyenler tarafından kullanılması halinde kişilerin mahremiyet haklarını güvence altına alma yükümlülüğüdür (Romansky, 2017). Kişisel verileri işleyen tüm kişi ve kuruluşlar bu eylemi yasal yollarla düzenlenmiş bir veri koruma politikası çerçevesinde yürütmelidir. Bu amaçla gizlilik politikasında verilerin hangi amaçla toplandığının açıkça belirtilmesi, verilerin ne kadar saklanacağı, kullanıldıktan sonra ya da kullanıcı verilerini silmek istediğinde verilerin gerçekten veri havuzundan silinmesi, kullanılan platformun ağ güvenliği yönünden gereken önlemleri almış olması gibi mutlaka uyulması gereken yasal zorunluluklara dikkat edilmelidir.

2.3. Dijital Çağda Kişisel Veri

İnternet bağlantılı teknolojiler, çevrimdışı dünyamızda zaten belirgin ve önemli bir sorun haline gelmiş olan daha fazla bilgi toplama eğilimini beslemektedir. Dönemin bilgi toplumunda maddi bir üründen çok bilgi üretmek, çoğaltmak ve pazarlamak değer kazanmıştır (Aktaş, 2007). Bu nedenle öncelikli olarak teknoloji çağının nasıl bir dijital dünya yarattığını, bireyin bu dijital dünyada “kullanıcı” sıfatıyla gerçek kimliğinin ne kadarını sanallaştırdığı ve bu sırada gizliliğini koruyabilmek adına ne gibi araçlar ve yasalar kullanabileceğini iyi belirlemek gerekir.

Geçmişte bilgilerin en iyi saklandığı yerler olan kütüphaneler, arşivler ve kişisel kitaplıklar bilginin korunma şansını artırmaktayken, bilginin yayılması ise günümüze göre çok kısıtlı ve yavaş bir süreç olmuştur. İnternet ağlarında bulunan bilgi ise küresel çapta, olağanüstü derecede hızlı bir şekilde yayılmaktadır. Çoğunlukla evde kullanılan kablolu internetin hızı saniyede gigabit (Gbps) indirme hızına, 1.000 Mbps’e

ulaşılabilmektedir (Anders, 2021). Üstelik son mevcut teknoloji fiber, eski internet bağlantı türlerinde yaygın olan hız sorunlarından etkilenmeden birkaç alanda 10.000 Mbps'ye varan hızlara sahip olabilmektedir (Holslin, 2021). Fakat internet ağında bulunan her türlü bilgi sürekli olarak tehditlere açık haldedir. Çünkü paylaşım dijital ortamda çok daha belirsiz ve rastgele bir süreç haline gelmiştir ve hangi bilginin kimler tarafından görüntülenebildiğini tahmin etmek neredeyse imkansızdır.

İnternet ve sosyal ağların etkinlik alanı artıkça, kişilerin ve mekanların da sanallaşmaya uyum sağlama ihtiyacı doğmuştur. Teknolojinin günlük hayatın içinde kullanımı bir tercihten zorunluluk haline dönüşmüştür. Dijital iletişim ağları yeni toplumsal yapının uyulması zorunlu unsurları haline gelmiştir ve her türlü bilgi bu ağların mümkün kıldığı ölçüde dünyanın her noktasına yayılabilmektedir (Castells, 2005). “Ağ toplumu” olarak adlandırılan bu yeni toplumsal yapının içerisinde internet yeni bir kamusal mekân, bir gerçeklik ve ekonomik bir pazar var etmiştir ve bireyler, sosyal gruplar bu dijital kültürün bir parçası olabilmek için sanal kimliklere ihtiyaç duymaktadır (Güzel, 2006). Russell W. Belk tarafından ortaya atılan ve kişinin sahip olduğu metalarla kişiliğini ilişkilendiren genişletilmiş benlik teorisi (1988, s.140) kişinin benlik duygusunun bir şeylere sahip olarak tatmin olabildiğini söyler. Bu teori 2013 yılında Belk tarafından dijitalleşmenin etkileri göz önüne alınarak güncellenmiştir. Belk dijital dünyada yer alan ve maddi olmayan öğeler için “Bu öğeler uzak bir sunucuda depolanıyorsa, gerçekten bizim mi? Yoksa fiziksel sahiplik, dijital öncesi düşüncenin bir parçası mı?” sorusunu sorar (2013, s.479). Araştırma göstermektedir ki, dijital nesneler de en az maddi nesneler kadar kabul görmektedir ve benliği tatmin etmektedir. Benlikler artık dijital dünyanın içinde avatarlar aracılığıyla temsil edilmekte olup, tüm kişisel bilgiler bu dünyaya maddi dünyada olduğuna benzer bir şekilde aktarılmaktadır. Sanal kimlikler kullanıcıların gerçek kimliklerinin sanal yansıması olabileceği gibi kişinin kendi isteğiyle oluşturduğu, gerçek kimliğin idealize edilmiş bir hali de olabilir (İsmayılzade, 2017). Her iki durum da kullanıcıların paylaşmaya rıza gösterdikleri, bazen daha fazlasını hatta kimi zaman erişilebildiğinin farkında bile olmadıkları birçok kişisel bilgiyi erişilebilir kılar. Bunun nedeni bu bilgilerin birer dijital veri parçası formunda çeşitli veri tabanlarına kaydediliyor olmasıdır (Weaver ve Gahegan, 2007). Bu veri parçaları “dijital ayak izleri” olarak adlandırılır. Bu izler internet kullanımının yaygınlaşması önderliğinde web siteleri, sosyal medya, internet bağlantısı teknolojisine sahip cihazlar gibi verilerin depolanmasına imkân tanıyan veri tabanlarının bulunduğu ortamlardaki kullanıcılara ait her türlü verinin kalıntısıdır.

“Hassas veri” olarak da adlandırılan özel nitelikli kişisel veriler 6698 sayılı Kişisel Verilerin Korunması Kanunu’nun 6.maddesinde (KVKK, 2016) belirtildiği üzere “kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verilerini” kapsayan, açığa çıkarıldığında kişinin özlük haklarına ve mahremiyetine zarar verebilecek düzeyde bilgilerdir. Günümüzde birçok çeşitli çalışma alanlarında kullanıcıların ve müşterilerin verilerinin saklanması ve şirket yararına işlenmesi büyük önem taşımaktadır.

Hukuk profesörü Jon Mills, “Bireysel mahremiyetten geriye ne kaldı ve nasıl kurtarılabilir” sorusunu sorarken şunları dile getirmektedir: “Bugün büyük veri ihlalleri pratikte günlük bir olay haline geldi. Bireyler etkisiz yasaların olduğu bir dünyada risk altındadır” (Mills ve Harclerode, 2018, s.773). Mills (2009), kişisel mahremiyete dair yeterli korumanın sağlanabilmesi için, mevcut uygulamaların yeniden değerlendirilmesi ve kapsamlı politika değişikliklerinin yapılması gerektiğini savunur.

2.4. Kişisel Verilerin İşlenmesinde Genel İlkeler

Bireyin mahremiyetinin korunması hakkı, “özel yaşama saygı hakkı” kapsamında yasalarca güvence altına alınmıştır (Öncü, 2019). Bu bireysel hakkın bir yönü de “kişisel verilerin korunması hakkı”dır. Kişisel verilerinin gizli ve güvende kalması kişinin temel hak ve özgürlüklerinden biridir ve devletin sorumluluğu altındadır. Verilerin toplanması, depolanması, kullanılması gibi eylemler “kişisel verilerin işlenmesi” olarak tanımlanır. Bugün birçok ülkenin anayasasında kişisel verilerin korunması hususunda düzenlemeler mevcuttur. Kişisel veriler, yalnızca yasalarca belirtilen gerekçeler kapsamında ve direkt kişinin açık rızası alınarak işlenebilir. Kişisel verilerin işlenmesi konusunda ilk hukuksal düzenlemeler internetin henüz doğduğu dönemler sayılan 1970 yılında, Almanya’nın Hessen eyaletinde yürürlüğe konulmuştur (Stepanova ve Jechel, 2021). Dünyanın ilk veri koruma yasası olarak kabul edilen bu yasanın amacı verilerin korunması karşılığında teknolojik gelişmeleri kısıtlayıcı nitelikte kurallar getirmek değil, bu işlemlerin sadece yetkililer tarafından yasal yollarla yapılmasını hukuk yoluyla desteklemektir (Küzeci, 2010). Avrupa genelinde onaylanan ilk yasal anlaşma ise 1981’de Avrupa ülkeleri tarafından imzalanan ve 1985’te yürürlüğe giren “Kişisel Verilerin Otomatik İşleme Tabi

Tutulması Karşısında Bireylerin Korunması Sözleşmesi”dir (Long, Raul, Blythe ve Kara, 2021). Her ne kadar imza aşamasında katılım gösterilmiş olsa da anlaşma o dönemde yalnızca Türkiye tarafından onaylanmamıştır ve Türkiye anlaşmaya 2016 yılında katılım sağlamıştır (Küzeci, 2010).

Avrupa’nın kabul ettiği kişisel veri anlayışına göre “kişisel veri, bir kişiyi özellikle bir kimlik numarasına veya fiziksel, fizyolojik, zihinsel, ekonomik, kültürel veya sosyal kimliğine özgü bir veya daha fazla faktöre atıfta bulunarak doğrudan veya dolaylı olarak tanımlayan bilgilerdir” (Romansky, 2017, s. 99). 2016’da Avrupa Parlamentosu tarafından onaylanarak kabul edilen ve 25 Mayıs 2018 tarihinde yürürlüğe giren Avrupa Birliği Genel Veri Koruma Tüzüğü (GDPR) ise Avrupa’da kişisel veriye dair hazırlanmış olan son güncel anlaşmadır. GDPR, Avrupa’da Avrupa Birliği üyesi vatandaşların veya geçici ikamet edenlerin kişisel verilerinin korunmasına yönelik bir yasal düzenlemedir. Yasa tüzüğünde belirtildiği üzere “isim, fotoğraf, e-posta, banka detayları, sosyal medya hesapları, tıbbi bilgiler, sosyal güvenlik bilgileri, pasaport bilgileri, bilgisayarın IP adresi gibi kişiyi doğrudan ya da dolaylı yollarla tanımlamaya yardımcı olacak veriler ve tarayıcıların topladığı çerezler (cookie)” GPDR ile kişisel veri kapsamına girmektedir ve bu kişisel verileri kullanan her kurum bu yasalara uymak zorundadır. (Toplumsal Bilgi ve İletişim Derneği, 2018).

2.4.1. Türkiye’de Kişisel Verilerin Korunması

Türkiye’de kişisel verilerin korunmasına dair hazırlanan düzenlemelerin geçmişine bakıldığında ilkinin 2004 yılında kabul edilen ve 2005’te yürürlüğe giren 5237 sayılı Türk Ceza Kanunu’nda yer aldığı görülmektedir. Kanunun “Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar” başlıklı Dokuzuncu Bölümü’nün 135. ve 140. maddelerinde kişisel verilerin korunmasına ilişkin suçlar ve bu suçların gerçekleşmesi sonucu uygulanacak çeşitli yaptırımlar belirtilmiştir (Kart ve Ketizmen, 2019).

Türk Ceza Kanunu’nda yer alan söz konusu maddeler şunlardır:

Madde 135- Hukuka aykırı olarak kişisel verileri kaydeden kimseye bir yıldan üç yıla kadar hapis cezası verilir. Kişisel verinin, kişilerin siyasi, felsefi veya dini görüşlerine, ırki kökenlerine; hukuka aykırı olarak ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin olması durumunda birinci fıkra uyarınca verilecek ceza yarı oranında artırılır (2004, s. 9001).

Madde 140- Madde 140- (1) Yukarıdaki maddelerde tanımlanan suçların işlenmesi dolayısıyla tüzel kişiler hakkında bunlara özgü güvenlik tedbirlerine hükmolunur (2004, s. 9002).

2010 yılında Kişisel Verilerin Korunması ile ilgili hazırlanan hüküm T.C. Anayasası'na dahil edilmiştir. KVKK'da belirtildiği üzere bu değişiklikle birlikte Anayasa'nın 20. maddesine bir fıkra eklenmiş ve böylece kişisel veriler, "özel hayatın gizliliği ve korunması hakkı" kapsamında kabul görmüştür.

Özel hayatın gizliliğine dair 20. maddede belirtilen:

Madde 20– Herkes, özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahiptir. Özel hayatın ve aile hayatının gizliliğine dokunulamaz (2001, s.3).

Bu ifadeye şu ek fıkra dahil edilmiştir:

“(Ek fıkra: 7/5/2010-5982/2 md.) Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir” (2010, s.2).

Mart 2016'da Türkiye'nin 1981'de imzalamış fakat onay vermemiş olduğu 108 No'lu Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi Türk hukukuna dahil edilmiştir. Nisan 2016'da 6698 sayılı Kişisel Verilerin Korunması Kanunu 29677 sayılı Resmî Gazete'de yayımlanarak yürürlüğe girmiştir. Mayıs 2016'da ise 181 No'lu Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi'ne Ek Denetleyici Makamlar ve Sınıraşan Veri Akışına İlişkin Protokol Türk hukukuna dahil edilmiştir.

KVKK'da belirtilmiş olduğu üzere, kişisel verilerin işlenme sürecine dair birçok ülkede uygulanan bazı temel ilkeler söz konusudur. Ülkemizde bu ilkeler “Kanunun 4. maddesinde kişisel verilerin işlenmesine ilişkin usul ve esaslar 108 sayılı Avrupa Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesine ve 95/46/EC sayılı Avrupa Birliği Veri Koruma Direktifine paralel şekilde” düzenlenmiştir (KVKK).

Kanunda belirtilmiş olan, kişisel verilerin işlenmesi konusunda zorunlu sayılan genel ilkeler aşağıda KVKK'nın sunmuş olduğu şekilde sıralanmıştır (Madde 4, 2016):

- Hukuka ve dürüstlük kurallarına uygun olma,
- Doğru ve gerektiğinde güncel olma,
- Belirli, açık ve meşru amaçlar için işlenme,
- İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma,
- İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme.

2.5. Kişisel Veriler Neden ve Nasıl İşlenir?

Teknoloji şirketlerinin kişisel verilere ihtiyaç duyması temelde geliştirdikleri teknolojileri iyileştirmek, kullanıcıyı daha iyi tanımak ve böylece ona daha iyi hizmet vermek amacından kaynaklanmaktadır. Kullanıcıyı doğru analiz etmek şirketler için daha hızlı ve daha doğru sonuçlar getirir, bu da kazanç demektir. Bilgi bir metadır. Şirketler bu verileri satın alır veya bir bulutta kaydeder; böylece bir veri havuzu oluşturulur. Bu veri havuzundaki bilgilerle bir bireyin kimliğini, faaliyetlerini ve beğenilerini gösteren bir profil oluşturabilir (Berman ve Mulligan, 1999). Şirketler tarafından kullanılan ve büyük verinin kaynağını oluşturan veriler, çoğu zaman bireylere ait kişisel bilgilerle oluşturulmaktadır (Richterich, 2018). “İsim, sosyal güvenlik numarası gibi bireyleri açık bir şekilde belirleyen özellikler kimi zaman silinse de bu veri tabanları bazen posta kodu, cinsiyet ve doğum tarihi gibi özellikler üzerinden kullanıcıyı tekrardan belirlemek için diğer açık veri tabanları ile” bir araya getirilebilirler (Eyüpoğlu, Aydın, Sertbaş Zaim ve Öneş, 2017, s. 177). Araştırmalar, veriler ilk etapta anonim olarak işlense bile, birbirleriyle eşleştirildikleri anda ait oldukları kişilerin belirlenebildiğini işaret etmektedir (Akıncı, 2019). Bu analizler sayesinde, tüketici davranışından kullanıcının bir sonraki işlemlerini, hareketlerini tahmine dayalı algoritmalar gibi birçok sistemi geliştirmek için, şirketler her gün büyük miktarlarda nicel ve nitel verileri düzenli olarak depolamakta ve analiz etmektedir (Freedman, 2020). Lyon’un (2013) ifade ettiği gibi, “Güvenlik artık geleceğe dönük bir projeye dönüşmüştür ve gelecekte olacak şeyler dijital teknikler ve istatistiksel akıl yürütme sayesinde denetlenmeye ve tespit edilmeye çalışılmaktadır” (s. 16).

İnternet kullanıcıları, bağlantı sırasında tarayıcılarını kullandıkları her an tarayıcı ve bilgisayar arasında birtakım veri alışverişi gerçekleşir. Bilgisayara kaydedilen önbellek bilgileri ve çerezler kullanıcı deneyimini iyileştirmeyi sağlar (Grustniy, 2019). Google’ın verdiği bilgilere göre iki tür çerez vardır. Bunlar, ziyaret edilen internet sitesi

tarafından oluşturulan ve üçüncü taraf çerezler olarak bilinen, diğer siteler tarafından oluşturulan çerezlerdir. Telefon uygulamalarında da benzer bir süreç vardır, Apple'ın belirttiği üzere ortalama bir uygulamada altı “izleyici” bulunur. İzleyici, çerezlerin izini sürebilmeye yarayan sistemlerdir ve amaç üçüncü taraflarla paylaşılacak verileri derlemektir.

Derlenen veriler veri tabanlarında saklanmaktadır ve günümüzde kaynağa doğru olağanüstü bir hızla veri akışı olduğu düşünülürse bu veriler oldukça fazladır. Bu dosyalar çok büyük boyuttadır ve bu verilerden faydalı bilgiler çıkarabilmek zor bir süreçtir; buna “veri madenciliği” denir. Bu veriler günümüzde çoğunlukla dijital teknolojilerle elde edilmekle birlikte “kişisel her türlü bilgi, sosyal medya hareketleri, sağlık kayıtları, telefon kayıtları, hükümet kayıtları” (Boyd ve Crawford, 2012, s. 673) gibi birçok farklı koldan bilgiler havuzda yer alır. Birçok farklı disiplinden faydalanan veri madenciliği; “istatistik, makine öğrenmesi, yapay zekâ, görüntü tanıma” alanlarını kullanır (Emre ve Erol, 2017, s. 163).

Kişisel verilerin kullanılmasının etik yolları olduğu gibi, şirketler öncelikle varsa güvenlik açıklarını ya da güvenlik risklerini kabul etmeli ve sistemler üzerinden veri toplama ve arşivleme eylemlerini sınırlamalı ya da anonimleştirmelidir. Jan van Dijk “Ağ Toplumu” kitabında (2016) kullanıcının haklarını ihlal etmeyen tasarımların mümkün olduğundan söz etmektedir. Öncelikle uygulamalar tek bir hedef doğrultusunda, sadece o amaca yönelik verileri derlemelidir. Ayrıca verilerin anonim kalabilmesi sağlanmalıdır. Yapay zekâ destekli akıllı cihazların makine öğrenimi yoluyla kullanıcı ile etkileştikçe gelişiyor olması bu cihazların diğer birçok teknolojik araçtan daha çok ve daha kolay veri derlemesinin önünü açmıştır. Bu sistemlerin insan etkileşimi yüksek olsa da ve kimi zaman gerçek bir insan algısı yaratsalar da kullanıcının kişisel verilerinin kaybı ve ihlali gibi ciddi güvenlik riskleri barındırmaları onları pek de kullanıcı dostu kılmamaktadır. Makine öğrenimindeki temel sorun, gizlilik ve öğrenim mekanizması arasındaki ilişkinin nasıl kurulacağıdır. Bir yandan, günlük veri kayıtlarının fazlasının depolanmasına yani gizlilik kaybına izin verilmemelidir. Öte yandan, sistemin derlediği orijinal verileri kullanarak öğrenmesine izin verilmelidir, bu da fayda kazancını ifade etmektedir (Chew, Wong ve Ooi, 2018). Verilerden otomatik olarak öğrenen yapay zekâ sistemleri daha nesneldir ve genellikle sonuçları teori odaklı oluşturulan modellerden daha iyi tahmin edebilirler (Mooney ve Pejaver, 2018). Otomatik öğrenen bir yapay zekâ modeli, kullanıcı kişinin günlük hayatındaki hemen hemen her bilgiyi hafızasına kaydedip işleme potansiyeline sahiptir. Bu bilgiler,

kullanılan akıllı cihazın hafızasını oluşturmakla sınırlı kalmamakta, cihazın üreticisi şirkete (Apple, Google, Amazon vs.) aktararak depolanmakta ve işlenmektedir; zira bu cihazlar yalnızca kullanıcıya hizmet etmekle kalmamakta, yaratıcı şirketlerine de hizmet etmektedir (Guzman, 2017).

2.6. Dijital Çağda Kişisel Verilerin Gizliliği, Güvenliği ve Korunması

Kişisel bilginin gizliliği, teknoloji sonrası doğmuş bir kavram değildir; fakat teknoloji etkisiyle çeşitlenmiş, kapsamı genişlemiş bir kavramdır. Tarih boyunca tüm toplumlar için kişinin özelini bilmek değerli olmuştur. Bu ihtiyacın, tehlikeyi önceden bilmek ve korunabilmek, toplumu analiz edebilmek ve çıkarımlarda bulunabilmek, otoritelerce duyulan denetim ve kontrol edebilme arzusu gibi birçok sebebi olmuştur. Sonuçları ise gözetim araçlarıdır. Dijital teknolojilerin yaygınlaşması, gözetleme eyleminin sağlanabileceği araçları çeşitlendirmiştir ve bunlar zamanla bireyin günlük hayatının bir parçası haline gelmiş, birey tarafından içselleştirilmiştir (Bauman, 2013).

Kişisel verilerin korunması hakkı mutlak bir hak olmadığı için, müdahalelerin hangi durumlarda bir ihlale dönüştüğüne mahkeme karar vermektedir (Öncü, 2019). Yine de kullanıcı farkındalığı ve bilgilendirme metinlerinin hukuki kavramsal ifadelerle dolu uzun metinler olmasına rağmen okunup anlaşılması çok önemlidir. Kişisel verilerin yalnızca kişinin izni dahilinde işlenebileceği Kişisel Verilerin Korunması Kanunu (KVKK) Madde 8’de (2016, s.3) “Kişisel veriler, ilgili kişinin açık rızası olmaksızın aktarılamaz.” ilkesiyle belirtilmiştir. Bilgilendirme metinleri adından da anlaşılacağı üzere kişiyi bilgilendirmeye yönelik gibi görünse de aslında mahkeme ya da hukuk alanındaki kişiler tarafından anlaşılması ve kullanılması için yazılmış metinlerdir (Koene, 2016). Oysa bu metinlerin içeriğinde belirtilen maddelerin kullanıcı tarafından okunmadan kabul edilmesi web tabanlı hizmetlere ve üçüncü şahıslara kullanıcı kişinin verilerini saklama, analiz etme ve satma hakkı verir. Bu metne onay vermek olası bir durumda kişilerin mahkemeye gitme haklarını ellerinden almaktadır (Berreby, 2017).

İnternet kullanıcılarına kullandıkları cihazların, internet aracılığıyla geliştirici şirketler için veri topladığını ve bunun sonuçlarının neler olabileceğini ifade edebilmenin en kısa yolu, bir onay butonunu tıklamadan önce kullanıcıya sunulan gizlilik politikalarıdır. Açıkça rıza gösterilmediği durumlarda elde edilen verilerin kullanımı yasal olmadığı gibi, kullanıcının mahremiyeti ve gizliliği açısından tehlike yaratmaktadır. Bu nedenle kişisel verilere erişim sağlayabilen tüm siteler, uygulamalar

ve geliştirici şirketler hangi kişisel verilerin ne amaçla paylaşılacağı konusunda ilgili kişileri bilgilendirmekle yükümlüdür (Erdinç, 2017). Ancak kullanıcılar kişisel bilgilerinin önemsiz olduğuna ve kimsenin ilgisini çekmeyeceğini düşünmeye yatkındır. Bunun yanında, kullanıcılar için gizlilik politikalarını okumak zor olsa da bu şirketlerin etkili bildirim sağlama ve gizliliği kontrol etme sorumluluğunu azaltmamaktadır. Pasquier, Singh ve Powles (2017, s. 4) yürüttükleri bir çalışmada bu metinlerin hazırlanırken üstlendiği bir dizi veri koruma kanunu yükümlülüklerine ilişkin ilkeler şöyle özetlenebilir:

- Şeffaflık: Gizlilik politikaları, kullanıcıları “veri işleme amacına dair, verilerin satıldığı kaynaklara dair ve hassas verilerin kullanımına dair bilgilendirmekle” yükümlüdür. Bunun sonucunda kullanıcıların kişisel bilgilerine erişim ve hizmete son verme hakları bulunmaktadır.

- Güvenlik: Şirketler gizlilik politikalarında belirttikleri doğrultuda “kişisel verileri korumak için gerekli önlemleri uygulamak ve gizliliği garanti etmekle” yükümlüdür.

- Kullanıcı haklarının etkinleştirilmesi: Kullanıcının “ham verilere ve verilerinin nasıl işlendiği bilgisine erişim hakları bulunmaktadır ve şirketler bu hakları kullanıcı talep ettiğinde onlara anlaşılır bir şekilde sunmakla yükümlüdür”. Ayrıca toplanan kişisel verilerin değiştirilmesi ve silinmesini talep etme hakları veya tüm kişisel veriler üzerinde belirli bir hizmeti durdurma hakları mevcuttur. Gizlilik politikaları bu haklara uyulup uyulmadığını ve veri akışlarının denetiminin ne derece sağlandığını göstererek kullanıcıyı aydınlatmalıdır.

BÖLÜM III

SESLİ SANAL ASİSTANLAR

Dijital çağda insanların sonsuz ihtiyaçlarına karşılık verebilmek için teknoloji şirketleri daima kendilerini yenilemektedir. Günümüzde özellikle iletişim teknolojilerinde hızlı bir gelişme söz konusudur. Bu gelişmeler, kullanıcı için büyük kolaylıklar sağlarken aynı zamanda dijital araçların kullanımı konusunda bilinçsiz kullanıcılar için büyük riskler barındırmaktadır. Özellikle internet bağlantılı araçlarla, kişisel veriler kullanıcının bilgisi ve izni olmadan üçüncü taraflarca görüntülenebilmekte, kopyalanıp arşivlenebilmektedir. SSA'lar da 2010'lu yılların başından itibaren bu araçların en popüler örneklerinden biri olmuştur. SSA'lar, kullanıcıların davranışlarını ve isteklerini yapay zekâ destekli makine öğrenimi doğal dil işleme teknolojileri aracılığıyla kavrayan ve bu sayede çeşitli görevleri yerine getirme kabiliyetine sahip teknolojilerdir (Canbek ve Mutlu, 2016). Bu asistanların kullanımının yaygınlaşması kullanıcı güvenliğine ilişkin bazı sorunları da beraberinde getirmiştir. Örneğin mobil telefonlarda ve akıllı hoparlörlerde bulunan uygulamalar kullanıcılara sesli, görsel ve yazılı hizmetler sunduğu için güvenilir bir gizlilik politikasına sahip olmaları şarttır. Geliştirici şirketlerin alacağı önlemler ve tehlikeler konusunda kullanıcıyı bilgilendirme zorunluluğu tek başına yeterli değildir. Kullanıcılar da bu araç ve uygulamaların gizlilik ve güvenlik ayarlarını doğru bir şekilde bilmeli ve kullanmalıdır (Geambasu, Kohno, Levy, 2009).

Bu bölümde SSA sistemlerinin temelinde bulunan teknoloji olan yapay zekanın geliştirilme süreci anlatılmıştır. Daha sonra SSA'lar ve çalışma sistemleri açıklanmıştır. SSA'larla temel farklılıkları olmasına rağmen çok sık birbirlerinin yerine kullanıldıkları sohbet botlarının neler olduğuna değinilmiştir. Ardından tez çalışmasının ana problemi olan kişisel veri gizliliği konusu SSA'lar üzerinden ele alınmıştır. Kullanıcıların bu asistanları ev ortamlarında kullanmaları veya sürekli olarak yanlarında taşıdıkları akıllı telefonları aracılığıyla kullanıyor olmalarının sonucunda akla gelen temel sorulardan olan “bu uygulamaların arkasındaki şirketlerin gizlilik politikaları neleri içermektedir” sorusu yanıtlanmak istenmiştir.

3.1. Yapay Zekâ Teknolojilerinin Doğuşu

İnsanoğlu antik çağlardan bu yana, insanın en benzersiz özelliği sayılabilecek olan zekayı keşfetme merakı duymuştur. Antik Yunan, Antik Mısır ve Çin İmparatorluğu dönemlerinde, insan zekasını taklit eden, akıllı makinelerin ilk örnekleri sayılabilecek ilkel mekanik sistemler yapıldığı bilinmektedir (Gonsalves, 2018). İnsanlık tarihi boyunca sembolik bir şekilde yorumlanan, düşünce sisteminde şekillenen yapay zekâ ve yapay zekâ temelli teknolojik sistemleri geliştirme süreci ise 1950'lerde başlamıştır. Araştırmaların temel hedefi, zekanın çalışma prensiplerini anlamak ve bu sayede makineleri daha donanımlı hale getirmek için benzer bir sistem geliştirebilmek olmuştur (Hunt, 1986). Bu hedefe giden başlıca çözüm yollarından biri de bilgi çağının en büyük icadı sayılabilecek bilgisayarları daha fazla bilgi depolamaya uygun, hızlı ve erişilebilir hale getirme isteğidir. Yapay bir zekaya sahip sistemlerin henüz ismi konulmadan önce, bu alanda cevaplar arayan önemli bir isim Alan Turing'dir. İnsanların problem çözmede makinelerden farklı olarak sadece aklı değil belleği de kullandıkları savından yola çıkan Turing (Anyoha, 2017), Turing makinesi fikrini ortaya atmıştır. Turing'in 1950 tarihli "Hesaplama Mekanizması ve Zekâ (Computing Machinery and Intelligence)" makalesinde bahsettiği ve mantıksal çerçevesini kurduğu bu makine, günümüz bilgisayarlarının atası sayılabilecek, bilgisayarın çalışma prensibini en basit haliyle yansıtan bir hesap makinesidir. Talimatları uygulayan bir çalışma prensibi olan bu makinenin en önemli ve ayırt edici özelliği, sonuçları saklayabileceği bir belleğe sahip olmasıdır. Bu basit bellek sistemi, bir veri bandına sahiptir. Bu veri bandı aracılığıyla işlemler semboller halinde banttan okunur ve banda yazılır (Strawn, 2014). Aynı makalede Turing, "Turing testi"nden de ilk kez bahsetmiştir. Turing testi, Turing'in bir makinenin zekâ derecesini ölçmek için geliştirmeyi planladığı bir sistemdir. Teste göre bir insan zeki bir makine ile karşı karşıya gelecektir ve karşılıklı diyalogların sonucunda eğer kişi karşısındakinin bir makine mi yoksa başka bir insan mı olduğunu ayırt edemiyorsa, bu makinenin zekasını kanıtlayacak ve test geçilmiş sayılacaktır. Turing testi, zekayı gerçekten değerlendirmeyip, sadece bir bilgisayarın bir insanın sorulara yanıt verme şeklini taklit etme yeteneğini kanıtlıyor olduğu gerekçesiyle eleştiriler almıştır (Walczak, 2018).

Yapay zekâ sistemlerinin geliştirilmesi sürecinin öne çıkan ilk örnekleri incelendiğinde karşılaşılan ilk ve önemli projelerden biri 1952'de geliştirilen ve temel sesleri tanıma özelliği sayesinde bilindik sesleri %90'a kadar doğru tanıyan Audrey

isimli sistemdir (Pinola, 2011). Audrey, sıfırdan dokuza kadar rakamların sesini algılayabilmektedir; fakat bunun için gereken elektronik sistem bir odayı kaplayacak büyüklüktedir (Moskvitch, 2017). Bir sonraki önemli örnek, IBM tarafından 1962'de geliştirilen Shoebox'tır. Shoebox, 16 kelimeye kadar anlayabilmiş ve sesli komut yoluyla matematiksel işlemler yapabilmeyi başarmıştır. Diğer bir doğal dil işleme programı, 1966'da Massachusetts Teknoloji Enstitüsü tarafından geliştirilen ELIZA'dır. Program bilinen ilk sohbet botlarından biri olup, insan-bilgisayar etkileşiminin yetersizliğini kanıtlamak üzerine geliştirilmek istenmiştir; ancak basit komutlara hazır yanıtlar verebilme yeteneği ile dönemin kullanıcılarını heyecanlandırmıştır (Ronkowitz, 2017). Ardından ARPA'nın (ABD'nin Savunma Bakanlığına bağlı Gelişmiş Araştırma Projeleri Dairesinin o dönemki adı) konuşmayı anlama üzerine beş yıl süren araştırmaları sonucu 1971'de geliştirdiği ve üç yaşındaki bir çocuğun kelime dağarcığı (yaklaşık 1011) kadar kelimeyi tanıyabilen Harpy bu teknolojinin ilk örneklerinden sayılmaktadır (Lowerre ve Reddy, 1976).

O yıllarda yapılan araştırmalar ses tanıma ve doğal dil işleme ile başlamış ve sanal bir asistan yaratmaya giden yolun ilk adımları olmuştur. Bu adımların atıldığı yer, tarihe "yapay zekâ" teriminin doğduğu yer olarak geçen, 1956'da Dartmouth Koleji'nde düzenlenen Dartmouth Yapay Zekâ Yaz Araştırma Projesi (The Dartmouth Summer Research Project on Artificial Intelligence)'dir (Kline, 2011). Katılımcılarının etkilendiği isimler, Avrupa'da sibernetik biliminin kurucusu kabul edilen matematikçi Norbert Wiener, yapay nöronlar üzerinde çalışan nörofizyolog Warren McCulloch gibi, erken dönem makine zekâsı üzerine düşünen ve fikir üreten bilim insanları olmuştur. Projeyi organize eden ve yapay zekâ teriminin yaratıcısı kabul edilen bilgisayar bilimci John McCarthy aynı zamanda LISP adlı, alanda ilk olan ve bugün hala kullanılan yapay zekâ programlama dilinin de tasarımcısıdır (Chang, 2020). O yıllarda bilgisayarların yapay bir zekaya sahip olamayacağı düşüncesinin arkasında bilgisayarların verilen komutları depolama gibi bir özelliği bulunmaması ve komutları yerine getiren bilgisayarların, bu komutları daha sonra hatırlayacak bir hafızaya sahip olmaması yer almaktadır (Anyoha, 2017). Bu da araştırmaları finansal anlamda destekleyecek isimler bulmayı zorlaştırmıştır. Dartmouth Projesi'nin başarısı, katılımcıları yapay zekâ teknolojisinin hayata geçirilebilir ve yaygınlaşabilir olduğuna ikna etmek ve gelecek yirmi yılda gerçekleşecek araştırmaların yürütülmesini sağlamak olmuştur (Kline, 2011).

Yapay zekâ çalışmalarının bu hızlı başlayan erken döneminin arkasından, ilki 1973-1979 ve ikincisi 1988-1994 tarihleri arasında olmak üzere iki kez bilimsel faaliyetlerin azaldığı duraksama dönemleri izlemiştir. “Yapay Zekâ Kışı” olarak adlandırılan bu dönemlerin ilki 1966'daki ALPAC raporu ve 1973'teki Lighthill raporunun yayınlanmasından sonra başlamıştır. 1964'te yapay zekâ projelerini finanse eden kuruluşlar tarafından talep edilen bu raporlar, 1940'lardan bu yana yürütülen çalışmaların başarısızlıklarını vurgulamaktadır (Poibeau, 2017). Yapay zekanın ilk yıllarında vaat ettikleri ve bu sebeple oluşan büyük beklenti, kısa zamanda yerini hayal kırıklığına bırakmıştır. Bunun sonucunda projelere sağlanan fonlar kesintiye uğramıştır ve bu durum alanda çalışan bilim insanlarının kısıtlanmasına neden olmakla birlikte aynı zamanda araştırmalara karşı güvensizliğe de yol açmıştır (Gonsalves, 2018). İkinci yapay zekâ kışı ise 1984'te Yapay Zekânın Geliştirilmesi Derneği (AAAI) tarafından düzenlenen panelde benzer sorunlara değinilmesinin ardından yaşanmıştır (Schuchmann, 2019). Bu süreç de birçok girişimcinin proje aşamasında başarısızlıklar yaşamasıyla sonuçlanmıştır.

Yapay zekâ araştırmaları 1990'ların ortalarından itibaren yeniden canlanmaya başlamıştır. 1997'de IBM'nin (International Business Machines Corporation) Deep Blue süper bilgisayarının Kasparov'a karşı aldığı zafer, 2011'de yine IBM'nin Watson'ının Jeopardy şampiyonlarına karşı kazandığı zafer gibi önemli kilometre taşları, bu sistemlerin gelişmişliklerine iyi birer örnek olmuştur ve yapay zekâ disiplinine olan inancı yeniden canlandırmıştır (Gonsalves, 2018).

3.2. Sesli Sanal Asistanlar

Yapay zekâ çalışmalarının en büyük etkilerinden biri, bilim insanlarına teknoloji ile insan etkileşimine odaklanan, kullanıcısıyla gerçek anlamda iletişime geçebilen makineler yaratmak için bir yol çizmesidir. Klasik makine- insan ilişkisinde makineler kodlanmış bilgileri algılar, bilgiyi işler ve uygun yanıtı karşılaştırma yoluyla bulup, bu yanıtı kullanıcıya iletir. İletişim eylemi gerçekleşirken makine bir kanal görevi görür. Günümüzde birçok teknoloji kullanıcıya bir iletişim ve bilgi akışı ortamı yaratmaktan çok daha fazlasını yapabilmektedir. Bu alandaki gelişmeler, insan etkileşimini ve duygusal zekayı taklit ederek rasyonel, mantığa dayalı sonuçlar elde edebilen makineler yaratmayı amaçlamaktadır (Krakovsky, 2018). Bu teknolojinin en yaygın uygulamalarından biri dijital asistanlar veya günümüzdeki isimleriyle, sesli sanal

asistanlar/akıllı sanal asistanlar/akıllı kişisel asistanlardır (Bu çalışmada alışmada “sesli sanal asistan-(SSA)” ifadesi kullanılmaktadır).

1970’lerde tasarımı olarak ortaya konulan, cep bilgisayarları olarak da bilinen kişisel dijital asistanlar (PDA), 1980’lerin başından itibaren geliştirilmeye başlanmıştır. Ancak dijital ve mobil bir kişisel asistanın piyasaya sürülmesi 1984’te üretilen Psion isimli taşınabilir el bilgisayarları ile gerçekleşmiştir. Bu cihazlar bir veri tabanına ve bir kilobayt belleğe sahiptir ve takvim, saat ve hesap makinesi olarak kullanılmakta olup (Wiggins III, 2004) sonraki yıllarda geliştirilecek modeller için prototip görevi görmüşlerdir. Ancak “kişisel dijital asistan” terimi çok daha yakın bir zamanda, 1990’ların başında Apple’ın o yıllardaki CEO’su ve başkanı olan John Sculley tarafından kullanılmıştır (Steele, 2021). Apple tarafından aynı dönemde not alabilen, faks gönderebilen ve el yazısını tanıyabilen ve metne çevirebilen Newton MessagePad’leri piyasaya sürülmüştür (Stengel, 2016). Zamanının ötesinde ve cep bilgisayarı kavramına en yakın örnek olmasıyla emsallerinden farklı bir cihaz olmasına rağmen Newton MessagePad, yazılım kaynaklı hatalar ve eksiklikler nedeniyle yeterince popüler olamamıştır (Hormby, 2013). 1990’ların ortasından itibaren dijital asistan, çağrı cihazı ve cep telefonu üreticilerinin bu cihazların tüm işlevlerini tek bir cihazda birleştirmeye karar vermesiyle, tarihin ilk akıllı telefonları üretilmeye başlanmıştır (Steele, 2021). IBM üretimi Simon Personal Communicator, 1994’te, Blackberry 2000’de ve iPhone 2007’de piyasaya sürülmüştür (Andrew, 2018).

1990’lardan itibaren algoritmaların yanı sıra sözlü dil yorumlama, doğal dil işleme, bellek kapasitesi alanlarında iyileştirilen yapay zekâ teknolojisi ile birlikte, kişisel asistanlar da ilk örneklerinden farklılaşmışlardır. Bu tür araçlar artık yalnızca belli işlevleri yerine getirmekle kalmayıp, kullanıcı ile etkileşerek onun isteklerini analiz edebilen, ona yanıt verebilen, hatta ondan öğrenebilen akıllı kişisel asistanlara (intelligent personal assistant ya da IPA) evrilmişlerdir. Makine öğrenimi ve doğal dil işlemedeki son gelişmelerle birlikte ses, insan-bilgisayar etkileşimi için birincil yöntem haline gelmiştir. Bu gelişmeyle birlikte sesli dijital asistanlar olarak adlandırılan, ses tanıma, konuşma sentezi ve doğal dil işlemeyi kullanabilen hizmet sağlayıcılar doğmuştur (Ramos, 2018).

SSA’lar, yapay zekâ desteğiyle insan konuşmasını algılayabilme ve yorumlayabilme, bu sayede yanıt vererek ses yoluyla etkileşim kurabilme özelliği olan yapay zekâ destekli yazılımlardır (Taba, 2019). Kullanıcısının sesli komutlarını algılayarak internette arama yapma, basit görevleri tamamlama, diğer cihazlarla bağlantı

kurma gibi işlevleri yerine getirebilirler. Kullanıcılar, asistanlarına soru sorabilir, ev otomasyon cihazlarını (arabaların ve evlerin kilidini açmak, ışıkları kontrol etmek, termostadı ayarlamak, televizyon kanalını değiştirebilmek gibi) sesli olarak kontrol edebilir ve e-posta atmak, hatırlatıcı alarm kurmak gibi diğer temel görevleri sözlü komutlarla yönetebilirler; arama yapabilir, metin mesajları gönderebilir, uygulamaları kullanabilirler (Hoy, 2018). 2011 yılında Apple tarafından geliştirilen Siri, akıllı telefonlarda yer alan ve SSA'ların yaygınlaşmasını sağlayan ilk uygulama olmuştur (Smartsheet, 2020). Onu 2016 yılında geliştirilen Android platformlarda yer alan Google Asistan (Google Assistant) takip etmiştir. Daha sonra Bixby (Samsung), Watson (IBM), Cortana (Microsoft), Nina (Nuance) ve başta Alexa (Amazon) olmak üzere akıllı hoparlör denilen cihazlarla birlikte kullanılabilen ev tipi asistanlar kullanıcılara sunulmuştur. SSA'lar 2019 yılında 3,5 milyon kullanıcı ile artık yaygın olarak kullanılan bir uygulama haline gelmiştir ve kullanıcı sayısının 2024 yılına kadar 8,4 milyon olması beklenmektedir (Statista, 2020). Bu yaygınlaşma o kadar hızlıdır ki, cep telefonu sayısının insan sayısını geçmesi 30 yıl almışken, SSA'lar ise bunu yarı yarıya daha kısa zamanda başarmışlardır (Nichinson, 2020).

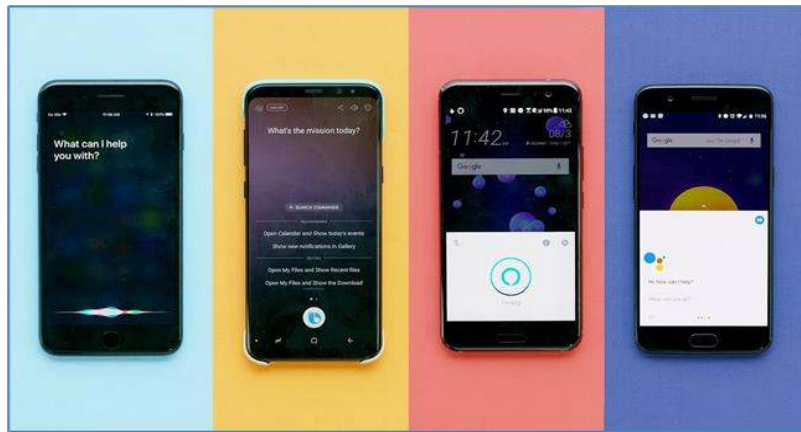
3.2.1. Sohbet Botları

Sohbet botları da SSA'lar gibi insanlarla etkileşim kurma yoluyla problem çözmek için geliştirilmiş, yapay zekâ tarafından desteklenen programlardır. İnsanlar hemen hemen her gün bu teknolojilerden biri veya her ikisi ile etkileşime girse bile, çoğu kullanıcı bu teknolojilerin her ikisinin de aynı olduğu görüşündedir (Shanbhag, 2020). Sohbet botları, müşteri hizmetlerine birer alternatif olarak geliştirilmiş, müşterilerle birer insan gibi etkileşime girerek onlara yardımcı olmak için tasarlanmıştır. SSA'ların kullanım alanı ise sohbet botlarının kullanım alanlarından çok daha geniştir ve kullanıcıların günlük etkinliklerine yardımcı olabilmek için tasarlanmış yazılımlardır. Sohbet botlarının çalışma sistemleri SSA'larındaki kadar gelişmiş değildir, dolayısıyla sohbet botunun algoritması izin verdiği ölçüde konuşmanın içeriğini algılayarak doğru bot akışını yürütebilseler de bu çerçevenin dışındaki sorulara yanıt bulamazlar veya kendi başlarına bir dizi aktivite gerçekleştiremezler (Srikanth, 2020). Ayrıca insan duygularını anlama, konuşma kesildikten sonra konuşmanın içeriğini hatırlamaya devam etme gibi özellikleri yoktur (Joshi, 2018). Bir SSA ise mevcut kaynaklar arasında gezinebilir ve çok çeşitli istekler için yardım sunabilir (Srikanth,

2020). Gelişmiş doğal dil işlemenin kullanılmasıyla SSA'lar, konuşmaları ve kimi zaman duyguları analiz edebilir (Joshi, 2018). Kullanıcılarla neredeyse “insani” denebilecek bir iletişim kurmaya çabalayan SSA'lara kullanıcısı tarafından bir ad ve cinsiyet dahi verilebilmektedir (Guzman, 2017). Ayrıca kullanıcıya ait bilgileri gerekliyse daha sonra kullanmak üzere bulutta depolayabilir.

3.2.2. Sesli Sanal Asistanların Çalışma İlkeleri

SSA'lar, problem çözebilme, öğrenebilme gibi insan zihniyle ilişkilendirilen bilişsel süreçleri yerine getirebilmeleri için bir yapay zekâ desteğine gerek duyan yazılımlardır (Poushneh, 2021). İnsan konuşmasını anlayabilmesini ve analiz edebilmesini sağlayan yapay sinir ağlarına ve bir hafıza gibi işlev gören, konuşma analizlerini gerçekleştirdiği bulut tabanlı bir tasarıya sahiplerdir. SSA'lar, iletişim olarak temelde ses üzerinde çalışır; ses sinyalinin sisteme işlenmesine, metne dönüştürülmesine ve gerekli işlemin yapılmasına odaklanır (Patil vd., 2021). Konuşma tanıma için çeşitli makine öğrenimi algoritmaları kullanılır. SSA'lar sohbet akışının görülebildiği bir arayüze sahiptir ancak sesli komutlar kullanılarak etkinleştirildiğinde arayüz olmadan da çalışabilir (Srikanth, 2020). Sesli komut özelliği, SSA'ların “Hey, Google”, “Alexa” veya “Hey, Siri” gibi bir tetikleyici kelime veya kelime öbeği ile etkinleştirilmesidir. Komut ifadesi kullanıcının isteğine bağlı olarak özelleştirilebilir ya da açılıp kapatılabilir. Asistan sesle etkinleştirildiğinde, kullanıcı genellikle bir ışık (Google Dot, Alexa Echo) veya değişen ekran görüntüsü (Apple veya Google telefonları) şeklinde bir geri bildirim alır (Lopatovska, 2019).



Resim 1. Etkinleştirilmiş mobil sesli sanal asistanlar

Kaynak: i.ytimg.com

Yoffie ve arkadaşları (2018), asistanların sesleri algılama ve işlevi yerine getirme sürecinde asistanın, kullanıcının talebini yakalayabilmek için dikkat dağıtıcı ses sinyallerini (ses yankıları, arka plan gürültüsü, cihazın kendi hoparlörü gibi) baskılayabilen bir filtreye sahip olduğunu belirtir. Algılanan komut daha sonra metne dönüştürülür ve analiz için bulutta bir doğal dil işleme algoritması aracılığıyla çalıştırılır. Doğal dil işleme süreci, ifadelerin niyetlere (istegin amacı nedir) ve varlıklara (istek bir tarih, saat veya bir kişi içeriyor mu) ayrılmasını içerir. Buna göre, veri tabanından olası yanıtlar seçilir ve bir ses kliline dönüştürülerek kullanıcıya geri gönderilir. Zamanla algoritma daha fazla veri ile beslenir ve böylece daha akıllı hale gelir (Yoffie vd., 2018).

SSA'lar, akıllı telefon ya da akıllı hoparlör gibi cihazların içerisine işlenmiş olarak gelirler. Birçoğu, işlevlerini yerine getirmek için şirketlerin bulut sunucularına veya diğer ağ bağlantılı cihazlara ihtiyaç duyar, arama motorlarına bağlanabilmek için bir internet bağlantısı gerekmektedir (Lopatovska, 2019).

3.2.2.1. Makine Öğrenimi – Derin Öğrenme

Makine öğrenimi, yapay zekâ destekli makinelerin gelişebilmek adına önceki deneyimlerini kullanabilmesini sağlayan tekniklerin kullanıldığı yapay zekanın bir alt kümesidir; derin öğrenme ise bu tekniklerden biri olup, öğrenmenin yapay sinir ağları yoluyla gerçekleştiği, makine öğreniminin bir alt kümesidir (Microsoft, 2021). Derin öğrenmedeki "derin" ifadesi, üçten fazla katmandan oluşan bir derin öğrenme algoritması olarak görülebilecek sinirsel (nöral) bir ağı ifade eder (IBM, 2020). Sinir ağları, yalnızca konuşma tanıma özelliğini iyileştirmekle kalmaz, aynı zamanda daha fazla veri depolandıkça yapay zekanın ifadeleri de daha iyi hale gelir. Çünkü sinir ağlarının çalışma sistemi sayesinde makine insanların diller arasında nasıl iletişim kurduğuna ilişkin kalıpları belirleyebilir ve bunlardan öğrenebilir (Klie, 2014).

Akıllı bir sistem makine öğrenimi sayesinde geçmişe dönük verileri özümseyerek ve onları kendi içinde kategorilendirerek, yeni problemler ortaya çıktıkça çözmek için doğrudan programlama algoritmalarını kullanmak yerine önceki örneklerden öğrenebilen bilişsel öğrenme algoritmaları geliştirmeyi amaçlar (Marsland'dan aktaran Brill, 2015). Makine öğrenimi, yapay zekâ sistemlerinin temel çalışma prensibi olup, programcının yarattığı analitik ve algoritmik sistemin zamanla deneyim, gözlem ve bilgi işleme süreciyle gerçek bir beyin gibi öğrenmesini ifade eder.

Makine öğrenimini geliştirebilmenin yolu daha fazla veriye sahip olmaktır (Pehlivan, 2019). Bu sayede makine, kullanıcıya kişiselleştirilmiş bir deneyim sunabilir.

3.2.2.2. Doğal Dil İşleme

İnsanlar ve makineler arası iletişimdeki boşluğu doldurmak için önemli bir süreç olan (Terzopoulos ve Satratzemi, 2019) doğal dil işleme (NLP), akıllı makinelerin insan dillerini anlama ve işleme yeteneğidir. Doğal dil anlayışı (NLU) ise, makinenin doğal dil komutlarını daha iyi anlamasını sağlayan, doğal dil işlemenin alt dallarındandır. SSA'lar da kullanıcının metin veya ses girişini algılayıp, yürütülebilir komutlarla eşleştirmek için doğal dil işlemeyi kullanmaktadır (Kondrats, 2018).

Konuşma tanıma, sözlü komutları tanıma ve bunlara tepki verme yeteneğidir ve SSA'nın temel becerilerinden biridir. Konuşma tanıma, titreşimleri dalga benzeri bir elektrik sinyaline çeviren ve bir ses kartı tarafından dijital bir sinyale dönüştürülen bir mikrofondan başlar. (Taba, 2019). Sinyallerin ön işleme yapıldıktan sonra, veriler sinir ağları sayesinde gruplara ayrılır ve bu süreçte tekrarlayan sinir ağları (RNN) sayesinde, gelecekteki sonuçları etkileyebilecek hafıza da oluşmuş olur (Kulshreshtha, 2020).



Resim 2. Konuşma tanıma işlemi süreci

Kaynak: i0.wp.com

İnsan etkileşimi sayesinde öğrenebilen ve bu sayede kullanıcının komutlarına yanıt verebilen bu sistemlere en eski örnekler 1962'de IBM tarafından geliştirilen, 16 kelime ve rakamları algılayabilen Shoebox; 1970'lerde Carnegie Mellon Üniversitesi'nde geliştirilen ve üç yaşındaki bir çocuğun kelime dağarcığı (yaklaşık 1011) kadar kelimeyi tanıyabilen Harpy'dir (Smartsheet, 2020). Yapay zekâ konuşma tanıma açısından o yıllardan bu yana büyük bir gelişme kaydetmiştir, böylece

günümüzde gündelik hayatta bile kullanabilen SSA'lar gibi teknolojilerden faydalanabiliyoruz. Daha da önemlisi, konuşulan dilde duyguların saptanmasını sağlayan duygusal yapay zekadaki gelişmelerle akıllı makinelerin kullanıcısının duygusal durumunu analiz edebilmesi ve etkileşimini daha da güçlü kılması mümkündür (ViaDialog, 2021). Şu an için ise bu teknoloji henüz SSA'lar için asgari düzeydedir fakat geliştirilmektedir (Alston, 2020). Bununla birlikte SSA'ların da kullanıcıya verdiği yanıtların daha fazla duygusal tepki içermesi için duygusal yapay zekâ üzerindeki çalışmalar da devam etmektedir (Koetsier, 2018). Algoritmalar iyi bir kullanıcı deneyimi sunabilmek adına sürekli olarak geliştirilmektedir ve SSA'lar büyük ölçüde doğal dil işleme teknolojisine bağlı olduğu için, doğal dil işlemenin sınırlamaları ile de kısıtlanmaktadır (TELUS International, 2021).

3.3. Sesli Sanal Asistanlar ve Kişisel Veri Gizliliği

Yapay zekanın öğrenme işlemi için veri toplaması şarttır, ne kadar çok veriyi derlerse bunları o kadar birbiriyle eşleştirebilir. Bu durum kullanıcıya sunulan bir kolaylık olsa da sürekli dinlemede kalma ihtimali potansiyel kullanıcıları bir hayli tedirgin etmektedir. Salesforce'un (2019) verilerine göre tüketicilerin yüzde 46'sı kendi verileri üzerindeki kontrollerini kaybettiklerini düşünürken, Pew Research Center'in (2019) araştırmasına göre Amerikalıların yüzde 63'ü, veri gizliliklerini korumak için halihazırda yürürlükte olan yasa ve yönetmeliklerden çok az şey anladıklarını veya hiçbir şey bilmediklerini söylemektedir. Beş yetişkinden sadece biri, her zaman (yüzde 9) veya sıklıkla (yüzde 13) bir şirketin gizlilik politikasını kabul etmeden önce okuduğunu söylemektedir. Yetişkinlerin yüzde 36'sı bir şirketin gizlilik politikasını kabul etmeden önce asla okumadığını dile getirmektedir. Tableau'nun (2019) istatistiklerine göre ise tüketicilerin yüzde 48'i, gizlilik endişeleri nedeniyle çevrimiçi satın almayı bırakmıştır. Buna rağmen bu teknolojiler hayatın her alanına entegre olmaya başlamış durumdadır. Kullanım yaygınlığı en çok artan akıllı cihazlardan biri de SSA'lardır. Bu hızlı artışa rağmen, araştırmalar evde SSA kullanımına dair duyulabilen çekincelerde gizlilik risklerinin rolünü ortaya koymaktadır (Guzman, 2017). The Smart Audio Report'un 2020 verilerine göre, SSA kullanıcısı olmayanların en önemli gerekçesi yüzde 65 oranıyla SSA'ların sürekli dinliyor olmasından duydukları rahatsızlıktır. SSA kullanıcılarının yüzde 58'i de sürekli dinleniyor olmaktan rahatsız olduklarını dile getirmişlerdir. Kullanıcı olmayanların diğer gerekçeleri ise bilgisayar

korsanlarının kişisel bilgilerine erişme ihtimali, geliştirici şirketlere güvenmemeleri ve hükümet tarafından özel konuşmaların dinlenebilmesidir. Böyle bir durumun yanlışlıkla bile yaşanmış olması büyük bir güvenlik sorunu yaratabilir. SSA'lar performans sağlayabilmesi için dinlemede ve çevrimiçi kalması gereken cihazlardır. Buradan da anlaşılabilir gibi SSA'lara yönelik endişelerin başında kişisel gizlilik ve mahremiyet sorunu gelmektedir çünkü kullanıcı için en büyük risk kişisel verilerinin güvende olmamasıdır. SSA'ların bazı gizlilik ve güvenlik sorunlarına açık sistemler olması güncel bir tartışma olsa da bu asistanlar sundukları kolaylıklar adına sıklıkla tercih edilmektedir. Paw Research'ün (2020) araştırmasına göre Amerikalıların yüzde 46'sı dijital ses asistanları kullanmaktadır. Zygmunt Bauman (2013, s. 35) dijital dünyanın etkisiyle hiç olmadığı kadar artan bu mahremiyet sorununu insanların içselleştirmeye başladığını ve yıllardır süregelen mahremiyet ihlali normalleştirme yönelik çalışmaların etkilerini göstermeye başladığını dile getirmektedir. Bauman "Mahremiyet hakkımızı kendi rızamızla katlettiriyoruz. Ya da belki sadece, bize sunulan harikalar karşılığında ödenecek bir bedel olarak mahremiyet kaybına rıza gösteriyoruz. Belki de kişisel bağımsızlığımızı mezbahaya kendi ellerimizle göndermemiz için bize uygulanan baskı o kadar kuvvetli ki ve durumumuz bir koyun sürüsünün durumuna o kadar benziyor ki ancak birkaç istisnai isyankâr, gözü pek, kavgacı ve dirençli irade ona karşı samimi bir girişimde bulunabiliyor." (2013, s. 35) diyerek toplumun teknoloji sahipleri ya da yöneticileri tarafından izlenmek konusunda artık rahatsızlık duymadığını, bunu kanıksadığını ve bireyin kendini izlemesi/izletmesi ve toplumun birbirini izlemesi boyutuna geçildiğini dile getirmektedir. İnsanın yarattığı bu teknolojiler ve onları hayatlarına entegre etme şekli bireylerin ve toplumun evriminde ve kendisini görme biçiminde ayrılmaz bir rol oynamıştır (Guzman, 2017).

SSA'lar eğer bilgilerinizi depolama izni verirsiniz mesajlarınızı okuyabilir, konumunuzu tespit edebilir, arama motoru ve uygulama geçmişinizi görüntüleyebilir, rehberinizi kontrol edebilir (Tulshan ve Dhage, 2019). Bu iznin rızayla verilmesi durumu kabul edilebilir kılmamaktadır zira kullanıcı hangi bilgilerin ne düzeyde takip edileceği veya paylaşılacağı konusunda bilgi sahibi olmayabilir. Üstelik araştırmalar SSA'lar zekâ, samimiyet, yaratıcılık gibi insani özellikler gösterdiklerinde kullanıcıların kendilerini güvende hissetmeye daha meyilli olduklarını göstermektedir (Poushneh, 2021). Bunların yanı sıra günümüzde kişisel verilerin toplanması konusunda bireyin verdiği onay veriler toplanırken alınmaktadır; sanal dünyada ya da bir sesli asistan sisteminin ev ortamını dinleme esnasında kaydedilen ve kullanılan birçok veri kişisel

verilerle doğrudan ilgili olmasa bile kullanıcıya yönelik çok önemli ipuçları ve kimliği tanımlayıcı bilgi barındırabilmektedir (Eroğlu, 2018). Hukuk profesörü Daniel J. Solove (2007, s. 747), "Saklayacak hiçbir şeyin yoksa, o zaman neden korkacaksın?", "'Eğer yanlış bir şey yapmıyorsanız, o zaman neyi gizlemeniz gerekir?" gibi argümanlarla bir kişinin yasal faaliyetlerde bulunduğu sürece tüm hayatının dinlenmesinden, verilerinin derlenmesinden ve saklanmasından endişe duymaması gerekiyormuş algısının yaratılmaya çalışıldığını, oysa bir bireyin hayatının herhangi bir alanına izinsiz dahil olmanın bireye doğrudan müdahale olduğunu ve bunun da gerçek bir mahremiyet sorunu olduğunu dile getirmektedir. Bireyin davranışları, bilgileri, sosyal çevresi ve kim olduğuna dair yabancı bir kaynağın ne kadar bilgi sahibi olacağı da kişisel mahremiyet meselesidir (Tataroğlu, 2003). Bir kişi hakkında bilgi toplamak da onun mahremiyetini ihlal etmektir. Solove (2007), mahremiyetin kötü şeyleri saklamakla ilgili olduğuna dair temel varsayımının yanlışlığını bu şekilde ifade eder.

Her bir ayrı veri parçası bir araya gelip sentezlendiğinde, kalıcı bir dijital profil oluşturmaktadır ve bu verileri kullanan şirketlerin kullanıcıları, şirketlerin onları, izin verdikleri ölçüden daha fazla tanımlarına neden olmaktadır (Creighton, 2016). Her ne kadar Siri de Google Asistan da bu verilerin etiketsiz olarak muhafaza edildiğini ifade etse de SSA'ların kullanıcıların tüm kişisel konuşmalarını kaydedebilme potansiyeli düşünüldüğünde bu sistemlerin gerekli güvenlik mekanizmalarına sahip olup olmadıkları sorusunun cevabı veri gizliliği açısından büyük önem arz etmektedir. Apple sözcüsü Trudy Muller 2013 yılında Apple'ın Siri tarafından elde edilen verileri iki yıl boyunca sakladığını açıklamıştır (McMillan, 2013). Güncel kaynaklarda ise bu süre altı ay olarak belirtilmiştir. Apple verilerin anonim kaldığını, yalnızca kullanıcıyı daha iyi anlamasına ve söylenenleri tanımasına yardımcı olmak için kullanıldığını belirtmiştir (Hern, 2019). Ancak bu açıklama Siri, Alexa, ve Google sesli asistanlarının kendi kendine aktif olmasını, tüm konuşmaları dinlemeye neden ihtiyaç duyduğunu ve hatta bu konuşmaları dinlemek için neden bir ekip oluşturmaya gerek duyduğu gibi soruları yanıtlamamaktadır. Bunun yanı sıra çoğu SSA mobil telefonların yazılımı içinde hazır olarak yüklenmiş şekilde kullanıcıya ulaşmaktadır. Her ne kadar kullanıcı tarafından daha sonra devre dışı bırakılabilse de SSA kullanımına dair bilgisi olmayan kullanıcılar için bu mümkün olmamaktadır. Steve Jobs'un bir konferans sırasında dile getirdiği "İnsanların zeki olduğuna ve bazılarının diğer insanlardan daha fazla veri paylaşmak istediğine inanıyorum." (All Things Digital Conference, 2010) ifadesi şirketin geliştirdiği hizmetlerin, kullanıcılarını daha fazla veri paylaşmaya ikna eden bir politika

içerdiğini göstermektedir. Oysaki bu teknolojilerdeki birçok güvenlik açığı kullanıcının bilgisi ve rızası dışında maruz kaldığı tehditlerdir ve veri paylaşımına onay verilse dahi bu verilerin nerede, hangi amaçla, kimler tarafından kullanıldığı sesli asistan geliştirici şirketler tarafından açıklanmamaktadır.

Aloufi, Haddadi ve Boyle (2019), “Emotionless: Privacy-Preserving Speech Analysis for Voice Assistants (Duygusuz: Sesli Asistanlar için Gizliliği Koruyan Konuşma Analizi)” adlı çalışmalarında sadece ses sinyalinin bile kullanıcının duygusal durumu, stres düzeyi, fiziksel durumu, yaşı, cinsiyeti gibi kişisel özellikleri hakkında bilgi verebileceğini ifade eder. Hizmet sağlayıcı şirketlerin bir kullanıcının demografik konumuna ve kişisel tercihlerine dair doğruluğu yüksek bir profil oluşturma riski olduğunun üzerinde durur. Aloufi, Haddadi ve Boyle (2019), çalışma kapsamında yaptıkları araştırmalar neticesinde bu sorunu çözebilmek adına kullanıcı ve bulut hizmetleri arasına gizliliği koruyabilecek bir ara katman önermektedir. Böylece sesli veriler toplandıktan sonra ve veriler hizmet sağlayıcı merkeze iletilmeden önce gizliliğin korunması için sinyal analiz edilecektir ve hassas temsiller ham sinyalin içerisinden ayıklandıktan sonra kayıtlı veri merkeze iletilir.

3.3.1. Sesli Sanal Asistanlar ve Güvenlik

SSA kullanımına bağlı olarak kullanıcının güvenliğinin sağlanması, veri gizliliğinin sağlanmasıyla aynı amaca hizmet eden farklı yöntemler gibi düşünülebilmektedir. Uluslararası Gizlilik Uzmanları Derneği (IAPP)’nin ifade ettiği üzere (2021) veri gizliliği, kullanıcının kişisel bilgilerinin gizliliğe uygun bir şekilde toplanması ve kullanılmasına yönelik politikalar oluşturmakla ilgilenirken, güvenlik meselesi daha çok SSA’ların teknik açıdan eksiklikleri sonucu yaşanabilecek siber saldırılar, kullanılan yazılımın açıkları – eksiklikleri, diğer teknolojik cihazlarla olan etkileşiminden doğabilecek açıklar gibi durumlardan korumaya yöneliktir. SSA’lar başta olmak üzere, internet bağlantılı cihazların birbirleriyle bütünleşmiş bir şekilde çalışması daha büyük risk taşımaktadır. Federal Ticaret Komisyonu (FTC)’nin web sayfasında (2022) vermiş olduğu bilgilere göre, bu tür riskler her zaman söz konusudur ve kullanıcı SSA kullanımında “ayarlar” sekmesine her zaman hâkim olmalıdır. Çünkü SSA’ların gizlilik politikalarına bakıldığında yazılımın sağladığı tüm güvenlik önlemleri (güçlü bir parola, çok faktörlü kimlik doğrulama, veri erişimini denetleme vs.) manuel ayarlar içermektedir. SSA çeşitli bilgilere ulaşır çünkü kullanıcı bunu rızayla veya

bilmeden kabul etmiş olur. Ayarlar değiştirilmediği sürece de aynı kalır. Kullanıcılar çoğu zaman bunu fark edememektedir çünkü gizlilik politikaları geliştirici şirketlerin niyetlerini ifade ediş yönünden zayıf kalmaktadır.

Edu, Such ve Suarez-Tangil'in 2021'de yayınladığı "Smart Home Personal Assistants (Akıllı Ev Kişisel Asistanları)" başlıklı makale bu güvenlik açıklarını şöyle özetlemiştir: öncelikle ABD'de bu tip asistanların güvenlik ihlali yaptığı yönünde sık sık ihbarlar yapılmaktadır ve kullanıcılar mağduriyetlerini dile getirmektedir. SSA'ların verileri depoladığı bulut sistemleri teknik anlamda donanımlı bir sistem değildir ve daha önce hackerlar tarafından kötü niyetli saldırılar gerçekleştirildiği basında yer almıştır. Edu, Such ve Suarez-Tangil, SSA'lara yönelik olarak kullanıcılar tarafından çok dile getirilen ihlalin bu olduğunu belirtmişlerdir. Üstelik yalnızca dışardan saldırılar değil, yetkili kişilerin erişimleri doğrultusunda kişisel verilerin amaç dışı kullanımı sonucu, içerden de bu ihlallerin gerçekleşmesi mümkündür.

Bulut sisteminin zayıflığının yanı sıra, SSA'ların en büyük avantajı olarak görülen, temel özelliği olan sesli komut da birçok veri ihlali riski taşımaktadır (Edu, Such ve Suarez-Tangil, 2021). Uyandırma sözcüğüyle SSA'yı aktif hale getirmek kullanıcıya kolaylık sağladığı gibi, sesin taklit edilmesi, başka bir sözcüğün SSA tarafından uyandırma sözcüğü gibi algılanması gibi durumlar sonucu SSA'lar kullanıcı dışında biri tarafından kolaylıkla aktif hale getirilebilir.

SSA'ların kişisel veri topladığı kesin bir bilgi olsa da bu verilerin hangi amaçlarla toplandığı her ne kadar gizlilik politikaları ortaya konulsa da belirsizliğini korumaya devam edecektir. Asla garanti edilemeyecek bir gizlilik anlayışı vardır ve eğer bu teknolojilerden faydalanılacaksa bu durumun muğlaklığı kabul edilmeli ve bu konuda neler yapılabileceği düşünülmelidir.

3.3.2. Sesli Sanal Asistanların Kullanım Alanları ve Veri Gizliliği Politikaları

SSA'lar, kullanıcıların günlük görevlerinin bir kısmını üstlenerek, onların üretkenliğini artırmayı ve zamandan tasarruf ettirmeyi amaçlar. SSA'ların yapabileceği görevlerin bir kısmı şunlardır: "Not almak, metinleri veya e-postaları sesli olarak okumak, telefon aramaları yapabilmek, hatırlatıcı görevi görmek, oyunlarla, şakalarla kullanıcıyı eğlendirmek, hava durumu bilgisi vermek, alışveriş yapmaya yardımcı olmak, diğer akıllı cihazların (ışıklar, kilitler, termostatlar, kapı kilidi vs. gibi ev sistemiyle bağlantılı olduğu durumlarda) kontrolünü sağlamak" (Srikanth, 2020). Sesle

aktif hale gelebildikleri için, kullanıcıların asistanlarını eller serbest halde kullanabilmelerine olanak sağlar (Siri Team, 2017). Böylece kullanıcı meşgulken ya da trafikteyken de SSA'ya komut verebilir. Bunun yanı sıra eğitim, sağlık, endüstri, e-ticaret gibi alanlarda faydalar sağlamaktadır (Tulshan ve Dhage, 2019). Günümüzün en popüler SSA'larının başında Siri, Google Asistan, Bixby ve Cortana gelmektedir, akıllı hoparlörlerde ise Amazon'un Alexa'sıdır (Adobe Analytics, 2019).

3.3.2.1. Siri

Başlangıçta Siri, AppStore'da yer alan bir uygulamayken, kullanıma girdikten iki ay sonra Apple tarafından satın alınmış ve ardından Ekim 2011'de piyasaya sürülen iPhone 4S'ye entegre edilmiştir (Kurtishi, 2018). Siri, 36 ülkede 21 dili ve Çince, Felemenkçe, İngilizce, Fransızca, Almanca, İtalyanca ve İspanyolcanın farklı lehçelerini desteklemektedir (Wiggers, 2018a). Apple'ın web sayfasında belirtmiş olduğu üzere Siri arama yapabilir, önemli notları hatırlatabilir, trafikte mesajları okuyabilir, merak edilen şeyleri arama motorlarından aratabilir, kullanıcıyı sabahları uyandırabilir, istenilen bir şarkıyı çalabilir. Bunlar SSA'ların gerçekleştirebildiği en yaygın görevler arasında yer alır (Apple-Siri).



Resim 3. Siri'nin orta tuş ile aktifleşmesi

Kaynak: <https://www.shutterstock.com>

Apple'da yer alan bilgilere göre (Apple Support), ses girişi gerçekleştiğinde veriler iPhone'da işlenir, ancak komutların dökümleri Siri'nin geliştirilmesi amacıyla Apple merkezine de gönderilir. Bu veriler kullanıcının Apple kimliği ile ilişkilendirilmez. Ayrıca kullanıcı isterse ses kayıtları Siri'yi geliştirmek amacıyla

Apple ile paylaşmayı kabul edebilir. Siri, kişisel bilgilerin yanı sıra sesli komut ile “dikte edilen” verileri depoladığını ve işlediğini açıkça belirtmiştir. Kullanıcı isterse bu verileri silme hakkı vardır ancak pek çok kullanıcının bu bilgiden yoksun olduğu tahmin edilebilmektedir. Apple’ın web sayfasında yer alan bilgiye göre, tüketici gizliliğini korumak için Siri aramalarını rastgele etiketlenir ve arama verileri altı ay boyunca saklanarak güvenlik risklerine karşı önlem alınır (Yoffie vd., 2018). Siri’nin işlevleri arasında arama yapma, önemli olan notları hatırlatma, trafikteyken gelen mesajları okuma, bir konu hakkında internette arama yapma, sabahları saat işlevi görerek kullanıcıyı uyandırması gibi özellikler yer almaktadır.¹ Guzman’a göre (2017) Siri kullanıcıları veri paylaşımı yaparak Apple’ın Siri’yi geliştirmek için ihtiyaç duyduğu bilgileri sağladığını kabul etmelidir. Bu da milyonlarca kişinin verisi anlamına gelmektedir ve bu oran Apple’a kullanıcı etkileşimi olmadan asla kendi başına üretemeyeceği miktarda bilgi sağlamaktadır (Guzman, 2017).

Common Sense isimli, uygulamaları yasal gereklilikler ve veri gizliliğine uygunluk açısından değerlendiren Gizlilik Programı SSA’ları da gizlilik politikaları yönünden değerlendirmiştir. Common Sense’de (2021) derlenen verilere göre Apple gizlilik politikaları içeriğinde kişisel veri gizliliğinin yasal bir hak olduğunu belirtir ancak Siri üzerinden yapılan aramaların ve komutların kullanıcının Apple kimliğiyle değil bir tanımlayıcı üzerinden ilişkilendirildiği belirtilmektedir. Bu nedenle kişisel bilgiler reklam amaçlı veya diğer kuruluşlara satmak için toplanmadığı ifade edilmektedir (Common Sense, 2021).

3.3.2.2. Google Asistan

Google’ın SSA’sı Google Asistan, ilk kez Mayıs 2016’da kullanıcılarına sunulmuştur (Yoffie vd., 2018). Google’ın yirmi yıllık web arama deneyimi, Google Asistan’ın alt yapısını ve geliştirilme sürecini desteklemektedir, bu nedenle diğer SSA’lara kıyasla bilgi talep edilen soruları yanıtlamada daha üstündür (Betters ve Grabham’dan aktaran Lopatovska, 2019). Uygulama, Google bünyesinde bulunan Google Books, Google Maps, Google Earth, Google Docs, Gmail gibi diğer hizmet sağlayıcılara entegre biçimde çalışabilir. Örneğin, Google Asistan aracılığıyla Google Maps üzerinde gezinebilmek ya da sesle Google Maps üzerinden tahmini varış süresini diğer kişilerle paylaşabilmek mümkündür (Tillman, 2021).

¹ <https://www.apple.com/siri/>



Resim 4. Google asistanın arayüzü

Kaynak: www.shutterstock.com

Destekleyebildiği dil bakımından sesli asistanlar arasında ilk sırada yer alan Google Asistan, 2017'de sekiz dil ve on dört ülkede olmak üzere toplam seksen ülkede otuzdan fazla dili desteklemektedir (Wiggers, 2018a). Google Asistan, sahip olduğu özellikler bakımından akıllı hoparlörlerin birçoğunda bulunan Alexa'dan daha geride olup, uyumlu olduğu akıllı ev cihaz türü de Alexa'ya göre daha azdır. Ancak cihazlar arasında ağ oluşturulduğunda daha iyi çalışmakta ve çok çeşitli Google uygulamaları ve hizmetleriyle birlikte çalışabilmektedir (Hall ve Van Camp, 2021). Ayrıca yapay zekâ sistemine sahip tüm yeni model Android telefonlarda kullanılabilmektedir (Tillman, 2021).

Google'ın web sayfasında (Google Support) yer alan bilgilere göre, Google'a bir komut verdikten kısa bir süre sonra o komutla ilişkilendirebileceği ikinci bir komut verdiğinizde Asistan ne demek istendiğini anlamak için önceki isteği kullanabilir. “Bu yalnızca o an için mi geçerlidir yoksa Google verileri gelecekteki işlemlerini iyileştirmek adına saklamakta mıdır” sorusunun yanıtı ise, Google'ın ifadesiyle “kişi kendi istemediği sürece” verilerin saklanmayacağı yönündedir. Buna karşın, kişisel herhangi bir verinin hiçbir zaman satılmadığını ancak “devlet talep ettiğinde” yasalara uygun görüldüğü takdirde bilgilerin paylaşılabildiği belirtilmiştir. Ayrıca, tetikleyici bir komut almadığı sürece bekleme modunda kalacağı ve bu durumdayken seslerin kayıt altına alınmasının mümkün olmadığı belirtilse de bazen “yanlış algılama” nedeniyle kendi kendine etkinleşebilmesinin mümkün olduğu ve bu durumu azaltmak adına üzerinde çalıştıkları da belirtilmiştir (Google Support/assistant).

3.3.2.3. Alexa

Amazon, bulut tabanlı ses teknolojisi olan Amazon Alexa'dan önce 2012 yılında piyasaya sürülen Evi adında, bir İngiliz şirketinin teknolojisini satın almıştır. Amazon, bu teknolojiden konuşma özellikli bir kitap okuyucu yapmak için yararlanmaya niyetlense de daha sonra bu fikri geliştirip konuşma tanıma ve sentezleme üzerinde çalışarak 2014'te Alexa'yı içeren Amazon Echo Smart Speaker'ı piyasaya sürmüştür (Yoffie vd., 2018).



Resim 5. Alexa'nın aktif haldeki görüntüsü

Kaynak: <https://image.shutterstock.com>

Alexa, sesli etkileşim yoluyla müzik çalma, alarm kurma, trafik durumu, haberler veya hava durumu gibi gerçek zamanlı bilgileri sağlama gibi her SSA'nın yapabildiği temel yeteneklere sahiptir ancak bunun yanı sıra ev otomasyon sistemi olarak kullanılarak evde Alexa'yı destekleyen cihazları da kontrol edebilir (Kurtishi, 2018). Yapay zekâ geliştiricileri Alexa'ya belirli bir kişilik kazandırmak ve onun daha konuşkan ve aktif olması, daha fazlasını hatırlaması ve daha uzun konuşmalar yapması gibi özelliklerin üstünde durmaktadırlar (Poushneh, 2021). Apple CarPlay gibi özelliklerle entegre hale getirilip, tıpkı evde olduğu gibi araçta da müzik seçebilmek, yol tarifi almak ve sorular sormak vs. gibi işlemler için sesle etkinleştirme özelliği kullanılabilmektedir (Ismail, 2021). Alexa, kırk bir ülkede yüz elliden fazla üründe mevcuttur, ancak tüm sesli asistanlar arasında desteklediği dil sayısı en az olan Alexa'dır. Alexa; İngilizce, İspanyolca, Fransızca, Almanca, İtalyanca, Hintçe, Japonca ve Portekizce olmak üzere sekiz dili ve bu dillerin bazılarının lehçelerini desteklemektedir (Wiggers, 2018a). Desteklediği diller arasında Türkçe bulunmamaktadır.

Bateman'ın haberine göre (2021), 2018'de bir Alexa kullanıcısı, Amazon'dan saklanan tüm kişisel bilgilerini öğrenmek için talepte bulunmuştur ancak Amazon, yanlışlıkla başka bir kullanıcının detaylı kişisel verilerini 1700 ses dosyası halinde bu kullanıcıya göndermiştir. Bunun üzerine bu kullanıcının dosyaları, bir dergiye göndermesiyle bu ihlal basında yer alabilmiştir.

Common Sense verilerine bakıldığında (2021) Alexa gizlilik yönünden “uyarı veren” barkod ile işaretlenmiştir. Bunun nedeni Amazon'un Alexa'nın gizlilik politikasında belirttiği üzere, kullanıcının Alexa'yı kullanabilmesi için verilerinin bulutta depolanacak olmasını kabul etmesi gerekmesidir. Amazon Alexa'nın kişisel verileri toplayarak kullanıcısının verileri aracılığıyla öğrendiği bilgileri, kullanıcının Amazon deneyimini kişiselleştirebilmek adına kullandığını dile getirmektedir. Kullanıcı Alexa'yı kullanmaya başlamak için uyandırma kelimesini söyleyerek Alexa'yı aktif hale getirmelidir ki bu durum gizlilik politikasını kabul etmek anlamına gelmektedir. Alexa'nın en yaygın kullanılan ev tipi model SSA'lar oldukları düşünüldüğünde bu durum kişisel verilerin güvenliği açısından kullanıcı için büyük bir risktir. Bu verilerin reklam amacıyla üçüncü kişilere satılmayacağı belirtilse de (Common Sense, 2021) hassas verilerin toplanması, kullanıcı kimliğinin doğrulanabilir olması ve bu işlemin otomatik olarak gerçekleşiyor olması Alexa'nın gizlilik yönünden eksikleri olduğu anlamına gelmektedir.

3.3.2.4. Bixby

Samsung tarafından geliştirilen sanal asistan Bixby, 2017 yılında Samsung Galaxy S8 telefonlarla birlikte tanıtılmıştır (Hall, 2022). Aynı yıl içinde Samsung'a ait akıllı televizyon ve buzdolabı modelleri ile de uyumlu hale getirilerek kullanımı yaygınlaştırılmıştır (Wiggers, 2018b). Daha sonra bu cihazlara tabletler, akıllı saatler, kablosuz kulaklıklar da eklenmiştir. Samsung telefonlar aynı zamanda Google Asistan'ı da desteklemektedir (Hall, 2022). Henüz Türkçe dil desteği bulunmayan uygulama “Hi Bixby” uyandırma cümlesi ile aktif hale gelebilme özelliğine sahiptir. Samsung'un web sayfasında² yer alan bilgilere göre, ses tanıma özelliğinin yanı sıra ön kameraya entegre Bixby Vision özelliğiyle nesneleri tanıyabilme, bulunulan konum hakkında bilgi verme, gösterilen ürün için fiyat araştırması yapma, metin okuma ve çevirme, görme engellilere betimleme yapma gibi özellikleri bulunmaktadır. Bunun yanında günlük rutin görevleri

² <https://www.samsung.com/tr/apps/bixby/vision/>

belirlenen bir sırayla yapabilmesi mümkündür, bunun için yalnızca bir etkinleştirme sözcüğü seçilmesi gerekir. Metin yazma ve seslendirme, ses açma veya kapatma, hava durumu, güncel haberler ve makaleleri okuma, arama yapma gibi diğer SSA’larda bulunan görevlerin yanında Bixby’nin en büyük iddiası kullanıcısının alışkanlıklarını analiz ederek kişiselleşmesidir. Aynı zamanda farklı sesleri de tanıyarak yanıtlarını kişiselleştirebilir (Hall, 2022).



Resim 6. Bixby’nin arayüzü

Kaynak: img.global.news.samsung.com

Samsung’un tanıtım metninde Bixby’nin kullanıcının neleri sevdiğini öğrendiğini ve sevilen uygulamalar ve hizmetlerle birlikte çalışarak kullanıcıya nasıl kolaylık sağladığına dikkat çekilir. Web sayfasında “Bixby, belirli uygulamaları kontrol edebilir; ilerleyen dönemlerde başka uygulamaları desteklemesi beklenmektedir.” ifadesi yer almaktadır. Sunduğu bu üçüncü taraf hizmetleri desteği ile WhatsApp, Twitter, Youtube, Facebook, Instagram, Gmail gibi birçok uygulama ile uyumlu şekilde çalışabilir (Wiggers, 2018b). Samsung, kişisel veri paylaşımının kullanıcıların izni dahilinde gerçekleştiğini iddia etmektedir. Samsung tarafından oluşturulan Samsung Veri Koruma Yönergeleri, her ülkenin kendi yasaları çerçevesinde hazırlanmıştır. Belirtildiği üzere verilerin toplanması, kullanılması ve paylaşılmasında kullanıcının bilgisi, izni ve kontrolü vardır. Ayrıca güvenlik tehditleriyle mücadele edebilmek için çalışmalar yapıldığı bilgisi yer almaktadır. Bununla birlikte kullanıcı Bixby’deki tüm verileri sıfırlayabilir veya Bixby’yi devre dışı bırakabilir. Ancak Common Sense’in verilerine göre (2021) kişisel bilgilerin toplanması veya saklanması sürecinde kişisel verilerin korunması adına şifreleme gibi güvenlik önlemlerinin alınıp alınmadığı bilgisi veya bir veri ihlali gerçekleştiğinde kullanıcıların bilgilendirilip bilgilendirilmeyeceğine

dair detaylar şartlarda açıklanmamıştır. Toplanan veriler hassas verilerdir ve Samsung bu veriler üzerinden ticari kazanç elde etmektedir. Veriler üçüncü taraf siteler ve hizmetler tarafından reklamların sunulması ve izlenme oranlarının değerlendirilmesi başta olmak üzere net olarak belirtilmemiş birçok amaç için kullanılabilir (Common Sense, 2021).

3.3.2.5. Cortana

Cortana Microsoft tarafından geliştirilen ve ilk kez 2014'teki Build konferansında tanıtılan bir sesli asistan uygulamasıdır. Hem Windows'un mobil telefonlarına hem de Windows 10 destekli bilgisayarlara entegre edilmiştir (Corden, 2017). Geliştiriciler yalnızca günlük işlerde yardımcı olan basit bir asistan değil, aynı zamanda kullanıcı alışkanlıklarını öğrenerek ileriye dönük bir şekilde yanıt veren, kısacası gelişebilen bir akıllı sistem oluşturmayı hedeflemişlerdir (Warren, 2014).



Resim 7. Cortana'nın arayüzü

Kaynak: <https://www.shutterstock.com>

Cortana, gelişebilen bir akıllı sistem oluşturmak için Microsoft Research tarafından geliştirilen makine öğrenimi algoritmalarını kullanırken, internetten bilgi sağlamak içinse Bing'in arama motorundan yararlanır (Corden, 2017). “Hey Cortana” uyandırma cümlesi ile aktifleşebilir. Cortana ile kullanıcı takvim düzenleyebilmekte, hatırlatıcı ve alarm kurabilmekte, kullanıcı komutuyla telefonda yer alan diğer uygulamaları başlatabilmektedir (Asus, 2021). Microsoft'un web sayfasındaki bilgilerde belirtildiği üzere (Microsoft Support/Cortana ve gizlilik) Cortana'yı kullanabilmek için bir kullanıcı hesabı oluşturulmalıdır. Cortana ilk etkinleştirmede isim, favori film,

yemek vs. gibi kişisel bilgi ve zevklere dair sorular sorar (Warren, 2014). Ayrıca kullanıcı, oturum açılan cihazdaki bilgilere erişim için izin vermiş sayılır. Kullanıcının deneyimi kişiselleştirmek için derleneceği belirtilen kişisel verilerin toplanmasını durdurma yetkisi vardır. Microsoft verilerin reklam amaçlı kullanılmayacağını ifade etse de Bing ile yapılan aramalarda reklamların bulunacağını da belirtir. Ayrıca ses verilerinin derlendiğini de kabul eden Microsoft, bunun kullanıcı izni dahilinde olduğunu belirterek verilerin “dil anlama ve makine öğrenimi modellerini geliştirmek için” kullanılacağını söylemektedir.

Common Sense’e göre (2021) Cortana web sayfasında her ne kadar reklam amaçlı veri paylaşımı yapılmayacağı belirtilmiş olsa da uygulamanın beraber kullanıldığı diğer hizmet sağlayıcılar aracılığıyla veri paylaşımı mümkündür. Kullanıcı bilgileri üçüncü kişilere aktarılabilir çünkü bu verilerin aktarılmadan önce silinip silinemeyeceği bilgisi belirsizdir.

BÖLÜM IV

KUŞAK KAVRAMI

Toplum yapısı gereği zamanla değişir. Toplumsal değişme toplumun kültürünün gelenek, görenek, dil, düşünce yapısı gibi manevi unsurlarına yönelik olabileceği gibi, mimari, teknoloji, giyim-kuşam, yeme-içme vs. gibi maddi unsurlarına yönelik farklılaşmalar olarak da ifade edilebilir (Aydın ve Baran, 2010).

20. yüzyıldan bugüne toplumsal yapıdaki farklılaşmalar incelendiğinde bugünün bilgi toplumu için bu değişimin en etkili nedenlerinden bir tanesinin yeni bilgi teknolojilerindeki gelişmeler olduğu söylenebilir. Teknolojinin toplumu şekillendirdiğine yönelik farklı görüşler olsa da teknoloji ve toplum arasında sürekli bir ilişki ve birbirini dönüştürme hali olduğu açıktır. Teknolojik deterministlere göre teknolojinin gelişimi toplumsal değişimin başlıca belirleyicisidir (Kline, 2015). “Biz araçlarımızı şekillendiririz ve daha sonra onlar bizi şekillendirir”. John M. Culkin’in McLuhan’ı anlattığı bir makalesinde (1967, s. 2) geçen bu yorum, teknolojik deterministlerin teknoloji-insan ilişkisine bakış açısını kısa ve öz bir şekilde ifade eder. İnsan doğayı taklit ederek çeşitli teknolojiler icat eder ve teknoloji sürekli olarak gelişmeye devam eder; bununla birlikte insan bu teknolojiler tarafından büyütülür, kontrol edilir ve değiştirilir (Hurme ve Jouhki, 2017).

Teknolojinin insan üzerindeki etkisinin çok az araştırmacı tarafından reddedilebileceğini düşünen Mackenzie ve Wajcman’e karşı (1999, akt. Dafoe, 2015), Duan, Zhang, Song ve Han’a göre (2020), teknolojinin üzerinde toplumsal değişimlerin bir belirleyiciliği yoktur. Aynı zamanda teknolojinin kuşaktan kuşağa etki edecek derecede büyük çapta bir değişimin tetikleyicisi olamayacağını varsayan görüşler de vardır. Wyatt’a göre (2008) tarihsel dönemleri ve bu dönemlere ait toplumları teknolojik icatlar çerçevesinde adlandırma, teknolojinin etkilerine göre birbirinden ayırmak eksik bir bakış açısıdır. Her dönemde her topluma etki eden etmenler, özellikle de yalnızca teknolojik etmenlerden bahsedildiği durumlarda, çoğunlukla birbirinden farklılaşır. Teknolojik determinizmin indirgemeci bakış açısını eleştiren bu görüş toplumsal inşacılıktan beslenerek “teknolojinin sosyal inşası” olarak adlandırılır. Toplumsal inşacılar, teknolojinin toplumun sosyal davranışlarını ve karakterini belirlediği fikrini tamamen inkâr etmeden, bu teknolojileri tecrübe eden toplumlarda ortaya çıkacak yorum farklılıklarının üzerinde durmuşlardır. Aynı zamanda teknolojinin toplumdan

soyut bir şekilde, bilimi temel alarak kendi gelişim mantığı ekseninde geliştiği düşüncesine karşıdır. Toplumsal inşacılar teknolojinin de toplumdan etkilendiği, etkileşimin karşılıklı olduğunu savunarak teknolojik gelişmelerin çeşitli sosyal, kültürel, ekonomik ve politik faktörlerce şekillendirildiğini iddia ederler (Johnson, 2021).

Tarihi çağları başlatan ve bitiren birçok buluş, hatta taşın veya demirin kendisi bile bugün sahip olduğumuz teknolojinin hammaddeleridir denilebilir. Dafoe'ye (2015) göre sorulması gereken soru, tarihte hangi teknolojilerin hangi sosyal grupları ne derecede etkilediği olmalıdır. Günümüzde yeni medya araçlarının kullanım yaygınlığı, toplumlarda eğitim, sağlık, sosyalleşme, alışveriş, eğlence alışkanlıkları gibi birçok alışkanlığı değiştirmiş, bu araçları kullanan bireylere kendilerini ve dünyayı tanımak adına yeni biçimler sunmuştur. Tarihsel süreçte teknolojik değişimin bu kadar ivme kazanmadığı dönemlerde, teknolojinin kuşak farklılıkları üzerindeki etkileri daha az hissedilse de bugünün teknolojisinin bireylerin düşünme ve kendilerini ifade etme biçimleri üzerindeki etkisi yadsınamazdır.

Kuşak sözcüğü TDK tarafından "Yaklaşık olarak aynı yıllarda doğmuş, aynı çağın şartlarını, dolayısıyla birbirine benzer sıkıntıları, kaderleri paylaşmış, benzer ödevlerle yükümlü olmuş kişilerin topluluğu" ve "Yaklaşık yirmi beş otuz yıllık yaş kümelerini oluşturan bireyler öbeği, göbek, nesil, batın, jenerasyon" olarak tanımlanmıştır³. Bu tanımlardan da anlaşılacağı gibi toplumun genç bireylerinin yeni bir kuşak olarak adlandırılması için belirli bir süreç içerisinde önceki kuşaklardan farklılaşmaya neden olan etkenler olması gerekir. Kültürel nedenler, politik nedenler, bilgi ve ardından bilgi teknolojileri toplum üyelerinin yaşayış biçimini yeni bir nesle özgü hale getirerek, özellikle de insanların nasıl iletişim kurduğu konusunda hızlı bir evrime neden olup, bu farklılaşmalardaki en büyük payı sırtlanmıştır (Dimock, 2019). 1946- 1964 yıllarında doğanları kapsayan Bebek Patlaması (Baby Boomers) Kuşağı için televizyonun icadı ve gelişimi, bu dönemin bireylerinin yaşam tarzlarını ve dünyayla bağlantılarına önemli etkilerde bulunduğu söylenebilir. 1965-1979 yılları arasında doğanların oluşturduğu X Kuşağı bilgisayarın icadına ve 1980-1999 arası doğanların bulunduğu Y kuşağı ise internetin icadı ve geliştiği dönemlere tanık olmuştur. 2000 yılı ve sonrası doğan Z kuşağı ise yakın geçmişte geliştirilen ve bugün hala kullanılan teknolojilerle birlikte büyüyen bireylerdir.

Kuşak (generation) kavramını sosyolojik alanda ilk kez teorileştiren isim Karl Mannheim'dır. Mannheim "The Problem of Generations (Nesillerin Sorunu)" başlıklı

³ <https://sozluk.gov.tr/>

makalesinde ortaya koyduğu "kuşak teorisi" ile bir kuşağa ait olmanın yalnızca doğum yılından ibaret olmadığını, o kuşağın temsilcilerinin ortak bir tarih ve ortak deneyimler paylaşması gerektiğini ifade eder (Knight, 2009). Mannheim, bu teoriyi anlamak için belirli bir kuşağı oluşturan bireylerin ilişkilerinin gözlemlenmesi sürecinin önemli olduğunun altını çizer, çünkü kuşağın bütünlüğü bireylerin fiziksel yakınlığıyla değil, aralarındaki birlik duygusuyla sağlanır (Mannheim, 1952). Bu bireyler arasında bir birlik oluşturan sosyo kültürel ortaklıklar, bir önceki kuşakla da farklılıklar yaratır (Troksa, 2016).

Norman Ryder (1965), demografik ve sosyolojik alanlarda yaptığı çalışmalar sonucunda İkinci Dünya Savaşı sonrası kuşağı olan Bebek Patlaması Kuşağını incelemiş ve demografik bulguların çok daha ötesinde çıkarımlara varmıştır. Ryder, o dönemde nüfusun ölüm ve doğum oranlarını karşılaştırırken birbirini takip eden doğum gruplarının, diğer bir ifadeyle nesillerin eğitim, sosyalleşme ve tarihsel deneyimlerin değişmesiyle birlikte farklı deneyimler edindiğini ortaya koyar. "Bir bireyde yaşamı boyunca meydana gelen değişiklikler, bir parçası olduğu popülasyondaki değişikliklerden ayırt edilebilir." (Ryder, 1965, s.843) diyerek toplumsal değişme kavramına vurgu yapmıştır. Biyolojik olarak bir canlı nasıl doğuyor, gelişiyor ve ölüyorsa; aynı şey toplumlar için de geçerlidir. Sosyalleşme, bireyi toplumsal tasarıma uygun hale getirmenin önemli bir yoludur (Ryder, 1965) ve nasıl sosyalleşileceği bile aslında o kuşağın yapısına özgüdür.

1990'ların başında, hayatın her yönden hız kazanmasıyla kuşak teorilerine dair araştırmalar daha fazla önem kazanır. Neil Howe ve William Strauss (1992) "Yeni Kuşak Farkı (The New Generation Gap)" başlıklı makalede 1961-1981 arası doğan kuşak (yazar Douglas Coupland'ın romanından sonra X kuşağı olarak anılan ve makalede Howe ve Strauss tarafından "13. Nesil" olarak ifade edilen kuşak) ile bir önceki nesil olan Bebek Patlaması Kuşağı arasındaki farklılıklara değinerek eski ve yeni nesil karşılaştırması yapar. Howe ve Strauss yalnızca yeni bir kuşak teorisi geliştirmekle kalmaz, aynı zamanda Mannheim'in çalışmalarında yer alan, tarihin etkilerinin bir nesli şekillendirdiği ifadesini ileri taşıyarak, aslında bir neslin de tarihe şekil verebileceğini ortaya koyar (Knight, 2009). Geliştirilen teoriye göre kuşaklar tarihsel süreçteki "kriz" ve "uyanış" anları olarak adlandırılan önemli olayların etkisiyle şekillenir; daha sonrasında ise bu nesil benzer şekilde bir sonraki döngünün kriz (toplumsal kenetlenmeyi gerektiren tehditler) ve uyanış (bireysel gelişmelere ve değerlere odaklanan olaylar) olaylarını tetikler ve bu böylece devam eder (Howe ve Strauss,

1991). Bu döngüler içerisinde kuşaklar çeşitli arketiplere sahip olur ve bunlar üzerinden tanımlanır. Bu kuşak teorisi o yıllarda popüler olmuş olsa da sınırlayıcı olması nedeniyle çokça eleştiri almıştır (Duymaer van Twist ve Newcombe, 2017).

4.1. Dijital Yerliler ve Dijital Göçmenler

Kuşaklar teorisi, belli tarihsel dönemlerde doğan grupların benzer yaşam deneyimlerine sahip olduğunu ve bu nedenle benzer becerilere, karakter özelliklerine, bakış açılarına sahip olabileceğini iddia eden tek teori değildir. Marc Prensky (2001), nesilleri doğdukları yıllara göre sahip oldukları varsayılan teknolojiyi kullanma becerilerine göre sınıflandırarak "dijital yerliler" ve "dijital göçmenler" kavramlarını ortaya çıkarmıştır. Bir yazar ve eğitim konuşmacısı (speaker on education) olan Prensky'nin bu kavramlara ihtiyaç duymasının temelinde, dönemin eğitim sisteminin artık yeni nesil öğrencilere hitap etmediğini düşünmesi yer almaktadır. 2001 yılının öğrencileri ile önceki yılların öğrencileri arasındaki bu hızlı ve büyük kopukluğun nedeni teknoloji araçlarının hızla gelişmesi ve daha yeni nesillerin bu gelişmelere çok daha kolay uyum sağlayabilmesidir. Bilgisayar, internet, video oyunları, video kameralar, cep telefonları gibi medya araçlarını aktif bir şekilde kullanan bu neslin bilgiyi algılayış ve işleyiş şekilleri de farklılaşmıştır. McLuhan'ın teknolojik araçları insan bedeninin bir uzantısı, bir uzuv gibi kabul etmesine benzer bir şekilde, Prensky de "yerlilik-anadili konuşan kişi" benzetmesiyle yeni dijital teknolojileri insani yeterliliği artıran, insanın düşünme, hissetme ve tepki verme kapasitesini iyileştiren (Varol ve Varol, 2019) araçlar olarak ele alır.

Prensky dijital dünyanın içinde doğmamış ancak bu teknolojilerle hayatlarının bir bölümünde tanışmış olan kişileri ise "dijital göçmenler" olarak adlandırır. Bu gruptakiler değişen düzene uyum sağlayabilmek adına dijital araçları kullanmayı tercih ederler (Askım Kurt, Güneç ve Ersoy, 2013). Aslında bu kavramların ilk kez dile getirildiği yıllarda bu teknolojilere alternatif sayılabilecek yollar hala hayatın bir parçası denilebilirdi, fakat günümüzde dijital göçmenlerin son üyeleri için bile bu araçların artık zorunluluk haline geldiği rahatlıkla söylenebilmektedir. Dijital göçmenler teknolojiyi ne kadar iyi kullansalar da teknoloji-öncesi alışkanlıklarını koruma eğilimleri daima olacaktır, Prensky bu alışkanlıkları dijital göçmenlerin "aksanları" olarak adlandırır.

Y Kuşağı öncesi doğanlar dijital göçmenler sayılırken, Y Kuşağı ve 2000 sonrası doğan, Z Kuşağı olarak adlandırılan kuşak, dijital yerlilerin en son yetişkin üyeleridir.

2010 yılından itibaren doğanların dahil olduğu Alfa Kuşağı ise günümüzün en genç dijital yerlileri sayılmaktadır.

4.1.1. Dijital Yerliler

Dijital yerliler, 1980-1994 (Prensky, 2001) yılları arasında doğmuş, birçok teknoloji tabanlı aracı aktif ve iyi derecede, hatta aynı anda kullanabildiği varsayılan (Brown, 2000) bireylerdir. Dijitalleşme süreci içerisinde doğan ilk kuşak oldukları için “yerli” olarak adlandırılan bu kuşağın bireyleri için dijital araçların tümü, internet ve sosyal medya araçları yaşam tarzlarıyla sıkı sıkıya bağlıdır; çünkü onlarsız bir yaşam tecrübe etmemişlerdir. Teknolojiyi iyi kullanabilme becerileri, takım çalışmasına yatkınlıkları, aynı anda birkaç işi birden yapabilme gibi özelliklere sahip oldukları kabul edilmektedir (Brown, 2000). Prensky'e (2001) göre dijital yerlilerin bilgiyi işleme ve öğrenme yöntemleri kendilerine özgüdür; görsel bilgilerle ve oyun tabanlı etkinliklerle daha hızlı öğrenmeye yatkındırlar. Tappscott (2008, s.4) “Ağ kuşağı” olarak adlandırdığı bu kuşağın bireylerine önceki kuşaklara kıyasla daha cahil, iletişim yönleri zayıf, okumayan, spor yapmayan ve internet bağımlısı bir kuşak oldukları yönünde eleştiriler geldiğini belirtmiştir. Fakat Tappscott’a göre bu kuşağın baktığı perspektif öncekilerden açıkça farklıdır çünkü teknolojiyi onunla birlikte büyüyerek özümsemişlerdir ve uyum sağlamak zorunda kalmamışlardır. Önceki nesillerin deneyimlerinin ise “iletişim kurmanın, bilgiye erişmenin ve kendini eğlendirmenin yepyeni bir yolunu öğrenmek ve buna uyum sağlamak” (s. 18) olduğunu söyler. Bununla birlikte okuyarak öğrenmeyi video izleyerek öğrenmekten daha çekici ve faydalı kılan noktaların neler olduğu da tartışmaya açıktır. Bu görüşlere karşın Bennett, Maton ve Kervin'in (2008) araştırması çoklu görevleri yerine getirebilme, hızlı öğrenebilme gibi becerilerin belirli bir kuşağa özgü durumlar olmadığını, yalnızca gelişen teknoloji ile birlikte kuşakların kullandıkları araçların değiştiğini ifade eder. Dijital yerlilerin sahip olduğu varsayılan davranış ve özelliklerin bu grupta yer alan bütün bireyler için genelleyici olması, toplumda bu kişilerin tümünden teknoloji alanında yetenekli olması beklentisi yaratmaktadır ve teknolojiyle ilgilenmeyen veya bu alanda daha az yetenekli bireylerin ihmal edilmesine, erişimi kısıtlayan sosyo-ekonomik ve kültürel faktörlerin göz ardı edilmesine neden olmaktadır (Bennett, Kervin ve Maton, 2008). Çoğu öğrenci çeşitli teknolojileri deneyimlemiş olsa da genel bir teknoloji kabiliyetinden söz edebilmek mümkün olmadığı gibi, her teknoloji tabanlı araç eşit

oranda kullanılmamaktadır (Ching, Basham ve Jang, 2005; Kennedy, Krause, Judd ve diğ., 2006; Wang, Myers ve Sundaram, 2012). Aynı zamanda kavramlar uzun yıllar önce adlandırıldığı için güncel bir tanımlanmaya da ihtiyaç duyulduğu söylenebilir.

Türkiye’de bilgi ve iletişim teknolojilerinin kullanımının yaygınlaşmasına bağlı olarak dijital yerli kavramının ne ifade ettiği ve hangi kuşakları kapsadığı konusunda daha önce çeşitli araştırmalar yapılmıştır. Kakırman Yıldız 2012 yılında 1987-1994 yılları arasında doğan Marmara Üniversitesi öğrencileri ile yaptığı araştırmasının sonucunda analog dönemden dijital döneme geçiş dönemine denk gelen bu yaş grubunu “dijital melezler” olarak adlandırmayı önermiş ve Türkiye’de dijital yerlilerin daha çok 2000 sonrası doğanları kapsaması gerektiğini ifade etmiştir. Bilgiç, Duman ve Seferoğlu (2011) dijital yerlilerin eğitim alanına ilgi duymaları ve bu alanda başarı gösterebilmeleri için teknoloji tabanlı eğitim anlayışı benimsenmesi gerektiğine vurgu yapmaktadır. Eşgi (2013) dijital göçmen olan ebeveynler ile dijital yerli çocuklarının teknoloji kullanım alışkanlıklarını karşılaştırarak iki kuşak arasındaki farklılıklardan bahsetmiştir. Eşgi’ye göre (2013) bu farklılıkların en önemlisi internette geçirilen süredir ve dijital göçmenler için doğal olan internet kullanım süresinin ebeveynler tarafından internet bağımlılığı olarak adlandırıldığını ifade ederek iki kuşak arasında bu gibi farklılıklardan doğan çatışmalar yaşanabileceğini dile getirir.

4.1.2. Dijital Göçmenler

1980 öncesi doğan bireylerin içinde bulunduğu dijital göçmenler, bilgi ve iletişim teknolojilerini kullanmayı sonradan öğrenen ve teknolojiye uyum sağlamak zorunda kalmış olan bireylerdir. Bu nedenle dijital araçları dijital yerliler kadar etkin bir şekilde kullanamayacakları varsayılır. Bu bireyler teknoloji söz konusu olduğunda daha “geleneksel” bir düşünme yapısına sahiptirler; yeni teknolojileri daha yavaş öğrenirler (Kurt, Günüş ve Ersoy, 2013).

Bu kavramlar kuşak teorilerinde olduğu gibi doğum yılları baz alınarak belirlendiği için sınırlayıcıdır. Dijital yerli ve dijital göçmenlerin doğdukları varsayılan dönemlerin kesinliğine dair araştırmalar yeterli değildir (Kurt, Günüş ve Ersoy, 2013). Bu nedenle her ne kadar yaklaşık olarak bu dönemlerde doğanlar için kullanılabilecek olsa da her bireyin bu grupların tüm özelliklerini göstermesi beklenemez. Bu aynı zamanda dijital göçmenlerin tümünün teknolojiye dijital yerlilerden daha az hâkim olabileceği kanısı kadar genelleyicidir. Bu sınırlılık beraberinde iki temel sorunu

meydana getirir, yaş ve erişilebilirlik (Wang, Sundaram ve Myers, 2012). Dünyanın her yerinde aynı yaş grupları teknolojiyi kullanabilme becerisine aynı oranda sahip değildir. Cinsiyete göre de teknoloji kullanımında farklılıklar görüldüğü iddia edilmektedir. Yapılan bazı araştırmalara göre teknoloji kullanımında bir cinsiyet eşitsizliği söz konusudur çünkü kadınlar hem bilgisayar kurslarına hem de evde bilgisayar başında zaman geçirmeye daha az yatkınlık göstermektedir (Ching, Basham ve Jang, 2005). Kaliforniya Üniversitesinin yayınlamış olduğu verilere göre⁴ (2021) matematik ve bilişim sektöründe çalışan kadın sayısı 1995'ten bu yana %19 azalmıştır. Araştırmalar sonucunda kesin yargılara varılmamışsa da dijital teknolojilere karşı erkeklerin daha yetenekli olduğuna dair toplumsal bir ön kabul ve erkeklerin ilgi ve öğrenimlerinin daha çok teşvik edilmesi bu sorunun gerekçeleri arasında gösterilebilir. Erişilebilirlik sorunu ise internet ve diğer dijital araçlara erişimin herkes için mümkün olmamasıdır. Statista'nın 2021 verilerine göre dünya çapında 4,66 milyar aktif internet kullanıcısı vardır ve bu da küresel nüfusun yüzde 59,5'ine denk gelmektedir (Statista, 2021). Uluslararası Telekomünikasyon Birliği'nin 2021 yılında yayınlanan raporlarına göre ise dünya nüfusunun yüzde 37'si hala internet kullanmamıştır (ITU, 2021). Dünya çapında dijital bağlantı oranlarına bakıldığında zaman zaman dijital yerli ve dijital göçmenler tanımlanırken kuşaksal bir ayırım yapmak fazlasıyla eksik bir tanım olacaktır.

Görüldüğü gibi literatürdeki dijital yerliler ve dijital göçmenler hakkındaki görüşler farklılıklar göstermektedir. Genel görüş, kuşaklar arasında teknoloji kullanımına dair temel farklılıkların bulunduğu ancak bunun kuşak farklılığından ziyade ekonomik, sosyal eğitimsel ve davranışsal faktörlere bağlı farklılıklardan kaynaklandığıdır.

4.2. Kuşakların Mahremiyet Algısı

Kuşaklar arası farklılıklar çoğu zaman genelleyici olsa da tarihsel deneyimlerden ötürü her kuşağın farklı bir yaşam tarzı vardır, dolayısıyla internet kullanımı ve bu kullanımın neden olduğu mahremiyet ihlalleriyle ilgili duydukları kaygılar da farklılaşmaktadır. Bu bölümde X, Y ve Z kuşaklarının çevrimiçi mahremiyet ve güvenlik anlayışlarındaki farklılıklar ele alınmıştır.

⁴ <https://ischoolonline.berkeley.edu/blog/women-computing-computer-science/>

4.2.1. Y ve Z Kuşağının Mahremiyet Algısı

Z kuşağını önceki nesillerden farklı kılan dijital teknoloji araçlarının icadının hızlandığı yıllarda doğmaları ve bu yenilikleri deneyimleme imkanlarının hayat boyu sürececek olmasıdır. Üstelik özellikle bu grubun bireyleri, önemli bir parçası oldukları dijital kültürü sürekli dönüştürmektedirler. Üç kuşak (X, Y ve Z) arasında cep telefonu kullanım oranının en fazla olduğu grup Z kuşağıdır (Pasztor ve Bak, 2021). Z kuşağı, günümüzde popüler sosyal medya platformlarına içerik üretmek, trend yaratmak, internet ve sosyal medyadaki çoğu güncel gelişmeyi takip etmek yönünde istek duydukları ve başarılı olmaya yatkın oldukları söylenebilir. Bu da onları teknolojiye zamanla adapte olmuş ve yeni teknolojileri kabul etmeye zaman zaman direnç gösteren, bu konuda zorluklar yaşamış kabul edilen X kuşağından ayırmaktadır. Z kuşağına dahil edilen yaş grupları dijital araçların normalleştiği bir dünyaya doğmuş ve teknolojiyi benimseme sürecinden geçmemiştir. Dijital araçların kullanımı bir zorunluluk halini almıştır. Dolayısıyla bu neslin mahremiyetle ilgili endişeleri ve tutumları önceki nesillerden daha farklıdır.

Z Kuşağı, Parker ve Igielnik'in "What We Know About Gen Z So Far (Z Kuşağı Hakkında Şimdiye Kadar Bildiklerimiz)" (2020) sonucunda bu zamana kadarki en eğitilmiş nesil kabul edilmektedir. Amerika merkezli araştırmanın sonuçlarına göre X ve Y kuşağına kıyasla liseyi bırakma oranları daha düşüktür ve üniversiteye kaydolma olasılıkları daha yüksektir. Dolayısıyla yine bu bireylerin mahremiyet ve bilgi güvenliği endişelerinin yüksek oranda olması beklenebilen bir durumdur. Eğitim seviyesi ile mahremiyet önlemleri arasında doğrusal bir ilişki bulunduğu bilinmektedir (Hoel ve Chen, 2018; Park ve Vance, 2021). SSA'ların geliştirildiği yıllara şahit olan Z kuşağı için bu asistanların mahremiyet endişesi yaratmasına ilişkin yapılan bir çalışmada (LoupVentures, 2019) evde akıllı hoparlör sistemi olanların %31'inin, cihazın sürekli dinleme modunda olduğuna dair endişeleri olduğu ortaya çıkmıştır; %33'ünün orta boyutta endişe ve %21'inin hafif boyutta endişe duyduğunu belirtmiştir. Ayrıca Z kuşağından evlerinde akıllı hoparlörleri olanların %84'ü bilgisayar korsanlarına karşı savunmasız olduklarına inanmaktadır.

Bütün bu beklentilere karşın Z kuşağının, taşıdığı tüm endişeler ise mahremiyete dair edindiği tüm eğitim, bilgi ve tecrübeye rağmen, bu kuşağın üyeleri arasında oldukça yüksek olduğu fakat yine de kendilerine sunulan birçok teknolojiyi kullanmaya devam ettikleri ortaya çıkmaktadır (Herman, 2019; Henley, 2013; Steeves, 2014; Boyd

ve Marwick, 2011 ve diğ.). Günümüzde Nesnelerin İnterneti denilen, ilk olarak 1999 yılında Kevin Ashton tarafından tanımlanan IoT (Internet of Things) (Gokhale, Bhat ve Bhat, 2018) internet tabanlı akıllı cihazların birbirini destekleyen yazılımlar sayesinde birbirine entegre olabilmesi anlamına gelmektedir (IBM, 2016). Yaygınlaşmasındaki hız Z kuşağına veri gizliliğinin neredeyse imkânsız olduğunu düşündürse de, kişiselleştirilmiş bir deneyim için veri paylaşımına açık olma fikrine sıcak bakmaktadırlar. Kısacası bu durumu kabullenme eğilimi göstermektedirler. Kişisel verilerin ifşa olma riskinin farkında olmakla beraber bu verileri ifşa etme davranışını gösterme durumu literatürde “gizlilik paradoksu” olarak adlandırılmaktadır (Liyanaarachchi, 2021). Y ve Z kuşağı kullanıcıların faydalanacağı hizmetler adına kişisel verilerin işleme ve saklanma riskinin olduğunun daha çok bilincinde olsa da bunu kabul etmeye de daha fazla eğilim gösterir. Her ne kadar dijital şeffaflık konusunda açık fikirli eğilimler gösterebilirler de çoğunluk şirketlerin kendileri hakkında hangi verileri işliyor ve saklıyor olduğunu bilmenin bir insan hakkı olduğu kanaatinde (Martinez, 2021).

Y kuşağı, Z kuşağından önce dijitalleşme süreci ile ilk karşılaşan nesildir. Dijital mahremiyet konusuna yaklaşımları Z kuşağıyla benzerlikler taşımaktadır. Ponemon Institute’nün araştırmalarına göre (Infosecurity, 2014) Y kuşağı kişisel verilerine erişime karşı kayıtsız olan ve verilerini gizli tutmakla ilgilenmeyenlerle, verileri için endişelenen fakat onları korumak konusunda çok az girişimde bulunanlar olarak iki gruba ayırmaktadır. Bununla birlikte dijital ortamda verilerini korumak adına alınabilecek önlemlere hâkim oldukları için gizlilik ayarlarını düzenlemek istediklerinde bunu yeterli düzeyde gerçekleştirebilmektedirler.

4.2.2. X Kuşağının Mahremiyet Algısı

X kuşağı, mahremiyet anlayışı söz konusu olduğunda kendisini yetiştiren kuşakların geleneksel anlayışları ve büyürken maruz kaldığı dijitalleşen dünyanın modern gerçekleri arasında bocalamış bir kuşaktır. İnternetin yaygınlaştığı yıllar X kuşağının ergenlik ve erken yetişkinlik dönemlerine denk gelmektedir. Bu nedenle teknolojiyi halihazırda şekillenmiş öğrenme yöntemleriyle tecrübe etmek zorunda kalmışlardır. Bu da zaman alan bir süreç olmuştur zira internetin yaygınlaşması da ülkeden ülkeye değişmekle birlikte zamana yayılan bir süreçtir. X kuşağı bireyleri interneti, e-postaları kontrol etmek, gazete ve blogları okumak, akademik araştırma

yapmak ve sosyalleşmek gibi amaçlar için kullanılmaktadırlar (Yılmaz ve Özkoçak, 2010). 2021 itibarıyla X Kuşağının %74'ü sosyal medya kullanıcısıdır ve bu oranla dijital göçmen sayılan kuşaklar arasında sosyal medyayı en hızlı benimseyen kuşak kabul edilmektedir (Chivers, 2021).

Salesforce'un 2018 verilerine göre Y kuşağı ve Z kuşağının yüzde 63'ü kişisel verilerinin şirketler tarafından nasıl kullandığını anladıklarını söylerken; X kuşağı ve sonrasının yalnızca yüzde 47'sinin bu konuda bilgisi olduğu ortaya çıkmıştır. İnternet kullanımında risk almaktan çekinen X kuşağı, her ne kadar büyük oranda sosyal ağ kullanıcılarından oluşsa da bu kullanıcılar çoğunlukla bildikleri platformlara bağlı kalma eğilimindedirler (Koch, 2019). Bu platformların başında Facebook gelmektedir; Y ve Z kuşağı içinse bu platform Instagram'dır (Alptekin, Türkmen ve Arslantaş, 2021).

X Kuşağı için çevrimiçi gizlilik bilinen fakat çok hâkim olunamayan bir problemdir. Birçok kullanıcı dijital ortamlarda mahremiyetin ihmal edilme riskinin söz konusu olduğunu tahmin edebilse de buna dair nasıl önlem alınacağı konusunda yeterli bilgiye sahip olmayabilmektedir. Vyver ve McDonald (2018), X kuşağının dijital ortamlarda mahremiyet adına dikkat etmesi gereken başlıca noktaların güçlü bir parola edinmek, güvenilir ağları ve antivirüs yazılımları kullanmak olduğunu vurgulamaktadır.

BÖLÜM V

YÖNTEM VE BULGULAR

5.1. Araştırmanın Yöntemi ve Kapsamı

Araştırmada örneklem olarak Çukurova Üniversitesi İletişim Fakültesi seçilmiştir. İletişim Fakültesi öğrencilerinin seçilmesindeki temel gerekçe, bu öğrencilerin yeni medya araçlarının sadece kullanıcısı olmayıp, araçların avantajları yanında toplumsal yaşam açısından dezavantajlarını da araştırıyor oldukları varsayımdır. Ayrıca dijital yerliler olarak adlandırılan bu bireylerin dijitalleşmenin hızlandığı dönemlerde doğmuş olmalarından dolayı dijital teknolojileri aktif ve iyi derecede kullanabildikleri varsayılmıştır. Örneklem yöntemi olarak ise olasılıklı olmayan örneklem türlerinden amaçlı ya da amaçsal örneklem yaklaşımı benimsenmiştir. Bu örneklem türünde araştırmacı, çalışmasının sorunsalına uygun olarak görüşülecek kişileri belirler. Amaçlı örneklem yöntemi, araştırmanın kriterlerine uygun yapıdaki grubun belirlenmesine ve derinlemesine araştırma yapılmasına olanak sağlamaktadır (Koç, 2017). Çukurova Üniversitesi İletişim Fakültesi öğrencilerine çevrimiçi ortam üzerinden yapılan çalışmaya ilişkin duyuru sonucunda SSA kullandığını söyleyerek araştırmaya gönüllü olarak katılmak isteyenler araştırmacıya yine çevrimiçi ortam üzerinden geri dönüş yapmışlardır.

Araştırmada nitel araştırma deseni esas alınmıştır. Karataş'a (2015, s. 63) göre nitel araştırma “disiplinler arası bütüncül bir bakış açısını esas alarak, araştırma problemini yorumlayıcı bir yaklaşımla incelemeyi benimseyen bir yöntemdir.” Araştırma için izlenen veri toplama tekniği araştırmada elde edilmek istenen verilere göre değişebilirken, bu araştırma için seçilen yöntem görüşme yöntemidir. Görüşme yöntemi katılımcıların düşüncelerini, bakış açılarını, tecrübelerini, değerlerini ve algılarını açığa çıkarmak için etkili bir yöntemdir (Karataş, 2015). Görüşme öncesi katılımcılara çalışmanın içeriği ve görüşme hakkında bilgi verilmiş, ardından görüşmenin kayda alınması için yazılı ve sözlü onayları alınmıştır. Görüşmeler pandemi koşulları nedeniyle Microsoft Teams uygulaması üzerinden tüm katılımcılarla tek tek ve çevrimiçi olacak şekilde gerçekleştirilmiştir. Araştırma için elli bir (51) gönüllü ile derinlemesine görüşme gerçekleştirilmiştir. Görüşmeler ortalama 10 dakika sürmüştür. Bir katılımcının görüşmesi daha sonra gizliliği ve bilgilerinin anonimliği konusundaki

endişelerinden dolayı kendi isteğiyle araştırmadan çıkarılmıştır. Görüşmeler için çalışmanın teorik çerçevesiyle uyumlu ve araştırma sorularına yanıt verecek 10 açık uçlu soru hazırlanmıştır. Görüşmeler uygulanma yöntemine göre yarı yapılandırılmış sorulara dayalı derinlemesine görüşmelerdir. Derinlemesine görüşme “açık uçlu soruların sorulması, dinlenmesi, cevapların kaydedilmesi ve ilişkili ilave sorularla araştırma konusunun detaylı bir şekilde incelenmesini mümkün kılar” (Kümbetoğlu, 2012, s.71). Yarı yapılandırılmış derinlemesine görüşme önceden hazırlanan sorular kapsamında ilerlerlerken aynı zamanda görüşmeci ve katılımcının görüşmenin akışına göre şekillenen esnek bir iletişim kurabilmesine olanak sağlar (Yüksel, 2020). Görüşme esnasında sorular katılımcılara sırasıyla yöneltilmiş, görüşmelerin tümünde görüşme gidişatı bu sorular çerçevesinde ilerlemiştir. Görüşmeler sonrasında verilerin işlenebilmesi adına alınan ses kayıtları deşifre edilmiştir. Deşifre işlemi, verilerin analiz sürecini kolaylaştırmak için alınan kayıtların metne dönüştürülmesi eylemidir (Çelik vd., 2019, s.384). Deşifre süreci tamamlandıktan sonra içerik analizi için önce eldeki veriler MAXQDA nitel veri analizi programı ile kodlarına ayrılmıştır. "Nitel veri terimi, sosyal bilimlerden gelir ve sayısal olmayan, yapılandırılmamış tüm veriler için bir şemsiye terimdir. Çoğu insan sayısal veriler altında hemen bir şeyler hayal edebilirken, nitel veriler söz konusu olduğunda bu o kadar kolay yapılmaz.” (Kuckartz ve Radiker, 2019, s.2). MAXQDA aracılığıyla yapılan kodlamalar aynı zamanda görüşmeden sayısal veriler elde edilmesine de olanak tanımıştır. Çalışmada bu veriler grafikler aracılığıyla gösterilmiştir.

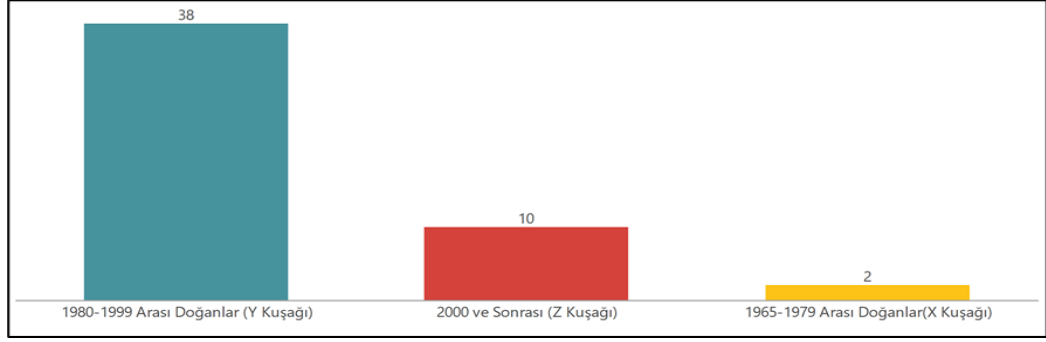
Nitel verinin nicelleştirilmesi; görüşme, gözlem veya dokümanların incelenmesi yoluyla elde edilmiş yazılı biçimdeki verinin, belirli süreçlerden geçirilerek sayılara veya rakamlara dökülmesidir. Sayılar ve rakamlar genellikle nicel araştırma türleriyle anılıyor olsa da nitel verinin belirli bir düzeyde sayılara indirgenmesi mümkündür. Nitel verinin sayılara indirgenmesinde amaç, istatistiksel yöntemlere başvurarak genellemeler yapmak veya sınırlı sayıdaki belirli değişkenler arasında ilişki aramak değildir. Zaten, nitel verinin doğası ve yapısı da buna izin vermez (Yıldırım ve Şimşek, 2003, s.177).

Çalışmada görüşme verileri kodlama yapılarak içerik analizine tabi tutulmuştur. İçerik analizi verileri kodlama işlemiyle detaylandırma yöntemidir. Bu kapsamda görüşme verileri sınıflandırılarak kodlara ayrılmıştır. Yıldırım ve Şimşek’e göre (2003, s.162) “...veriler, içerik analizinde daha derin bir işleme tabi tutulur ve fark edilemeyen kavram ve temalar bu analiz sonucu keşfedilebilir.” Kodlama, verilerin

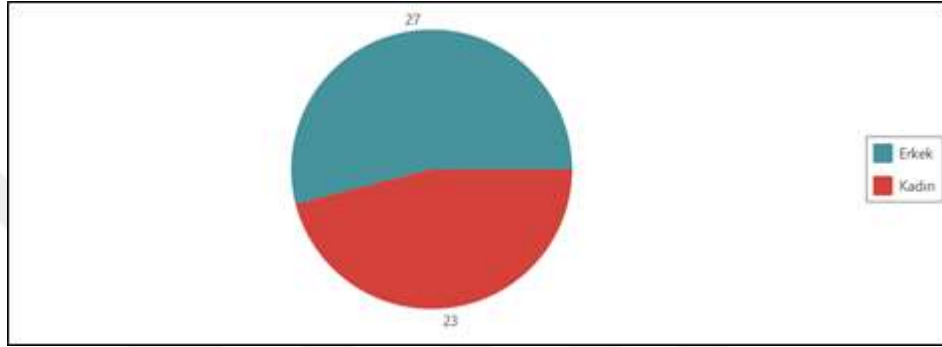
çalışma kapsamında ortaya çıkan ve vurgulanması önem arz eden parçalarını öne çıkarmak için işaretleme ve etiketleme işlemidir (Çelik vd., 2019). Ana kodlar ve alt kodlar belirlendikten sonra kodlama işleminin görselleştirilmesi için tablo ve istatistiksel grafikler kullanılmıştır. Görüşmelerin içeriğinin analiz edildiği bölümlerin başlığı ana kodları temsil etmektedir ve böylece içerik analizi tek tek başlıklar altında metinleştirilmiş görüşmeler üzerinden gerçekleştirilmiştir. Alt kodlar görüşme sonrası şekillendiği için Strauss ve Corbin'e (1990) göre "verilerden çıkarılan kavramlara göre yapılan kodlama" kabul edilmektedir. (Strauss ve Corbin, 1990'dan akt. Yıldırım ve Şimşek, 2003).

Araştırmaya 51 öğrenci katılmıştır. Öğrenciler SSA kullanıcısı olduğunu belirterek araştırmaya katkıda bulunmaya gönüllü olmuştur; ancak bir katılımcı görüşme sırasında SSA kullanmadığını ifade etmiştir. İki öğrencinin ise SSA kullanmadıkları, SSA'ya benzer sohbet botlarını kullandıkları ortaya çıkmıştır ve bu bulgular da yine araştırma analizi içerisinde değerlendirilmiştir. Öğrencilerden biri görüşme sonrası görüşme katılım formunu imzalamak istememiş, gizlilik endişeleri olduğunu belirterek görüşmeden çekilmek istemiştir, bu nedenle söz konusu görüşme araştırmanın dışında tutulmuştur. Öğrenciler farklı yaş gruplarından olup yaşları 21-55 yaş arasında değişmektedir. Böylece araştırmanın kuramsal çerçevesine uygun olacak şekilde her üç kuşaktan (X, Y ve Z) da öğrenci ile görüşülmüştür. Çalışma grubunun yaş ve cinsiyet dağılımına ilişkin bilgiler Şekil 1 ve 2'de verilmiştir. Grafiklere bakıldığında katılımcıların 38'inin Y kuşağından olduğu görülmektedir, 10 katılımcı Z kuşağından, 2 katılımcı ise X kuşağındandır. Katılımcıların çoğunluğu erkektir (27 katılımcı).

Çalışmada içerik analizi sonucu ortaya çıkan bulguların güvenilirliğinin sağlanması için alanda çalışma yapan iki akademisyenin görüşme verilerini incelemeleri sonucunda oluşturdukları kodlar ve alt kodlar da dikkate alınarak analizin nihai şekli verilmiştir.



Şekil 1. Katılımcıların yaş dağılımları



Şekil 2. Katılımcıların cinsiyet dağılımları

5.2. Araştırmanın Bulguları

Araştırma bulgularının analiz edilme sürecinin ilk etabında görüşmelerin deşifresi sonucu elde edilen veriler MAXQDA programına yüklenerek, görüşme verileri analiz edilmeye uygun hale getirilmiştir. Araştırmanın bu bölümünde, farklı katılımcılardan elde edilen bulgular arasındaki ilişkinin daha açıklayıcı ve daha sistematik şekilde görülmesini sağlamak için içerik analizi yapılmıştır. Bunun için 10 ana kod belirlenmiştir. Görüşme sorularının her biri birer tema kabul edilerek, ana kodlar bu şekilde oluşturulmuştur. Strauss ve Corbin (1990, aktaran Yıldırım ve Şimşek, 2003) bu kodlama biçimini “genel bir çerçeve içinde yapılan kodlama” olarak adlandırmaktadır. Bunun anlamı görüşmenin yapılacağı çerçevenin, yani görüşme sorularının, önceden belirlenmiş olduğu ve daha sonra bu çerçeve içerisinde ana kodların oluşturulduğudur. Bu ana kodlar ise katılımcıların cevapları doğrultusunda görüşme metinleri üzerinden etiketlenerek alt kodlarına ayrılmıştır. Ana kodlar, alt kodlar ve kodların kaç kez kullanıldığını gösteren sıklık (frekans) oranları tablo haline getirilmiştir (Tablo 1). Kodlanmış bölümlerin tablo halinde görselleştirilmesi ve incelenmesi frekans analizi olarak adlandırılmaktadır.

Kodlamalarla oluşturulan grafiklerin bazılarında katılımcı sayısı ve kodlama sıklıklarının eşit olmadığı görülmektedir. 50 katılımcıya karşılık olarak, 50’den daha fazla veya daha az kodlama yapılmış olabilir. Bunun nedeni katılımcıların bazı sorulara yanıt vermemiş olmasından dolayı kodlama yapılmamış olması veya katılımcıların verdikleri yanıtların birden fazla alt kod sınıfında kodlanmış olmasıdır. Örneğin, bir katılımcı SSA’ların avantajlarını açıklarken birden fazla avantaj dile getirmişse bir katılımcının yanıtı birden fazla alt kodda gösterilmiş şekilde grafikte belirtilmiştir.



Tablo 1.*Kodların ve Alt Kodların Frekans Analizi*

1. Tanım	29
2. 1. Kullanılan SSA'lar	
Siri	27
Google Asistan	22
Kullanmıyor	3
Alexa	2
3. 2. Kullanım Amacı	
İnternet Araması	31
Telefon Görüşmesi Yapmak	15
Diğer Uygulamaları Aktifleştirmek	14
Alarm Kurmak	10
Not Almak	9
Hava Durumunu Öğrenmek	9
Konum, Harita ve GPS Özellikleri	7
Eğitim	4
Mesaj Yazmak	4
Eğlence	4
Hatırlatıcı Oluşturmak	3
Çevrimiçi Alışveriş	2
Ev Kontrol Sistemi	2
Sesli Mesaj Göndermek	1
Haberleri/Gündemi Takip Etmek	1
Bildirimleri Kontrol Etmek	1
4. 3. Kullanılan Mecralar	
Özel Alan	29
Her İkisi de	20
Kamusal Alan	
5. 4. SSA'ların Avantajları	
Zaman Kazandırması	34
Kolaylık	25
Çoklu Görev	12
Yeni Fikirler Sunmak	4
Eğlenmek	1
Avantajı Yok	1
6. 5. Kullanıcı Farkındalığı	
Bilgisi Yok-Gizlilik İhlali Var	16
Bilgisi Var-Gizlilik İhlali Var	15
Bilgisi Yok	12
Bilgisi Var-Gizlilik Endişesi Yok	5
Bilgisi Var-Emin Değil	1
7. 6. Bilginin Kaynakları	
Ders-Eğitim	8
Araştırma	5
İnternet-Sosyal Medya	5
Tecrübe	4
Sosyal Ortam	2
Bilgilendirme Metni	2
Belgeseller	1
8. 7. SSA'ların Dezavantajları	
Verinin Dep. ve Kay. Riski	34
Var Ancak Kabul Edilebilir	10
Yok	5
Kişiyi Tembelleştirmesi	3
Dinlenme Riski	3
Başkasının Sesiyle Aktifleşebilmesi	1
Veri Hırsızlığı	1
9. 8. Gizlilik P.'larına Dair Bilgilendirme	
Bilgilendirilmediğini Düşünüyor	36
Bilgilendirme Metnini Okumuyor	24
Bilgilendirilse de Fark Etmemiş	14
Bilgilendirildiğini Düşünüyor	2
10. 9. Kullanıcı Tecrübesi	
Yaşamadı	33
Yaşadı	16
11. 10. Kişisel Önlemler	
Önlem Almıyor	28
Önlem Alıyor	21

Tablo 1’deki kod listesi incelendiğinde araştırmanın belirlenmiş 10 adet ana kodu ve her ana kodun kullanıcıların yanıtlarındaki farklılıkları temsil edecek şekilde farklı sayılarda olmak üzere toplamda 56 alt kodu olduğu görülmektedir. Tabloda her ana ve alt kodun frekansı yani kodlanma sıklığı görülmektedir. Buna göre ana kodların frekansı birbirine yakındır çünkü ana kodlar görüşme sorularından yola çıkılarak oluşturulmuştur. Görüşme sorularına ek olarak yalnızca “Tanım” kodu eklenmiştir. Bu kodun amacı daha çok içerik analizine fayda sağlamaktadır çünkü görüşmenin başında katılımcılara yöneltilen demografik bilgilerden sonraki ilk soru olan “SSA denince aklınıza ne geliyor?” sorusuna verilen yanıtı temsil etmektedir. Bu yanıtın önemi, katılımcıların SSA’lara dair akıllarına gelen ilk imajı paylaşmış olmalarıdır. Oluşturulan alt kodlar ise farklılık göstermektedir çünkü her biri katılımcıların verdikleri cevaplar doğrultusunda kodlanmıştır.

Birinci ana kod katılımcılar arasında en çok tercih edilen SSA’ları temsil etmektedir. Alt kodlara bakıldığında en sık tekrarlanan kodun “Siri” alt kodu olduğu görülmektedir. İkinci ana kod katılımcıların SSA’ları kullanım amaçlarını temsil etmekte olup, en sık tekrarlanan kod “İnternet Araması” alt kodudur. Bu da SSA’ların katılımcılar tarafından en çok internette arama yapma gerekçesiyle kullanıldığını göstermektedir. Üçüncü kodlama kullanıcıların SSA’ları kullanmayı tercih ettikleri ortamları temsil etmektedir. “Özel Alan” alt kodunun sıklığına göre SSA’ları yalnızca özel alanlarda kullanmayı tercih edenlerin sayısının en fazla olduğu görülürken, “Kamusal Alan” alt kodu hiç kodlanmamıştır ve tabloda hiç kodlanmamış olan tek alt koddur. Dördüncü ana kod SSA’ların kullanıcılara sağladığı avantajları temsil etmektedir ve burada da en sık tekrarlanan alt kodun “Zaman Kazandırma” alt kodu olduğu görülmektedir. Beşinci, altıncı, yedinci, sekizinci ve dokuzuncu ana kodlar çalışmanın temel araştırma sorularına yöneliktir. Araştırmanın bu kilit ana kodları katılımcıların gizlilik politikaları konusunda ilgili algılarını, gizlilik politikaları konusunda bildiklerinin ve tecrübelerinin yanı sıra kullanıcıların bu bilgileri nasıl edindikleri konusunda tespitler sunmaktadır. Beşinci ana kodun alt kodlarına bakıldığında veri gizliliğine ve güvenliğine dair bilgisi olmayanların sayıca daha fazla olduğu görülürken, gizliliğe dair verilerinin ihlal edildiğini düşünenlerin sayısı da herhangi bir ihlal olmadığını düşünenlere göre daha fazladır. Aynı zamanda yedinci ana kodun temsil ettiği “SSA’ların veri gizliliği yönünden dezavantajları”na yönelik yanıtlarda da kişisel bilgilerinin kaydedildiğini ve depolandığını düşünen katılımcı sayısının fazlalığı göze çarpmaktadır. Bu verilerin sundukları sonucunda genel olarak

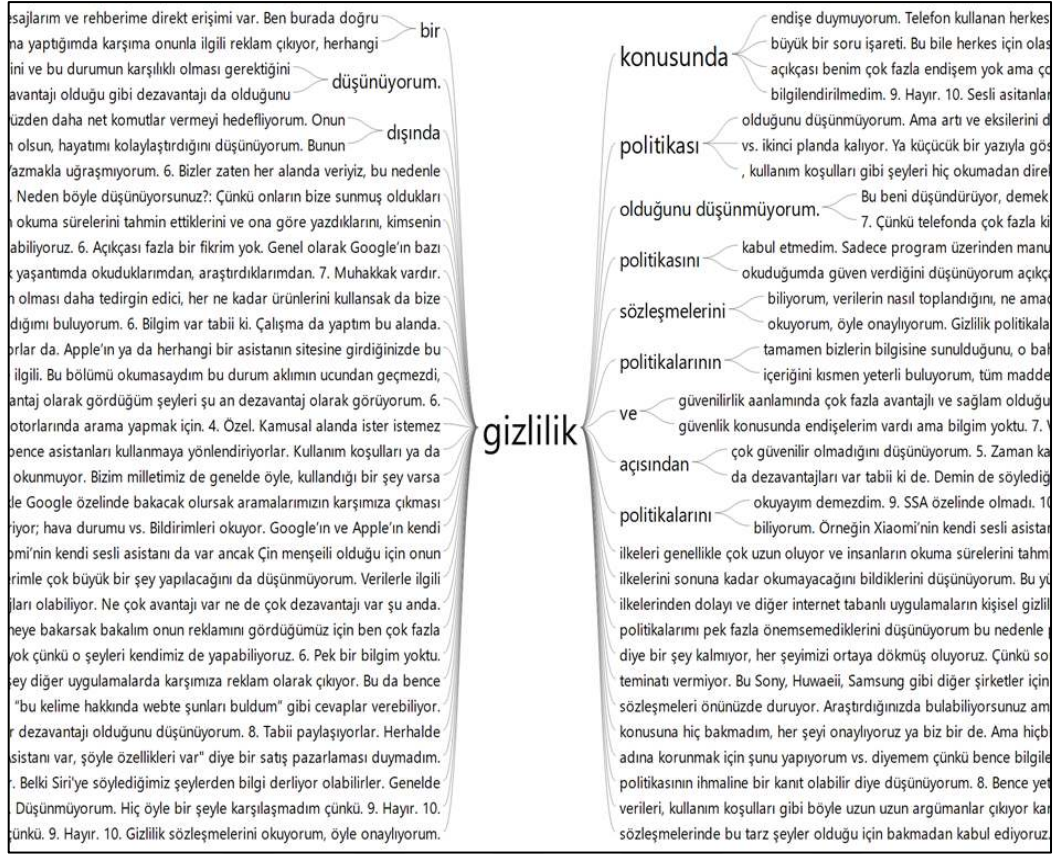
söylenbilir ki katılımcılar gizlilik politikaları konusunda çoğunlukla bilgi sahibi değilken bile kişisel verilerinin risk altında olduğunu düşünmektedirler. Yedinci ana kodun sıklık yönünden ikinci alt kodu, 10 katılımcının bu riskleri SSA kullanımı adına kabul edilebilir bulduğunu göstermektedir.



Şekil 3. Alt kodların kelime grubu

Şekil 3’te alt kodların kodlanma sıklığına göre oluşturulmuş kelime bulutu yer almaktadır. Tablo 1 ve 2’de frekansları verilen alt kodların arasında en çok öne çıkanın “Bilgilendirilmediğini Düşünüyor” alt kodu olduğu görülmektedir. Bu bulguya göre katılımcılar tarafından en sık dile getirilen ifade, geliştirici şirketler (yalnızca araştırma katılımcılarının kullandığı SSA’lara göre) olan Apple, Google ve Amazon tarafından SSA’ların gizlilik politikaları konusunda bilgilendirilmedikleri görüşüdür. Alt kod 36 kodlamaya sahiptir, bu da 50 katılımcıdan 36’sının bu kanıda olduğunu göstermektedir.

İkinci en sık tekrarlanan alt kodlar ise eşit sayıda katılımcının görüşüyle her biri 34 kez kodlanmış olan “Zaman Kazandırma” ve “Kişisel Bilginin Kaydedilme ve Depolanma Riski” alt kodlarıdır. Bu alt kodların biri SSA’ların avantajları arasından diğeri ise dezavantajları arasından en çok dile getirilen görüşü temsil etmektedir. Buna göre SSA’lar kullanıcılarına en çok gündelik yaşantılarında zaman kazandırarak yardımcı olmaktadır. Eşit sayıda katılımcı, SSA’ların kişisel verilerinin kaydedilmesi ve depolanması yönünden riskler barındırdığını ifade etmiştir ve bu ifade SSA’ların en çok dile getirilen dezavantajı olarak kaydedilmiştir.

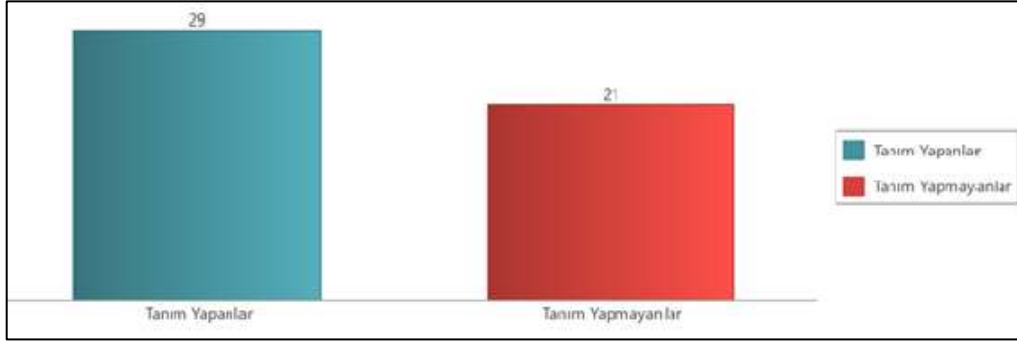


Şekil 4. “Gizlilik” kelimesiyle oluşturulan etkileşimli kelime ağacı

Şekil 4’te “gizlilik” kelimesiyle oluşturulmuş etkileşimli kelime ağacı görülmektedir. Şekil tüm katılımcıların görüşlerinin bir araya getirilmesiyle oluşturulmuştur. Katılımcıların cümleleri birbirinin uzantısı haline getirilerek birbiriyle ilişkilendirilmiştir. “Gizlilik” kelimesinin en çok etkileştiği kelimeler çalışmanın içeriğinden de bekleneceği gibi “politikası, konusunda, sözleşmelerini, ilkeleri” gibi kelimelerdir. Kelime ağacı incelendiğinde katılımcılar arasındaki görüş benzerlikleri ve farklılıkları daha belirgin bir şekilde görülebilmektedir. Örneğin, “gizlilik” kelimesinin “politikaları” kelimesine bağlandığı yerde oluşan iki ayrı koldaki ifadelerden biri “gizlilik politikalarını okuyayım demezdim” iken, bu ifadenin altında başka bir katılımcının “gizlilik politikalarını biliyorum” ifadesi yer almaktadır. “Gizlilik” ve “konusunda” ifadelerinin bağlantısı takip edildiğinde kollardan birinde ifade “endişe duymuyorum” iken, diğer kolda “büyük bir soru” şeklinde devam etmektedir.

5.2.1. Sesli Sanal Asistanları Tanımlamak

Katılımcıların SSA'ları tanımlama biçimlerinin “tanım” ana kodu altında verilmiştir. Verilen yanıtlar doğrultusunda Şekil 5’te görülen grafik oluşturulmuştur.



Şekil 5. SSA'ları tanımlamış ve tanımlamamış katılımcılar

Katılımcılardan SSA'ların onlara neyi çağrıştırdığını dile getirmeleri istenmiş, böylece SSA'ların onlar için ne ifade ettiği ve bu teknolojinin ne kadar biliniyor olduğu ortaya çıkarılmak istenmiştir. Buna göre katılımcıların yalnızca 29'u kullandıkları SSA'ları dair bir tanımlama yapabilmıştır. Diğer 21 katılımcı ise SSA kavramını açıklarken bir tanımlama yapmamış, yalnızca bildikleri SSA uygulamalarının isimlerini belirtmiştir.

Katılımcı 2, 11 ve 18 bu tanımlarla birlikte SSA'nın onun için sağladığı avantajı da dile getirmiştir. SSA'yı “kolaylık” kavramıyla ilişkilendirdiğini belirtmiştir.

Aklıma kavram olarak “kolaylık” geliyor. Çünkü SSA dediğimiz şey dijital bir ortamda gerçekleştirdiğimiz, kısa yoldan yaptığımız işlemler gibi geliyor bana (Katılımcı 2).

Görüşmelerin tümüne bakıldığında 3'ü olumsuz anlamda olmak üzere 31 katılımcı “kolay” kelimesini kullanmıştır. Bunlardan 14'ü tanım ifadesidir, yani 14 kişi SSA'ları kolaylık sağlıyor olmaları üzerinden tanımlamıştır.

Kolaylık. Telefonuma ya da önümdeki klavyeye dokunmadan istediğimi sesli komut ile aratma (Katılımcı 11).

Kolaylık geliyor. Telefondaki uygulamalarımı asistanı kullanarak buluyorum. Benim yerime yapmam gerekenleri yapıyor. Zoru kolaylaştırıyor (Katılımcı 18).

Katılımcı 10, 14, 17, 22 SSA'ları kullanmaktan hoşnut olduklarını özellikle vurgulamışlardır. Katılımcı 22, bedensel engelinden dolayı gündelik yaşamındaki işlerini daha kolay kılmak adına faydalandığı SSA'ı bir "rehber" olarak tanımlamıştır. Çalışmanın bu aşamasındaki bulguların en dikkat çekici tarafı, katılımcıların hiçbirinin SSA'ları olumsuz bir ifadeyle tanımlamamış olmasıdır. Görüşmenin ilerleyen aşamalarında araştırmacının sorular sormak dışında hiçbir müdahalesi bulunmamışsa dahi katılımcıların SSA'lar hakkındaki görüşleri daha olumsuz bir boyuta evrilmiştir.

Windows olsun ya da diğer yazılım şirketlerinin bizlerin hayatını kolaylaştırmak için tasarlamış oldukları web sistemleri (Katılımcı 10).

Dijital asistan bir yapay zekâ ürünü ve hayatımızı kolaylaştıran bir şey olduğunu düşünüyorum ben. Aklıma dijitalliği ve yardımcı olabilecek bir ürün olduğu geliyor (Katılımcı 14).

Hayat kolaylaştırıcı bir uygulama, gerçekten bir asistan olarak görüyorum bu uygulamaları. Özellikle Bluetooth kulakların çıkmasından sonra artık telefon cebimizde veya Bluetooth'un bağlanabileceği bir uzaklıkta olduğu zaman Siri'ye seslendiğimiz zaman bir sürü işimizi görebiliyoruz. Özellikle arama yapma konusunda baya etkili oluyor ve kullanışlı (Katılımcı 17).

Erişilebilirlik kavramı aklıma geliyor. Ben engelli bir bireyim ve sesli asistanları, ulaşım sağlayamayacağım cihazlara daha rahat ulaşım sağlamamı ve o cihazları kullanmamı sağlayacak bir rehber olarak görüyorum (Katılımcı 22).

Katılımcı 10, 14, 17 ve 22'nin ortak özellikleri veri gizliliğine dair bilgilendirilmediğini düşünüyor olmaları fakat buna rağmen veri gizliliğinin olmadığı ve SSA'lar tarafından mahremiyetin ihlal ediliyor oluşundan emin olmalarıdır. Verilerinin depolandığını ve ticari amaçlarla satıldığını düşünmelerine ve görüşmeleri sırasında akıllarına gelen her türlü veri ihmaline değinmelerine rağmen Katılımcı 22 haricinde hiçbirisi veri ihlali konusunda SSA'lar ile kişisel bir tecrübe yaşamamıştır ve hiçbirisi verilerini daha güvenli hale getirmek için bir önlem almamaktadır. Yine de SSA kullanmakta ve SSA'ları faydalı teknolojiler olarak kabul etmektedirler.

5.2.2. Kullanılan Sesli Sanal Asistanlar



Şekil 6. Katılımcılar arasında en sık kullanılan SSA'lar

Katılımcılar arasında en çok kullanılan SSA 27 kişinin (katılımcıların %54'ü) yanıtına göre Siri'dir. İkinci sırada 22 kişinin (%44) kullanımı ile Google Asistan yer almaktadır. Bu iki SSA uygulamasına ek olarak kullanılan tek SSA ev tipi akıllı hoparlör olan Alexa'dır ve Alexa kullanan 2 katılımcı da aynı zamanda Siri kullanıcısı olduklarını belirtmiştir. Katılımcılardan biri İngilizce bilmediği için telefonunda yer alan Bixby'den faydalanamadığını ve bunun yerine Google Asistan'ı tercih ettiğini dile getirmiştir. Bixby'nin henüz bir Türkçe desteği yoktur ve Samsung telefonlar aynı zamanda Google Asistan'ı da desteklemektedir (Hall, 2022). Alexa Türkçe dil desteği olmayan bir diğer SSA'dır. Alexa kullanan iki katılımcı bu konuda bir olumsuzluk dile getirmemişlerse de Türkçe dil desteğinin olmaması bazı kullanıcılar için bir dezavantaj kabul edilebilir.

Evet, Google Asistan kullanıyorum. Diğer asistanları hiç denemedim. Samsung telefon kullanıyorum, fakat Bixby'yi İngilizce konuşmam gerektiği ve İngilizcem çok iyi olmadığı için onu kullanamıyorum (Katılımcı 12).

Katılımcı 31, yerli sesli asistan CEYD-A'yı kullanma deneyiminden bahsetmiştir. 2010'lu yıllarda geliştirilmeye başlanan ve 2019'a kadar 3,5 milyon kişi tarafından indirilen CEYD-A, açık kaynak kodlu, yani kullanıcıları tarafından değiştirilmeye ve geliştirilmeye izin veren bir yazılıma sahiptir ve yaratıcısı Cenker Şişman'dır (Emeç, 2019).

Google Asistan. Bir ara CEYD-A kullandım ancak memnun kalmadım. Söylediklerimi tam anlayamıyordu ya da cevap veremiyordu, yeterli bulmadım (Katılımcı 31).

Katılımcı 32, görüşme sırasında SSA kullanmayı tercih etmediğini belirtmektedir. Bu katılımcı yaşı itibarıyla X kuşağına ait bir bireydir. İfadelerine göre katılımcı dijital teknolojileri kullanmak yönünde çekinceleri olduğunu ve “mümkün olduğunca” kullanmamayı tercih ettiğini belirtmiştir. Bu ifadeler X kuşağına atfedilen, teknolojik gelişmeleri kullanma alışkanlıkları konusunda Y ve Z kuşaklarına kıyasla gelenekçi bir tutum sergiledikleri ve teknolojiyi kullanmayı sonradan öğrenmek zorunda kalmalarından dolayı bunun olumsuzluğunun etkilerini yaşıyor oldukları görüşleriyle uyumluluk göstermektedir (bknz. Bölüm 4.2.2. X Kuşağının Mahremiyet Algısı).

Yaşım itibarıyla teknolojiden biraz çekiniyorum, sadece zorunlu olunca kullanıyorum. Birincisi öğrenmesi zor, ikincisi insan makineye konuşuyor gibi hissediyor, karşıda robot varmış gibi. Rahat hissedemiyor insan. Bizler kişisel iletişimi ön plana çıkardığımız için, ben bir kitabı ve gazeteyi elime alıp onun kokusunu hissetmek isterim. Telefonda konuşuyorsam da kişinin sesini duymak isterim. Banka işlem varsa bankaya giderim, internet bankacılığını kullanmam. Ben zorunluluk dışında kullanmıyorum teknolojiyi (Katılımcı 32).

Görüşmeler sırasında 2 katılımcının (Katılımcı 33 ve Katılımcı 6) aslında SSA kullanmadıkları fakat kullandıkları bazı sohbet botları ve sesi algılama özelliği bulunan programları SSA olarak adlandırdıkları görülmüştür.

Vodafone ve TürkNet'in SSA'larını kullanıyorum. SSA aracılığıyla yardımcı oluyorlar. Çok elzem bir durum olduğu sürece müşteri hizmetlerine gönderiyorlar. Telefonum android ancak Google Asistan'ı kullanmadım (Katılımcı 33).

Youtube, Google Chrome. Navigasyon araçları. Telefondakileri kullanmıyorum. (Katılımcı 6).

Katılımcılardan 5'inin bazı sohbet botlarını ya da mikrofon aracılığıyla sesli arama yapılabilen arama çubuklarını da SSA olarak değerlendirdikleri görülmüştür. Bu ifadeler, kullanıcıların bu teknolojilerin aynı olduğunu düşündüklerine (Shanbhag, 2020) örnek gösterilebilir. Oysaki SSA'ların sunduğu hizmetler sohbet botlarının kullanım alanlarından geniş ve farklıdır. SSA'lar kullanıcıların günlük etkinliklerine yardımcı olabilmek için tasarlanmış yazılımlarken sohbet botları çeşitli web sayfalarında ve uygulamalarda kullanıcıya yalnızca belirlenmiş kısıtlı işlemler çerçevesinde yardım edebilen sistemlerdir. Sohbet botlarının çalışma sistemleri SSA'larındaki kadar gelişmiş değildir.

Evet kullanıyorum hatta iş yerinde de kullanıyoruz. Bu tarz teknolojileri kullanıyoruz. Yalnızca cep telefonlarındaki yol tarif eden asistanlar gibi değil, aynı zamanda dijital dosyalarımızı bulmak için de cihazlar var, belli başlı kullanıcılara yönelik. Sesli komutlarla o dosyaların ismini kodladığım zaman onları bulabiliyor. Onlar da sanal asistan olarak geçiyor. Onları da kullanıyoruz, aklıma o da geliyor (Katılımcı 5).

Katılımcı 5 OpenProject isimli, daha çok ofis ortamlarında kullanılan, proje oluşturma ve geliştirme hizmeti veren web tabanlı bir proje yönetim sisteminden bahsetmektedir.

Evet, Google. Ayrıca Google dökümanlarda ses ile komut vererek yazma özelliğini de kullanıyorum. WhatsApp'ın da sesli komut özelliğini kullanıyorum. Telefonumda ise Siri'yi kullanıyorum (Katılımcı 11).

Katılımcının bu ifadesinde WhatsApp'ın sesle yazma ve Google'ın dikte özelliklerinin de SSA olarak değerlendirildiği görülmektedir.

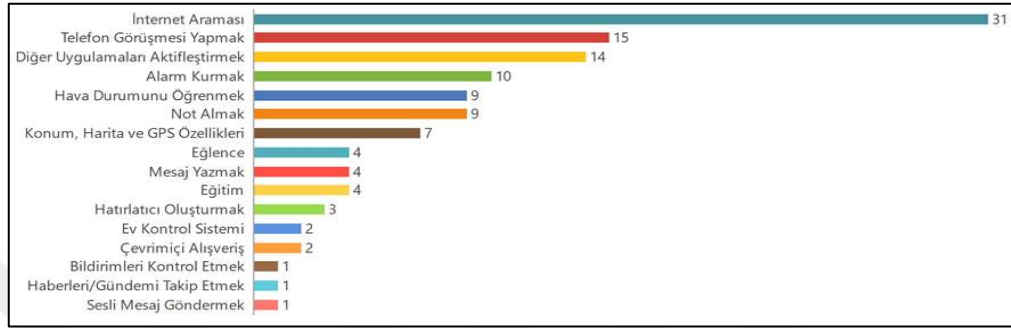
Daha önce Siri kullanıyordum. Örneğin Siri yalnızca benim sesimle değil, başkasının sesiyle de aktif hale gelebiliyordu. “Hey Siri x'i ara” dediğimde birini arayabiliyor ve kamusal bir alanda telefonumu bir yerde kaybettiğimde ya da istemediğim birinin eline geçtiğinde bunu yapabilmek hatta belki şifre girmeden birine mesaj gönderebilmek bile mümkün olabilir. Böyle bir şey yaşadım. İstemediğim birine bir başkası tarafından bir mesaj gönderildi. Bu olaydan sonra IOS'u kullanmayı bıraktım (Katılımcı 19).

Katılımcı 19, önceden Siri kullanıyor olduğunu fakat artık tercih etmediğini ifade etmiştir. Bunu nedeni ise göndermek istediği mesajın Siri tarafından başka bir kayıtlı kişiye gönderilmesi yani teknik yetersizlikten kaynaklanan bir mahremiyet ihlalidir.

Siri. Diğerlerine pek güvenim yok açıkçası. Mesele güvenlikle Apple'a güveniyorum. Son zamanlarda Çin ile veri paylaşımına dair haberler çıktı ancak detayını bilmiyorum. Ama Apple bana daha güvenilir geliyor. Hem elektronik alet hem SSA olarak. Diğerleri hem teknolojik olarak yavaşlar, sorun yaratıyorlar. Google Asistan falan hep yarı yolda bıraktı o yüzden Siri. Bütün aletlerimi Apple'a çevirmeye başladım. Bunun birinci sebebi daha memnun kalmam, ikincisi de aletlerin kendi arasında iletişimi olması (IoT), o bana daha rahat geliyor. Hangisini açarsam açayım direkt her taraftan ulaşabiliyorum her şeye (Katılımcı 24).

Katılımcı 24 ise eskiden Google Asistan kullandığını fakat teknolojisini yetersiz bulduğu için tercih etmediğini belirtmiştir. Siri kullanımındaki gerekçelerden biri olarak IoT’u göstermiştir.

5.2.3. Sesli Sanal Asistanların Kullanım Amaçları



Şekil 7. SSA’ların kullanım amaçları

Katılımcıların belirttiği üzere SSA’ların kullanım amaçlarında ilk sırada internet araması yapmak yer almaktadır. Daha sonra sesli komut ile rehberden isim belirterek telefon görüşmesi yapmak ve diğer uygulamaları SSA aracılığıyla etkinleştirmek gibi amaçlar gelmektedir. Katılımcılardan 9’u (%18) SSA’ları telefonlarına fiziksel erişim sağlayamadıklarında ya da yazmak yerine sesli komut vermeyi tercih ettiklerinde kullandıklarını belirtmişlerdir.

Eğitim amaçlı. Mesela “Siri, Adorno hakkında makaleleri bulur musun?” diyerek kendim daha uzun sürede araştırmak yerine SSA’dan faydalaniyorum. Benim 5-10 dakikada ya da daha fazla sürede ulaşabileceğim belgeleri o tek tek sıralıyor (Katılımcı 1).

Google veya Safari ile aramaktansa direkt sorumu asistana yöneltiyorum. Ya da sesli bir şey dinlediğim zaman onun sesini aktarıp cevabını öğrenebiliyorum (Katılımcı 17).

Birinci amacım araç kullanırken telefona bakmamak. Acil bir şey yapacaksam ellerimi kullanmaktansa direkt telefona söylemek. Güvenlik için daha iyi oluyor ve daha rahat oluyor. Araç kullanırken ya da bulaşık yıkarken o an ellerimi kullanamayacaksam SSA kullanıyorum. Aslında normal kullanım daha konforlu, boş zamanım varsa SSA kullanmıyorum. Ancak iki elimi kullandığım, konsantrasyon gerektiren bir iş yaptığımda kullanıyorum (Katılımcı 24).

Örneğin akşam telefonu şarja takıyorum ve yattığım yerde uzanmak yerine direkt “Hey Siri” diye seslenip alarm kurabiliyorum (Katılımcı 41).

Katılımcı 22, bedensel engeli nedeniyle gün içinde yaşadığı birtakım zorluklardan dolayı SSA kullanmayı tercih ettiğini ifade etmektedir.

Günlük hayatımda kullanmak zorundayım çünkü kollarımı çok fazla kullanamıyorum. Günlük konuşmalarım da kullanıyorum. Ancak en çok ödevlerimi yaparken sesle yazı yazma özelliği çok işime yarıyor (Katılımcı 22).

Katılımcı 34, 35 ve 24 SSA’ların evdeki diğer akıllı cihazlarla etkileşimine vurgu yapmıştır.

Ev içerisinde Alexa’yı kullanırken genelde ışık kapama açma, onun dışında müzik açma gibi şeylerde kullanıyorum sesli asistanı (Katılımcı 34).

Evdeyken de biraz daha tembelleşmemden kaynaklı olsa gerek, ışığı yakmaya o kadar üşendiğim zamanlar oluyor ki, tabii bunu sesli komutla yaptırabiliyorum. Evdeki kapı kilidi Xiaomi mesela, onu otomatikman program üzerinden de kilitleyebiliyorum (Katılımcı 35).

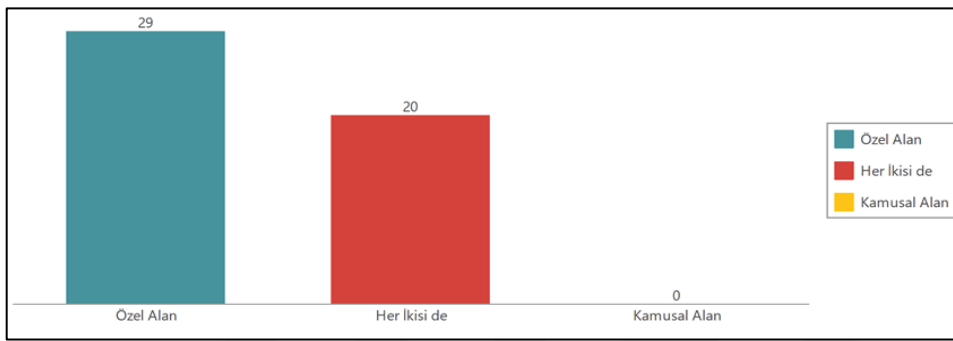
Bütün aletlerimi Apple’a çevirmeye başladım. Bunun birinci sebebi daha memnun kalmam, ikincisi de aletlerin kendi arasında iletişimi olması, o bana daha rahat geliyor. Hangisini açarsam açayım direkt her taraftan ulaşabiliyorum her şeye (Katılımcı 24).

Katılımcı 27 ve 40 ise güncel olarak SSA kullanmadıklarını belirtmişlerdir. Bunun nedeni Google Asistan kullanıcısı olan Katılımcı 27 için dinleniyor olduğu düşüncesiyle, Siri kullanıcısı olan Katılımcı 40 için SSA kullanımını faydalı bulmamasından kaynaklanmaktadır. Burada dikkat çeken bir nokta, SSA’ları tanımlarken Katılımcı 27’nin dahi olumlu ifadelerle tanım yapmasıdır. Katılımcı 40 ise tanımlama yapmamış, “eskiden kullanıyordum ama artık ihtiyaç duymuyorum (Katılımcı 40).” diyerek kullanmıyor olduğunu dile getirmiştir.

1, 1,5 yıl kullandım fakat daha sonra rahatsız olmaya başladım. Şu anda kullanmıyorum, o özelliği kapattım telefonumda. Google Asistan. Başlarda kolayca kaçmak hoşuma gidiyordu açıkçası ancak daha sonra arkadaş ortamında bahsettiğimiz bir çantanın sürekli reklamları gelmeye başladı. Dinleniyor muyum acaba düşüncesi oluştu bende. Büyük abi imajı çizildi gözümde, o yüzden rahatsız oldum ve kullanmayı bıraktım (Katılımcı 27).

Bir şeyler araştırırken, herhangi bir konuda kaynak bulması için komut vererek Siri'yi kullanıyordum. Daha sonra artık kullanmamaya, önemsiz bulmaya başladım. Çünkü bu asistanlar telefonun bir özelliği olarak fazlalık gibi gelmeye başladı bana. Gereksiz bulmaya başladığımı söyleyebilirim. Kolaylık sağlıyordu fakat telefonda bir şeyi kendi kendimize araştırmanın beyni çalıştırma açısından da güzel olduğunu düşünmeye başladım. Kolaya kaçmak istemedim. En başta eğlence amaçlı da kullanıyordum fakat daha sonra sıkıldı. İnterneti ona kapattırırdım kolaylık olsun diye, uygulamaları ona başlattırırdım. Kapatmadım ama kullanmıyorum (Katılımcı 40).

5.2.4. Sesli Sanal Asistanların Kullanıldığı Mecralar



Şekil 8. SSA'ların kullanıldığı mecralar

Katılımcıların SSA'ları kullanmayı tercih ettikleri mecralara bakıldığında 29 katılımcının (%59,2) SSA'ları yalnızca özel alanlarda kullanmayı tercih ettikleri görülmektedir. 20 katılımcı (%40,8) hem özel hem kamusal alanda kullanmakta sakınca görmediğini belirtirken, yalnızca kamusal alanda kullanmayı tercih ettiğini söyleyen katılımcı olmamıştır. SSA'ları kamusal alanda kullanmamayı tercih eden katılımcılar teknik nedenler, pratik olmadığı, gürültü kirliliği nedeniyle anlaşılamamak gibi gerekçeler dile getirirken, katılımcılardan yalnızca 4'ü kamusal alanda SSA kullanmama gerekçesi olarak gizlilik endişelerini göstermiştir. Buradan elde edilen bulgu kamusal alanlarda SSA kullanımının tercih edilmemesinin nedenlerinin çoğunlukla teknik sorunlar olmasıdır.

Kamusal alanda kullanmayı tercih etmiyorum. Belki Google yerine Siri kullansam kullanabilirdim, Google ile sesli komutu aktif hale getiremedim. Dışarıda onu açmakla uğraşacağıma kendim o işlemi yaparım zaten. Pratik olmadığı gerekçesiyle kullanmıyorum (Katılımcı 8).

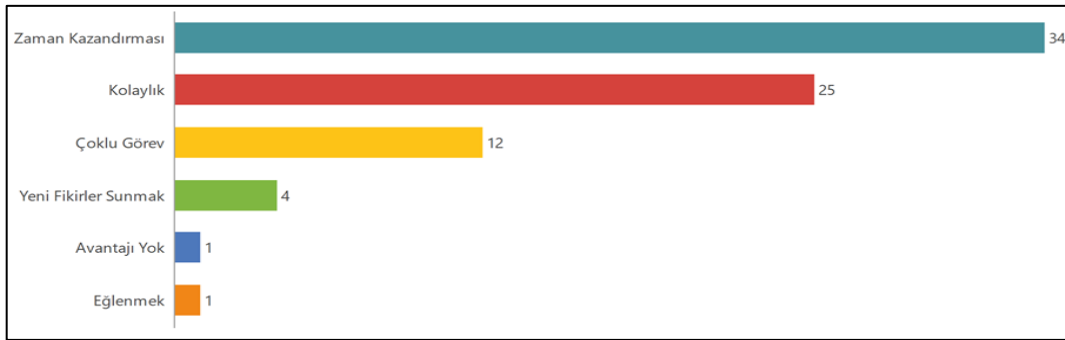
Özel alanda kullanıyorum. Kamusal alanda kullanmayı tercih etmiyorum çünkü bazı şeyleri söylediğimde belki benim telaffuz etme şeklimden dolayı kamusal alanda sesli asistan tarafından doğru anlaşılmadığımı düşünüyorum (Katılımcı 11).

Özel diyebilirim. Herkesin bulunduğu bir ortamda sesli aramada kesinlikle bulunmuyorum. Genellikle özel alanımda, ev içerisinde veya yalnız olduğum bir ortamda kullanıyorum. Kamusal alanda kesinlikle kullanmıyorum. Çevremdeki insanların dikkatini çeker diye düşündüğüm için. Onların ilgisini çeker, kulak misafiri olurlar veya neler arattığımı merak ederler diye (Katılımcı 12).

Katılımcı 22, kas rahatsızlığı nedeniyle kamusal alanda SSA kullanmayı tercih etmediğini dile getirmektedir. Özel alanda çok fazla SSA kullansa da kamusal alanda SSA kullanmak konusunda çekinceleri olduğunu belirtmiştir.

Kamusal alanda hiçbir şekilde bir teknolojik araç kullanmaya ihtiyaç hissetmiyorum. Kollarımı kullanmakta yaşadığım zorluktan dolayı (kas rahatsızlığı) kamusal alanda herhangi bir teknolojik cihazı kullanmamayı tercih ediyorum (Katılımcı 22).

5.2.5. Sesli Sanal Asistanların Sağladığı Avantajlar



Şekil 9. SSA'ların kullanıcılara sağladığı avantajlar

Katılımcıların ifadelerine göre SSA'ların kullanıcılarına sağladığı avantajlardan en çok öne çıkan bu araçların kullanıcılarına zaman kazandırmasıdır. 34 katılımcı (%69) SSA ile yapılan işlemin normalden daha hızlı yapılabilildiğini ve böylece onlara zaman kazandırdığını ifade etmiştir. Bununla birlikte Katılımcı 27, SSA'ların bu özelliğinin kişiyi tembelleştirdiğine dikkat çekerek başlarda avantaj gibi görünen bir özelliğin daha sonra bir dezavantaj gibi gelmeye başladığını belirtmektedir.

Açıkçası kullanırken zaman açısından avantajlıydı. Bir şeyi yazarak aratmakla sesli komutla aratmak farklı, bunun avantajlı olduğunu düşünüyordum. Bir süre sonra makineleşme hissi oluşmaya başladı çünkü sürekli sesli komut veriyorum ve telefon onu gerçekleştiriyordu. Basit şeyleri bile kendim yapmamam beni çok rahatsız etmeye başladı. O zaman avantaj olarak gördüğüm şeyleri şu an dezavantaj olarak görüyorum (Katılımcı 27).

Gündelik yaşamda hız en büyük artımız, neoliberal politikalar çerçevesinde belirli hız ve zamanda bazı işleri gerçekleştirmemiz gerekiyor. O yüzden bu yönde avantaj sağladı (Katılımcı 22).

SSA'lar trafikte de kullanıcılarına avantaj sağlamaktadır. Katılımcı 6, 18 ve 21 SSA'ları özellikle arabalarında kullanmayı tercih ettiklerini belirtmektedir. Bununla birlikte kullanıcılar bir işle meşgulken SSA yardımıyla eş zamanlı olarak başka işlerini de yapabilmenin mümkün olduğunu dile getirmektedir, bütün bunlar SSA'ların çoklu görev yapabilmeye olanak sağladığı anlamına gelmektedir. Hatta Google, bu ihtiyaca yönelik olarak 2018'de Google Asistan'a Rutinler özelliğini getirerek SSA'nın birden fazla görevi tek bir sesli komutla yapabilmesine olanak sağlamıştır (Forrest, 2018).

O an işim oluyor ya da elim dolu oluyor ve yazamıyorsam sesli bir komut verebiliyorum. Ödev yaparken de sesimle bir şeyler aratabiliyorum, o bana sistemden buluyor (Katılımcı 7).

Hızlı bir arama yapacağım zaman, klavyeyle uğraşmamak için sesli arama yapıyorum. Otomobilde, dikkatim dağılmasın diye, ekrana bakmak yerine (Katılımcı 6).

Örneğin araç kullanırken birini aramam gerekiyor ya da mesaj göndermem gerekiyorsa Siri benim yerime, ekrana bakmama gerek kalmadan bunu yapıyor (Katılımcı 18).

Katılımcı 21, SSA'ların neredeyse fiziksel bir yardımcı gibi, "yanında biri varmış" hissi uyandırdığını dile getirmiştir.

Ellerim doluyken sesli komut ile sanki yanımda başka biri varmış ve o an benim yerime o işi yapıyormuş gibi kullanmak avantaj sağlıyor. Pratiklik olarak da avantaj sağlıyor. İşim bölünmemiş oluyor, konsantrasyonum bozulmuyor (Katılımcı 21).

Katılımcı 19, 22 ve 33 SSA'ların fiziksel engeli bulunan kullanıcıların hayatını kolaylaştırmasına vurgu yapmaktadır. Bu duruma yönelik farklı görüşler bulunmaktadır.

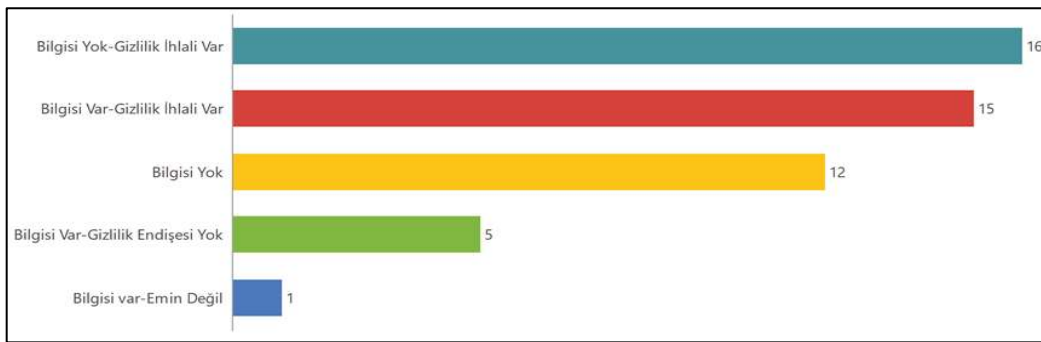
Buna göre sesle çalışan bir yapay zekâ sistemini kullanmakta zorlanabilecek konuşma bozuklukları, kekemelik gibi durumlarda SSA kullanımı bir avantaj sağlamamaktadır. Adams'ın New York Times'da yayınlanan "Voice Assistants Don't Understand Us. They Should. (SSA'lar Bizi Anlamıyor. Anlamalılar.)" başlıklı makalesine (2021) göre SSA geliştirici şirketler bu konuda çözüm üretmek için çalışmalar yürütmektedir. Apple'ın Siri için kekemelere ait ses klipleri toplama girişimi, Amazon'un konuşma kalıplarını öğrenebilen bir uygulama olan Voiceitt ile ortak çalışmaları, Microsoft'un konuyla ilgili geliştirici teknolojilere 25 milyon dolar bütçe ayırması, Google'ın çeşitli konuşma kalıplarını tanıyabilen yazılımlar geliştirmesi gibi SSA'ların hemen hemen tümü ses tanıma sistemlerini geliştirmeye yönelik ciddi hamleler yapmaya başlamıştır.

Sesli asistanları en çok kullananlar görme engelliler, böyle insanlarla karşılaşıyorum. Bir engeli ortadan kaldırdığına inanıyorum (Katılımcı 19).

Sesli asistan aslında benim görme engelli arkadaşlarımda tanıdığım bir teknolojiydi. Ayrıca bazı konularda engelli bir birey olarak "yapamazsın" denilen şeyleri yapmamda bana yardımcı olduğunu düşünüyorum (Katılımcı 22).

Kolaylık sağlıyor. Özellikle görme engelli ya da ileri yaştaki kullanıcılar için böyle olduğunu düşünüyorum. Ben de bu nedenle kullanıyorum açıkçası (Katılımcı 33).

5.2.6. Veri Gizliliği ve Güvenliğine Dair Kullanıcı Farkındalığı



Şekil 10. Veri gizliliği ve güvenliğine dair farkındalıklar

Katılımcılar SSA'ları kullanmaya yönelik veri gizliliği ve güvenliği konusunda ne tür bir bilgiye sahip olduklarına dair beş farklı yanıt sunmuştur. 16 kişi (%32,7) SSA'nın veri gizliliği politikaları hakkında bilgisinin olmadığını fakat buna rağmen

kullanıcı verilerine yönelik bir gizlilik ihlali söz konusu olduğunu düşündüğünü dile getirmektedir. 15 kişi (%30,6) bu hususta bilgisi olduğunu ve kişisel verilere yönelik bir gizlilik ihlali olduğunu düşündüğünü ifade etmektedir. 12 kişi (%24,5) yalnızca veri gizliliğine dair hiçbir bilgisi olmadığını belirtirken, konu hakkında bilgisi olan fakat gizlilik ihlaline yönelik endişesi olmadığını dile getiren kişi sayısı 5'tir (%10,2). 1 kişi (%2) ise bilgisinin doğruluğundan emin olmadığını dile getirmektedir. Veri gizliliği ve güvenliği konusunda bilgisi olan katılımcılar çoğunlukla bu bilgilerin reklam amaçlı satılmak için kaydedildiğini ve saklandığını düşündüklerini dile getirmektedir. Görüşmelerin tümünde “reklam” kelimesi aratıldığında 28 katılımcının (%57) bu kelimeyi kullandığı görülmektedir.

Herkesin standart bildiği şeyler. Örneğin bir ortamda bir ayakkabıya dair bir şey konuşuyoruz ve Instagram'da karşımıza reklam olarak çıkıyor. Sesli asistanda da bununla ilgili şeyler vardır muhtemelen. Yani o güvenlik açısından kalkıp telefonumuzu hackleyeceklerini düşünmüyorum ama bu tür reklamlar amacıyla muhtemelen çok da güvenilir olduğunu düşünmüyorum (Katılımcı 30).

Açıkçası bu konuda bir araştırma yapmadım ancak bu ve benzeri internet ortamında “veri gizliliğiniz korunacaktır” diyen hiçbir yazıya güvenmiyorum. Çünkü eğer Google reklamları benim arama yaptığım şeyler sonucu bana öneriliyorsa demek ki benim aramalarım paylaşıyor. Google ad sizin aramalarınıza yönelik reklam gönderiyor. Bu nedenle aramalarım Google tarafından paylaşıyorsa başka yerlerle de paylaşılabilir. Ben güvenilir bulmuyorum. Yakın zamanda Whatsapp ile de benzer sorunlar ortaya çıktı. Paylaşılanlar paylaşıyor zaten, Whatsapp kullanımı da yine devam edecek. Bu yüzden benim için bir sakınca yok, zaten edinecekleri bilgiyi edindiler (Katılımcı 33).

Görüşmeler sırasında katılımcılardan 8'i WhatsApp'ın o dönem gündemde olan Avrupa'daki gizlilik politikalarını değiştirdiği yönündeki haberlere atıfta bulunmuştur (TRT, 2021).

Veri güvenliğinin olduğunu düşünmüyorum. Verilerin korunduğunu söylemek bence bu aşamada mümkün değil. Geçenlerde okuduğum bir haberde iPhone'un yeni iOS sisteminde Facebook'un insanları dinlemesi engellenecekmiş. Facebook ve iOS arasında bir şeyler olabilir. Zaten reklam çağında yaşıyoruz, bu nedenle verilerimizin korunduğunu düşünmüyorum. Özellikle de herhangi bir asistanla (Katılımcı 8).

Katılımcı 8 burada iOS 14 güncellemesi ile gelen AppTrackingTransparency (Uygulama Takip Şeffaflığı) özelliği sonucunda Apple'ın kullanıcıları izinsiz takip eden

uygulamalara yönelik olarak takip eylemini gerçekleştirmek ve bu doğrultuda reklamlar sunabilmek için kullanıcıdan izin isteme koşulunu getirmesi ve Facebook'un reklam politikalarının bundan olumsuz etkilenmesi haberlerine değinmektedir. SSA'ların gizlilik politikalarına baktığımızda halihazırda verilerin kaydediliyor olduğu bilgisinin kullanıcıya veriliyor olduğu görülmektedir (Apple ve Google bu bilgilerin kullanımının izne tabi olacağını ve gizlilik politikalarına uygun olarak işleneceğini belirtir. Katılımcıların büyük bir kısmının belirtmiş olduğu “SSA aracılığıyla aratılan şeyin reklamlarına maruz kalma” durumu ise çoğunlukla arama motorlarının reklam politikalarıyla ilgili olup doğrudan SSA ile ilgili değildir. Çünkü SSA burada yalnızca bir arayüz görevi görmektedir. Örneğin, Apple Siri aracılığıyla derlenen internet aramaları ve komutların kullanıcının kimliğiyle ilişkilendirilmediğini iddia etmektedir. Google ve Amazon da kişisel bilgileri reklam amaçlı veya diğer kuruluşlara satmak için toplamadığını kendi websitelerinde kamuya açık bir şekilde paylaştıkları gizlilik politikalarında belirtmişlerdir. Bu durumda SSA kullanımı sonrasında aratılan kelimelerin reklam olarak çıkmasının SSA'larla ilgisi olmaması gerekmektedir. Diğer ihtimal ise kullanıcıya verilen bu bilgilerin doğru olmaması ve veri ihlalinin gerçekleşiyor olduğudur.

Rachels'in (1975) belirttiği gibi, mahremiyet kişinin paylaşmaktan çekindiği ya da paylaşmanın kişi için dezavantaj yaratabileceği bilgileri de içerir. Dijital çağda bu bilgiler kullanıcının bilgisi olmadan çeşitli yollarla suiistimal edilebileceği gibi, bazı durumlarda kullanıcı paylaşmak istemediği bilgilerin paylaşımına da rıza gösterebilmektedir. O andan sonra veri gizliliği ve güvenliği şirketlerin inisiyatifine kalmaktadır. Şirketlerin bu hususlarda izlemiş oldukları kişisel verilerin ticari amaçlı kullanımına olanak sağlayana politikaları, veri hırsızlığı, verilerin üçüncü kişilere satılması gibi haberler basında sık sık yer almaktadır.

Görüşmeler içinde SSA kullanımına karşı olan ve kullanmayı reddeden tek kullanıcı olan Katılımcı 32, bu tür uygulamaların tümünün kişisel bilgilere erişiminin mümkün olduğunu ifade etmektedir. Bu nedenle kullanılmamasını tavsiye etmektedir. Katılımcı 32 aynı zamanda X kuşağı grubuna giren katılımcılardandır ve bakış açısı X kuşağı bireylerinin internet bağlantılı teknolojilere karşı muhafazakâr bir tutum sergilediği genel görüşüyle benzerlikler göstermektedir.

Günümüzde herhangi bir şeye ulaşıyorsanız, en az on yerden de size ulaşıldığını bilmeniz gerekir. Burada kullandığımız bilgiler sonrasında aleyhimize delil olarak kullanılabilir. Bu yüzden eğer kişisel bilgiye kullanılmaması yararlı olur diye düşünüyorum. Onun dışında elbette kimsenin bilmesinde sakınca olmayan fikirler, görüşler söylenebilir. Ancak verilerimizi başkasının bilmesini istemiyorsak bundan kaçış yok. Elimizde cep telefonu varsa bunu zorunlu olarak kabul etmiş oluyoruz. Teknoloji ile ne kadar az haşır neşir olunursa o kadar iyi olur diye düşünüyorum (Katılımcı 32).

Katılımcı 4, Z kuşağı bireyleri arasında yaygın olan yeni teknolojileri kullanmak zorunda hissetme baskısına vurgu yapmaktadır. Forbes'un (2011) "5 Things People Buy Because Of Peer Pressure (İnsanların Akran Baskısı Nedeniyle Satın Aldığı 5 Şey)" başlıklı yazısında listenin ikinci sırasında akıllı telefonlar, dördüncü sırada ise Apple ürünleri bulunmaktadır. Bu durum teknoloji kullanımını üzerindeki akran ve sosyal çevre baskısını doğrulamaktadır.

Pek fazla bilgiye sahip değilim ama günümüzde birçok kişi telefonunun dinlendiğini ve bilgilerinin kaydedildiğini biliyor, ben de onlardanım. Ama yine de kullanmak zorundayız çünkü çağımızın gerekliliği haline geldi (Katılımcı 4).

Veri gizliliğinin ihlal edilme riskine dair bilgisi olan fakat buna rağmen SSA ve benzeri teknolojileri kullanmaya devam ettiğini söyleyen katılımcılar mahremiyet kontrolünün azaldığı 21. yy'da mahremiyet endişelerinin de etkisini kaybetmeye başladığı görüşü olan gizlilik paradoksuna örnek teşkil etmektedir.

Bu konuda ciddi birkaç başlık olduğunu ben de biliyorum. Açıkçası bildiğim halde kullanmaya devam ediyorum diyebilirim (Katılımcı 20).

Bu uygulamaların kullanıcı verilerini kullanarak kendi sistemlerini iyileştirdiği gibi şeyler duymuştum, zaten kullanmak için de çeşitli izinler istiyor en başında. Ben çok umursamıyorum açıkçası, pek fazla kaygım yok bu konuda. Sonuçta bu teknolojiyi geliştirmek amacıyla kullanıyor ve ücretsiz olarak erişim sağlayabiliyoruz (Katılımcı 48).

Katılımcılar SSA'ların kullanıcıların kişisel verilerini kullanabildiğini ve yetkiyi kullanıcıdan aldığını bilmektedir. Buna rağmen çeşitli sebeplerle bu durumu kabul etmektedirler.

Bu konuda ciddi birkaç başlık olduğunu ben de biliyorum. Açıkçası bildiğim halde kullanmaya devam ediyorum diyebilirim. Bu bilgileri medya üzerinden ediniyorum, online gazete ve dergilerde bu konuda başlıklar okumuştum (Katılımcı 20).

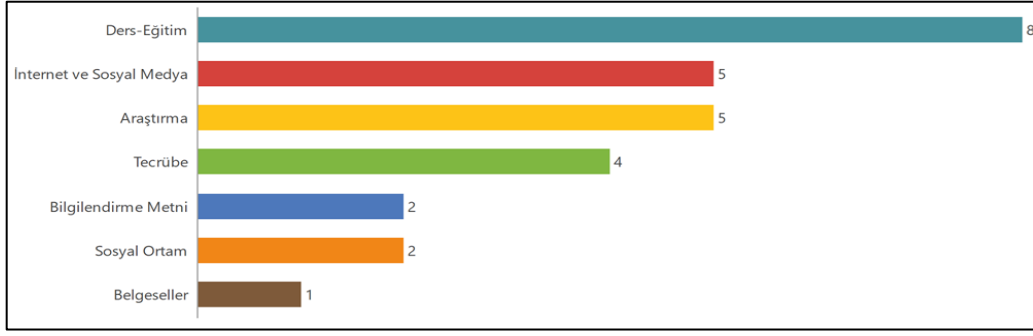
Katılımcı 35, bir kullanıcı olarak verilerinin korunmadığını düşünmektedir. Mahremiyetini koruyabileceği bir alan ve sınırlılık talep etmediği gibi kendisinin “önemli biri” olmaması nedeniyle verilerinin korunmaya değer olmadığı düşüncesindedir.

2021 dünyasında yaşıyoruz artık. Kaba bir tabirle ruhumuzu şeytana satmış durumdayız. Oradaki insanlar bizi bizden iyi tanıyorlar. Bu Facebook için de geçerli, verilerimizi alıp satıyorlar. Ben önemli bir diplomat falan olmadığım sürece de benim verilerimle çok büyük bir şey yapılacağını da düşünmüyorum. Verilerle ilgili gizlilik politikasını okuduğumda güven verdiğini düşünüyorum açıkçası. Ama ne kadar güven veriyor ya da ne tür bir yasa açığı var yurt dışında, Amerika’da bu konuyla ilgili çok fazla bir bilgim yok. Ama çok da güvendiğim söylenemez. Ama yapabileceğimiz bir şey de yok zaten. Bunlar ister istemez Silikon Vadisi’nde depolanacak. Yapabileceğimiz bir şey yok bu konuda ama güvenlikte benim tek aklıma takılan şu olur, ki bunu da kabul etti Apple; Siri bizi dinliyor. Ve bizim kendi konuşmamızdan belli verileri seçip ona göre reklam sunuyor, tanıtımlar yapıyor. Ve AI dediğimiz yapay zekâ olduğu için işin içinde, daha kolaylık sağlamak adına kendini geliştiriyor. Ama tabii ki bu söyledikleri ne kadar doğru, sadece veri almak için mi yoksa başka amaçlar için mi dinliyorlar orasını bilmiyorum. Ama ben Siri’yi kullanırken de ayarlardan Siri dinleme ayarını kapalı tutuyorum her zaman (Katılımcı 35).

Katılımcı 9, kullanıcıyı “veri” olarak tanımlayarak aslında dijital dünyanın hammaddelerinin kişisel veriler olduğunu vurgulamıştır. Üstelik bugün internet kullanmaktan vazgeçse bile bunun çözüm olmayacağını düşünmektedir.

Bizler zaten her alanda veriyiz, bu nedenle gizlilik konusunda endişe duymuyorum. Telefon kullanan herkesin bütün bilgileri var. Sadece Google asistan için özellikle tedirginlik duymuyorum. Gizli kalabilmek için interneti hiç kullanmamam gerekir. Mesela E-devlette bile her bilgim kayıtlı. Derslerimizde büyük veriyi ele aldığımız ve bildiğimiz için endişe duymuyorum. Hiç internet kullanmam gerekiyor. Kullanmasam bile geçmiş bilgilerim yine ellerinde olacak. Her halükârda veriyim (Katılımcı 9).

5.2.7. Veri Gizliliği ve Güvenliğine Dair Bilginin Kaynakları

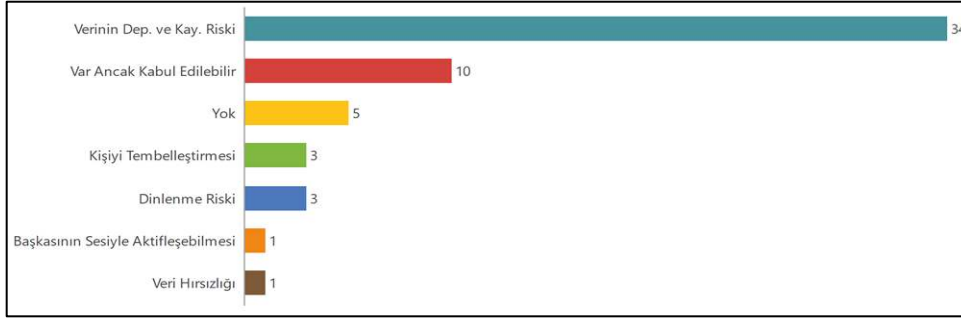


Şekil 11. Veri gizliliği ve güvenliğine ilişkin bilgi kaynakları

Katılımcılar arasında veri gizliliği ve güvenliğine dair bilgisi olanların bazıları bu bilgileri nasıl edindiklerini anlatmışlardır. Şekil 11'deki grafikte görüldüğü üzere bilginin kaynağını en çok dersler ve eğitimler oluşturmaktadır. Bunun önemli bir nedeni görüşme yapılan katılımcıların oluşturduğu örneklemin İletişim Fakültesi öğrencileri olmasıdır. Buradan yola çıkarak okullarda müfredata zorunlu ders olarak eklenmesi gerekliliği uzun süredir tartışılan medya okuryazarlığı dersinin önemi bir kere daha anlaşılmaktadır. Kullanıcılar bu sayede kişisel verileri üzerindeki haklarını ve gizlilik politikalarını bilerek bu uygulamaları kullanmaya veya kullanmamaya karar verebilmektedir. Katılımcılar için veri gizliliği ve güvenliğine dair bilgi edindikleri diğer kaynaklar ise günümüzde bilgiye ulaşmanın en hızlı yolu olan internet ve sosyal medyadır. Her ne kadar internette doğru bilgiye ulaşmak zor olsa da kullandığı uygulamaların gizlilik şartlarını ve kullanıcı olarak bu şartlar karşısında ne yapması gerektiğini bilmek isteyen bilinçli bir kullanıcı bu bilgilere kolaylıkla erişebilmektedir.

Grafikte dikkat çeken önemli bir nokta da katılımcıların çok azının aslında bir gizlilik ihlali tecrübe ettiğini düşünmesidir. Çünkü Kullanıcı Farkındalığı yanıtlarının kodlamalarında görüldüğü gibi toplamda 31 kişi (%63,3) gizlilik ihlali olduğunu düşündüğünü belirtmiştir. Buradan anlaşılmaktadır ki, kullanıcılar gizlilik ihlalinin birinci elden tecrübe etmemiş olsalar bile bu konuda bir bilinç oluşturabilirler. Ya da tam tersi olabilir ve SSA'lar ile olumsuz bir tecrübesi olan kullanıcı buna rağmen kendi rızasıyla SSA'ları kullanmaya devam edebilmektedir.

5.2.8. Sesli Sanal Asistanların Gizlilik Yönünden Dezavantajları



Şekil 12. SSA’ların gizlilik yönünden dezavantajları

Katılımcılara SSA’ların dezavantajları sorulduğunda 34 kişinin (%69,4) kişisel bilginin kaydedilme ve depolanma riskinin dezavantaj olarak değerlendirdiği görülmektedir. Bu verinin, çalışmada yer alan önceki soruların sonuçlarına ilişkin grafiklerle karşılaştırıldığında SSA’ların veri işleme süreçlerinde gizlilik ihlali olduğunu düşünen kişi sayısı (31 kişi) hemen hemen tutarlı olduğu görülmektedir. Katılımcı 18, SSA’lar aracılığıyla günümüzde birçok kişisel bilgimizin depolanıyor oluşuna dikkat çekmektedir ve kullanıcıların bu durumu yaşadıklarının farkında olmadığını ifade etmektedir. Fakat bu katılımcının ve diğer birçok katılımcının ifadeleri aslında katılımcıların kişisel veri gizliliği ihlalleri konusunda az ya da çok bilgisi olduğunu göstermektedir.

Hepimiz birtakım yöntemlerle sesli asistanları kullanıyoruz. Sesimiz, parmak izimiz, gözlerimiz, bunlar bir yerde depolanıyor ve bir gün bunlarla bir yerde karşılaşacağız. Bir şekilde fişleniyoruz ve bunu bilmeden yapıyoruz. Çünkü sesli asistana yönelttiğimiz sorular, yaptığımız aramalar (konuşmalar) ya da bir arama yaptıktan sonra bunlar reklam olarak karşımıza çıkıyor. Bu da bilgilerimizin bize karşı kullanıldığının göstergesi (Katılımcı 18).

Kişisel veri gizliliğinden bahsederken görüşmelerin yapıldığı günlerde gündemde olan WhatsApp’ın Avrupa’daki gizlilik sözleşmesini değiştirdiği ve onay vermeyen kullanıcıların hesaplarının silineceği haberlerine değinen katılımcılardan anlaşıldığı üzere, bu olumsuz gelişme birçok internet, sosyal medya ve SSA kullanıcısının gizlilik sözleşmesi konusunda bilgi sahibi olmasını sağlaması açısından iyi bir örnek olmuştur. Fakat çoğunlukla, her koşulda bu teknolojiler kullanılmaya devam edecektir. Katılımcı 2’nin belirttiği gibi kullanıcılar bu şirketlere güven duymak ya da daha gerçekçi tabirle hizmet şartlarına boyun eğmek zorunda kalmaktadır.

Katılımcı 10, SSA'ların dezavantajları olduğunu fakat bunların kabul edilebilir boyutta olduğunu düşünmektedir. Aynı zamanda Katılımcı 24'ün belirttiği gibi bazı kullanıcılar kişisel verilerinin uygulamaları geliştirmeye yönelik olduğu sürece şirketler tarafından işlenmesine onay vermektedir.

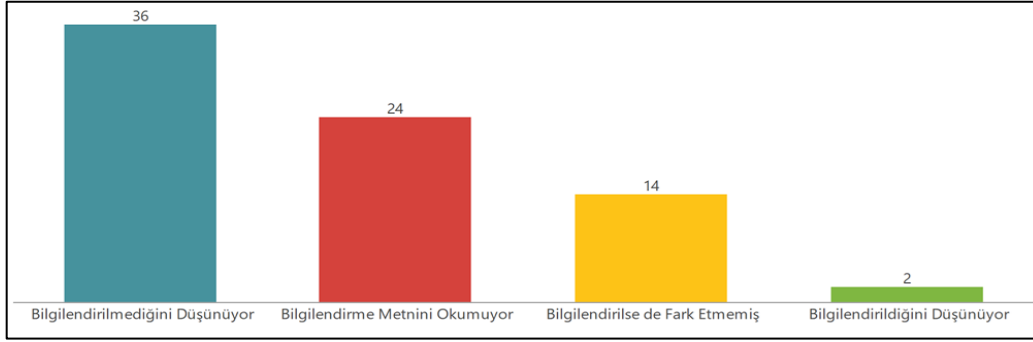
Bence bir şirket böyle bir şey geliştiriyorsa verileri koruyordur diye düşünüyorum fakat yine de konumum, e-postalarım gibi bilgileri aktarırken bir düşünce içinde oluyorum. Yine de bir taraftan bu bilgilerin gizlendiğini düşünüyorum. Haberlerde çok sık duyuyoruz o nedenle biraz şüpheliyim (WhatsApp örneğini veriyor). Bu nedenle “acaba sanal asistanlarla da dinleniyor muyuz, verilerimiz kullanılıyor mu” diye tereddütte düşünüyorum. Yine de bu şirketlere güven duymak zorundayız (Katılımcı 2).

Bana kalırsa şu an kullandığımız dijital aletlerin tümü veri topluyor zaten. Sözleşmesini imzalıyoruz. Apple, Google gibi büyük şirketlerin sözleşmelere uymaları zaten şart. Çünkü çok büyük hukuki sonuçları olabilir. Apple o konuda biraz güven veriyor bana. Tabii ki verileri topluyor ve pazarlıyorlar ancak bunların ne olduğu, hangi verilerin ve ne amaçla kullanıldığı tabii ki Apple kullanmamın ana nedenlerinden bir tanesi. Ancak şimdi Apple “tüm verilerinizi hükümetlerle, reklam şirketleriyle, anket şirketleriyle paylaşacağım” derse kullanmaktan vazgeçmem ancak yaptığım şeyler (kullanma yöntemim) değişir. Örneğin benim verilerim bir meta gibi kullanılmasın ancak haber akışında, ihtiyacım olan, ilgilendiğim şeylerde, alışverişte vs. kullanılsın. Bu benim için de iyi çünkü ihtiyacım olan şeyler önüme çıkıyor. Bu konuda o kadar katı değilim ancak bu durum Whatsapp'ta olduğu gibi politik ve sosyolojik bazı bilgilerimizi edineceklerse durum değişir. Tabii ki kullanırım yine de ancak çevrimdışıyken Siri'nin kapanmasını isterim. Şu an açık ve sesli komutla bana dönüş yapıyor ama mesela öyle olaylar olursa kapatırım. İhtiyacım olduğunda kullanırım. Konum bilgisini ona göre paylaşırım vs. hangi verilerin toplandığı ve onun kimlerle paylaştığı meselesi önemli benim için (Katılımcı 24).

Derslerimizde büyük veriyi ele aldığımız ve bildiğimiz için endişe duymuyorum. Hiç internet kullanmam gerekiyor. Kullanmasam bile geçmiş bilgilerim yine ellerinde olacak. Her halükârda veriyim (Katılımcı 9)

5 Katılımcı SSA'ların dezavantajı olmadığını düşündüğünü ifade etmiştir. Aslında bu cevaplarda “olabilecek mahremiyet ihlallerini dezavantaj olarak algılamamak” düşüncesi vardır. Kişisel verilerin dijital çağda, sanal bir ortamda korunabilmesinin hiçbir yolu yoktur, bunun için internet kullanmamak gerekir. Bu ifadeler, kişisel verileri koruyabilmek adına alınan kişisel önlemlerin değerlendirildiği başlıkta görülebileceği gibi neden çoğu katılımcının önlem almıyor olduğunu açıklamaktadır.

5.2.9. Kullanıcıların Gizlilik Politikaları Konusunda Bilgilendirilmesi



Şekil 13. Gizlilik politikalarına dair bilgilendirilme durumları

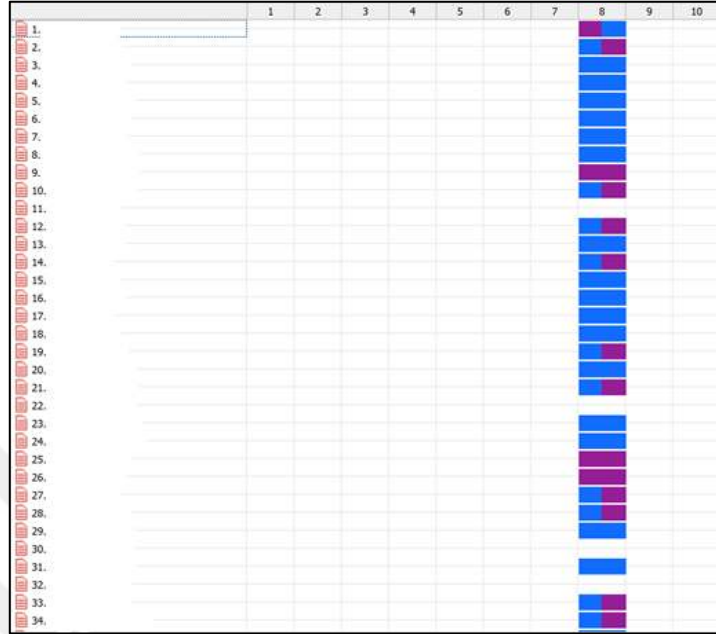
Kullanıcının bilgilendirilmesi yasal bir süreçtir. Bununla birlikte çalışmada önceden belirtildiği üzere kullanıcılar çoğunlukla kişisel bilgilerinin önemsiz olduğunu düşünmeye eğilimlidirler. Katılımcı 44'ün ifadesi bu duruma örnek gösterilebilir. Kullanıcılar için gizlilik politikalarını açıklayan bilgilendirme metinlerini okumak zordur çünkü bu metinler uzun ve detaylıdır. Kullanıcının ne düşündüğünden bağımsız olarak şirketler her koşulda verilerin güvenliğinden sorumludur.

Tam bilmiyorum. Mesela ben önemli birisi değilim ve çoğunluk da öyle. Aldığı bilgiler basit ve uygulamaları bizim için geliştirmeye yönelik bilgiler sadece. Bize bir fayda sunuyor. Ama mesela benim bilmediğim şeyler de olabilir, bizim için kaydedilen bilgiler istemediğim bir yerlere gidebilir ama ben bunu tam bilmiyorum. O yüzden benim için fazla dezavantaj yok. Dinleniyor olmak da benim için dezavantaj değil. Bilgilerimi alıyorsa ne faydası var, alsınlar. Bence bir önemi yok. Tamam özel ve bana ait ama aynı zamanda telefon benim bir parçam ve bu onun KDV'si. Bir bedel. O uygulamalar bizim için geliştiriliyor. Sadece uygulamalar için değil mesela siyasi, hükümet için sebeplerle kullanıyorsa biz bilemeyiz. Zaten biz normal insanlarız, aldıkları bilgiler neye yarayabilir ki? (Katılımcı 44).

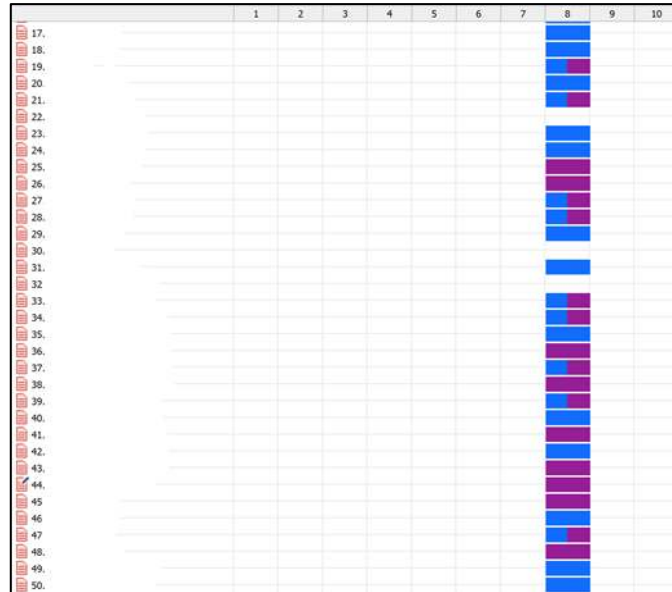
Katılımcılara gizlilik politikalarına dair ne kadar bilgilendirildikleri sorulduğunda 36 katılımcı (%73) bu konuda bir bilgilendirmeye karşılaşmadıklarını ifade etmektedir. 24 katılımcı (%49) ise bilgilendirme metinlerini okumadıklarını, okumadan onay verdiklerini belirtmiştir. Bu iki kullanıcı grubundan 14 katılımcı hem bilgilendirilmediğini hem de bilgilendirme metinlerini okumadığını söylemektedir.

Tablo 2.

Katılımcıların Gizlilik Bilgileri ve Bilgilendirme Metinlerini Okuma Oranları Arasındaki İlişki

**Tablo 3.**

Katılımcıların Gizlilik Bilgileri ve Bilgilendirme Metinlerini Okuma Oranları Arasındaki İlişki 2



Tablo 2 ve 3'te bilgilendirildiğini düşünmeyen katılımcılar lacivert renkli kutucuklar ile, bilgilendirme metinlerini okumayan katılımcılar ise mor renkli kutucuklar ile temsil edilmiştir. Yandaki sayılar katılımcıları göstermektedir. Tabloya

göre 14 katılımcı hem bilgilendirilmediklerini düşündüğü hem de bilgilendirme metinlerini okumadığı görülmektedir. Bu katılımcılardan biri olan Katılımcı 12 gizlilik metinlerini tatmin edici bulmadığını ve bu metinlerin yüzeysel bilgiler içerdiğini ifade etmektedir.

Bu konuda derinlemesine bir araştırma yapmadım ancak internet üzerinden, sosyal medyada okuduğum bilgilere göre bende bu düşünce oluştu. Tonlarca bilgiler yazsalar da beni tatmin edecek bilgiler sunduklarını düşünmüyorum. Bilgileri kendilerine özel bir şekilde sakladıklarını düşünüyorum. Çünkü onların bize sunmuş oldukları gizlilik ilkeleri genellikle çok uzun oluyor ve insanların okuma sürelerini tahmin ettiklerini ve ona göre yazdıklarını, kimsenin gizlilik ilkelerini sonuna kadar okumayacağını bildiklerini düşünüyorum. Bu yüzden de bize vermiş oldukları tüm o bilgilerin aslında kısıtlı bilgiler olduğunu düşünüyorum. Yani bize arka planını sunduklarını düşünmüyorum. Yüzeysel bilgiler veriyorlar (Katılımcı 12).

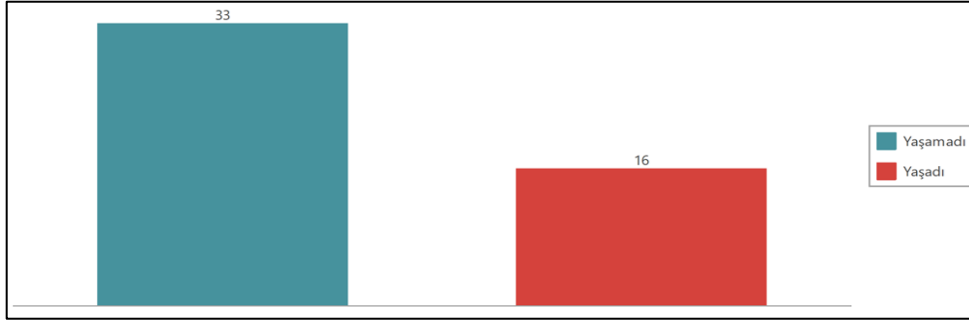
Hem bilgilendirilmediğini düşünen hem de bilgilendirme metinlerini okumayan katılımcılardan bir diğeri olan Katılımcı 14 bilgilendirme metinlerinin “çok pozitif” olduğunu ve bu nedenle okumayı tercih etmediğini, inandırıcı bulmadığını dile getirmiştir.

Bir uygulamayı indirdiğimizde uzun bir sözleşme çıkıyor ve o sözleşmenin birkaç maddesini okuyorum ve o maddeler de çok pozitif oluyor; uygulamanın hayatımızı kolaylaştıracağını, bize çok yardımcı olacağını ve her yerde kullanabileceğimizi ifade eden maddeler. Ve bunları görünce ben gerisini okumuyorum. Yeterince bilgilendirilmiyoruz, daha çok Google şirketinin daha pozitif ve yardımcı bir uygulama geliştirdiğini sanmamızı istediğini ve bizim de buna ayak uydurduğumuzu düşünüyorum (Katılımcı 14).

Bununla birlikte bazı katılımcılar bilgilendirme metinlerini okumakta ve bu doğrultuda gizliliklerini koruyabilmek adına kişisel önlemler almaktadırlar. Katılımcı 35 bilgilendirme metinlerini okuyarak bir aracı kullanıp kullanmayacağına karar verdiğini ifade etmektedir.

Google’ın ve Apple’ın kendi gizlilik politikalarını biliyorum. Örneğin Xiaomi’nin kendi sesli asistanı da var ancak Çin menşeli olduğu için onun gizlilik politikasını kabul etmedim. Sadece program üzerinden manuel bir şekilde evdeki kilit sistemini kullanıyorum (Katılımcı 35).

5.2.10. SSA'ların Veri İhlaline İlişkin Katılımcıların Kullanıcı Tecrübesi



Şekil 14. SSA'ların veri ihlaline ilişkin katılımcıların tecrübeleri

Katılımcılardan 33'ü (%67,3) sesli sanal asistanlar kaynaklı veri gizliliği ve güvenliğine ilişkin kişisel bir tecrübe yaşamadığını beyan etmektedir. 16 katılımcı (%32,7) ise böyle tecrübeler yaşamış olduklarını ifade etmişlerdir. Tecrübesi olan katılımcıların birçoğu bu tecrübeyi SSA ile arattıkları şeylerin daha sonra reklam olarak karşısına çıkması olarak tanımlamışlardır.

Ben yakın zamanda sürekli abiye elbiselere bakıyordum. Bunu bir kere Siri'de arattım. Yaklaşık bir buçuk aydır hiçbir şekilde bakmıyorum ve hala reklamlarımda abiye kıyafetleri görüyorum. Karşıma çıkan başka bir reklam yok, bütün reklamlarda. Daha önceden aratmış olduğum bu ürünün reklamlarını görüyorum (Katılımcı 34).

Katılımcıların çoğu SSA'ları kullanırken onlarda veri gizliliğine dair olumsuz düşüncelere neden olmuş olan durumlarla karşılaşmadıklarını belirtmiş olsa da, kişisel verilerle ilgili duyulan endişe boyutunun yüksek olduğu görülmektedir. Çoğu dijital yerli olan katılımcıların böyle kaygılar taşımasındaki temel gerekçenin, dijital çağın bireylerde yarattığı “gözetleniyor olabilirim” düşüncesi olduğu söylenebilir. İnternet bağlantılı cihazlarla donatılmış olmak, kameralar, kişi internet kullanıcısı ise her gün bir şekilde kişisel bilgi paylaşımında bulunuyor olmak gibi birçok unsur bireyler üzerinde gizlilik endişesi yaratmaktadır.

Sadece daha önceki telefonumu kullanırken şöyle bir şey geldi başıma: ben bir ayakkabı markası söyledim. Ve bu ayakkabının reklamı ben ne kadar algoritmayı değiştirmek için uğraşsam da 6-7 ay kadar karşıma çıktı. Zor kurtuldum reklamdan. Mesela bir SSA'a Trendyol dersiniz, bitti. Bundan sonra her banner'da sadece Trendyol çıkar (Katılımcı 36).

Katılımcı 28 ünlü bir oyuncunun yaşadığı olumsuz tecrübeyi paylaşmıştır.

Hayır. Amerikalı bir oyuncunun her şeyi ortaya dökülmüştü onu okumuştum ve o dönemde kullanmayı azaltmışım ancak sonra tekrar başladım (Katılımcı 28).

Katılımcı 10, bir tecrübe yaşamamış olmasına rağmen duyduğu bir kötü tecrübeyi paylaşmaktadır ancak SSA'lar özelinde bir durum değildir. Katılımcı yine de kişisel verinin ihlalinin çağrıştırdığı bir olumsuz deneyimi dile getirmek istemiştir.

Henüz bir şey yaşamadım. (Burada arkadaşının kuzeni ile ilgili bir durumu anlatıyor, kartından para çalındığını.) Mahkeme süreci olmuş ve ona internet ortamında hesap kart bilgilerini ve kart şifresini paylaşp paylaşmadığı sorulmuş. Alınan karar doğrultusunda veri açığından faydalanarak bilgilerin çalındığı ortaya çıkmış. Çözüme ulaşmadı ve bunu yapanı da bulamadılar. (S. Asistan kaynaklı bir durum muydu diye sorduğumda “Hayır” diyerek anlatmaya devam etmiştir) (Katılımcı 10).

Katılımcı 5 haberlerde ve internette duyulan olumsuz deneyimlerin doğruluğu kanıtlanamadığı için inandırıcı bulmadığını dile getirmektedir.

Kişisel bir tecrübem olmadı ve hiç duymadım. Yalnızca haberlerde ve internette duyduğum şeyler. O bilgiler de teyide muhtaç bence (Katılımcı 5).

Kullanıcı farkındalığının incelendiği bölümde de üzerinde durulduğu gibi, SSA aracılığıyla aratılan ifadelerin ve içeriğindeki ürünlerin, nesnelerin vs. katılımcıların karşısına reklam olarak çıkması, katılımcıların yaşadıkları gizlilik ihlallerine örnek sunarken en çok dile getirdiği detay olmuştur.

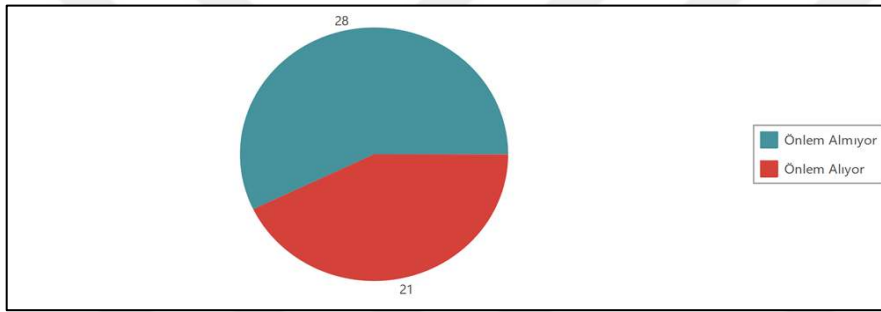
Bence herkesin olmuştur ancak kimi kabul etmekte zorlanıyor ya da farkına varmıyor. Bizler iletişim öğrencisiyiz, bu yüzden farkındayız belki. Ama özellikle reklamlar konusunda dikkatimi çekiyor benim. Ben de reklamcılık alanında ilerlemek istiyorum. Reklamlar konusuna özellikle Google özelinde bakacak olursak aramalarımızın karşımıza çıkması gizlilik konusunda büyük bir soru işareti. Bu bile herkes için olası bir tehdit ve aynı zamanda edinilen bir tecrübe (Katılımcı 33).

Benim daha önce vermediğim bilgilerle bana dönüş yapması başlarda tuhaf gelse de böyle şeyler olabileceğine dair öğrendiklerimden sonra alıştım. Tek kaygım, ilerde bir gün benim telefonumdaki mesajlar, bilgiler ve numaraların başkalarının eline geçmesi (Katılımcı 7).

Katılımcı 1'in Siri ile yaşamış olduğu kötü tecrübenin uygulamanın yazılımındaki yetersizlikler nedeniyle gerçekleştiği söylenebilir. Bu nedenle kullanıcı büyük bir veri ihlali ile karşılaşma riski yaşamıştır. Katılımcı 1 bu tecrübesinden sonra SSA kullanımına kişisel kısıtlamalar getirdiğini belirtmiştir.

Çalıştığım dönemde yaşadım. Eldeki dokümanlarla, resmi evraklarla Siri üzerinden işlem yapmamaya dikkat ediyordum ancak bazen kullanmam gerekiyordu. Bir evrağı Siri, ismi aynı olan iki Gümrükçüden yanlış olana gönderdi. Eğer bu kişi karşı firmadan biri olsaydı, bilgi sızdırmakla suçlanabilirdim. Bu tecrübemden sonra kamusal alanda Siri'yi kullanmadım. Siri akıllı bir teknoloji olsa da bir insan zekâsı değil. Bu nedenle böyle tehlikeli durumlarda Siri'yi kullanmıyorum (Katılımcı 1).

5.2.11. Kullanıcıların Aldığı Kişisel Önlemler



Şekil 15. Katılımcıların aldığı kişisel önlemler

Katılımcılara sesli sanal asistan kullanırken veri gizliliği ve güvenliklerini koruyabilmek adına aldıkları kişisel önlemler sorulduğunda katılımcıların 28'i (%57,1) herhangi bir önlem almadığını belirtmektedir. 21 katılımcı (%42,9) önlem aldıklarını belirtmiş, bu önlemler genellikle SSA'ların erişimi olan diğer uygulamaları kısıtlamak ya da gizliliği önemsenen aramaların SSA'lar ile yapılmaması olmuştur, ki telefonun kendi arama motoru kullanıldığı zaman bu önlem bir sonuç vermeyecektir. Gizlilikleri konusunda kaygılanan kullanıcılar SSA'ları kullanmadıkları zamanlarda kapalı tutmak gibi çözümler uygulamaktadırlar (Edu, Such ve Suarez-Tangil, 2021). Katılımcı 20 ve Katılımcı 35 bu şekilde bir önlem aldıklarını dile getirmiştir.

Apple cihazları için şuna dikkat ediyorum. Siri'yi uzaktan aktive eden “Hey Siri” komutunu olabildiğince kapalı tutmaya çalışıyorum. Çünkü arka planda çok fazla çalışıyor ve o özelliği kullanırken sizi sürekli dinlemesi gerekiyor. Ayrıca çok fazla özel ve spesifik, detaylı bilgileri paylaşmamaya dikkat ediyorum. Daha çok “hava nasıl” gibi gündelik meselelere dair aramalar yapıyorum (Katılımcı 20).

Evet var. Alexa ve Siri’de dinleme özelliğini kapalı tutuyorum. Anlık konumu da kapalı tutuyorum. Gerçekten güvenilir programlarda Siri kullanımına izin veriyorum, fakat üçüncü kişilerle bilgi paylaşan, güvenlik açığı bulunan programlarla Siri kullanımına izin vermiyorum. Banka hesaplarımda da kullanmıyorum (Katılımcı 35).

Alexa kullanıcısı olan Katılımcı 34, Alexa kullanırken aldığı önlemler olduğunu ifade etmektedir.

Alexa’nın bir özelliği de ev içerisinde kamera sistemi denilen bir özelliği var. Onla bağlantılı olarak kameraları mümkün mertebe gece saatlerinde, uyku saatlerinde çok fazla etkin olarak çalıştırmamaya çalışıyorum. Özellikle kendi kişisel alanlarımda, örneğin mutfakta veya koridorda olabilir ama kendi yatak odama veya banyoma yerleştirmemeye çalışıyorum. Onun dışında kendimle ilgili çok özel ve kişisel şeyleri bu tarz sistemlerde aratmamaya çalışıyorum ki bu alınabilecek en basit önlem (Katılımcı 34).

Kendimi alacağım bütün önlemlere rağmen güvende hissetmeyeceğim için çok büyük önlemler almıyorum (Katılımcı 22).

Hayır yok. Ben zaten dezavantajı varsa bile bunu kabullenmişim, o yüzden önlem alacak bir durum bence yok (Katılımcı 2).

Bu çağda istediğimiz kadar tedbir alalım, araştırdığımız her şey kayıt altında. Bence önlem almak imkânsız, bundan bir kaçış yok. Önlem alınsa da önüne geçilemez (Katılımcı 6).

Ne kadar önlem alsam da Google Asistan’ı aktif ettiğim andan itibaren, telefonu kapatsam bile bilgilerime erişebileceğini düşünüyorum. Önlem alsam da bir işe yaramayacağını düşünüyorum (Katılımcı 7).

Katılımcıların dile getirdikleri bir diğer ortak husus ise her ne kadar önlem alınırsa alınsın veri gizliliği ve kişisel mahremiyetleri açısından olumlu sonuç vermeyeceğini düşünüyor olmalarıdır. Bu bulgular da yine gizlilik paradoksuna örnek gösterilebilir.

SONUÇ

Bu tez çalışması, SSA'ları mahremiyet ve kişisel veri gizliliği yönünden ele alarak Türkiye'de SSA'ların tekniğine ve SSA kullanıcılarının deneyimine odaklanan mevcut çalışmaların bulunduğu literatüre katkı sağlamayı amaçlamıştır. 2011 yılında kullanıcıya sunulan SSA'lar şimdiden milyonlarca kullanıcıya sahiptir. Her bir kullanıcı mobil cihazlarında veya akıllı hoparlörlerinde bulunan bu yazılımları ev ortamlarında, iş yerlerinde, kişisel araçlarında, okullarında kullanmaktadır. Bu yazılımların ait olduğu dev şirketlerin yalnızca birinin bile veri ihlali yapması milyonlarca bireyin veri gizliliği ve mahremiyetinin çiğnenmesi anlamına gelir. Mahremiyet sorunu SSA ve benzeri akıllı teknolojilerin yaygınlaşmasıyla artacağı öngörülen ve kullanıcı yönünden önlem alması gittikçe zorlaşan bir “dijital çağ” meselesidir.

Görüşmelerden sonra katılımcılardan birinin mahremiyet endişeleri olduğunu belirterek çalışmada yer almak istemediğini beyan etmesi, mahremiyet endişelerinin boyutlarını ortaya çıkaran bir örnek olmuştur. Öğrencilere bilgilerinin gizli kalacağı ve anonimlik hakları açıkça beyan edilmiş olsa dahi bu beyanlar bazen yeterli bulunmamakta ve kişileri tatmin etmemektedir. Çalışma grubu yaş dağılımı bakımından homojendir, katılımcılar büyük oranda 1991-2001 yılları arasında doğmuştur ve bu yaş aralığı Y ve Z kuşağın bireylerine denk gelmektedir. Çalışmanın örnekleminin İletişim Fakültesi öğrencileri olması, çalışmanın dijital yerlilerin dijital teknolojileri aktif ve iyi derecede kullanabildikleri varsayımına yakın nitelikte sonuçlar elde edilmesinde etkili olmuştur zira katılımcılar hem iletişim alanında eğitim almakta hem de SSA kullanmaktadır. Zaten çalışmanın örnekleminin belirlenmesindeki temel gerekçe dijital çağda doğup büyüyen bu bireylerin veri gizliliği ve güvenliği konusunda farkındalık geliştirip geliştiremediklerini sorgulayabilmektir. Nitekim net çizgilerle bir dijital yerli-dijital göçmen ayrımı yapılamayacağını doğrularcasına, dijital yerli olarak kabul edilen bazı katılımcıların sohbet botları ve SSA'ları karıştırdığı görülmüştür. Çok yakın teknolojiler olmalarından dolayı bu doğal bir durum olsa da bu teknolojiler yazılım yönünden birbirinden ayrılmaktadır. Bu nedenle çalışmada bu iki teknolojinin temel farklılıklarına değinilmiştir. Tüm katılımcılar arasında yaşı en ileri olan katılımcı hiç SSA deneyimi olmadığını belirtmiştir. X kuşağının bir bireyi olarak bu katılımcı dijital göçmenlere atfedilen şu özellikleri doğrulamıştır: dijital göçmenler yeni teknolojileri öğrenirken zorlanmaktadır ve geleneksel yöntemleri teknolojiye tercih ederler. Çalışmadaki bir diğer X kuşağı bireyi olan katılımcı ise aktif bir SSA kullanıcısı

olmakla birlikte mahremiyet endişeleri taşıdığını fakat bu endişelerin bilgisizliği nedeniyle olduğunu dile getirmiştir. Bu bulgular ışığında, X kuşağının teknolojilere hâkim olabilme yönünden Y ve Z kuşağından daha fazla çaba harcaması gerektiği düşünülse de, bu kuşağın bireylerinin birer aktif teknoloji kullanıcısı olamayacağını varsaymak da yine son derece eksik bir değerlendirme olacaktır.

Çalışmada en sık dile getirilen SSA kullanım amacı internette arama yapmaktır ve Easwara Moorthy ve Vu'nun 2014 yılında yaptığı "Voice Activated Personal Assistant: Privacy Concerns in the Public" başlıklı araştırmasında belirtildiği üzere, SSA'ların ilk yılları sayılabilecek dönemlerde de en yaygın kullanım amacı internette arama yapmaktır. Çalışmalarda bu açıdan benzer sonuçlar elde edilmiştir. Katılımcılardan bazılarının SSA'ları evdeki diğer akıllı cihazlarla etkileşimli hale getirerek kullandığını ifade etmesi, nesneler arası internet bağlantısı ve cihazların etkileşimli çalışmayı desteklemesinin (IoT) Türkiye'de de kullanılıyor olduğunu göstermektedir. Mobil SSA'ların akıllı hoparlör tipi SSA'lardan daha fazla kullanıldığı gözlemlenmiştir. İleriki çalışmalarda akıllı hoparlörlerin kullanımının yaygınlaşmasıyla bu modeller özelinde mahremiyet ihlaline değinen çalışmalar yapılabilir.

SSA gibi teknolojiler insanlara kolaylık getirirken bir yandan da en küçük işleri bile yapmalarına gerek kalmamasını sağlamaktadırlar. Görüşmede bazı katılımcılar SSA'ların sunduğu avantaj-dezavantaj belirsizliğine bu yönden dikkat çekmiştir. Özellikle COVID-19 salgını sonrası yoğun dijital teknoloji kullanımı ve hayatın neredeyse teknolojiye adapte olmuş olmasından sonra daha çok tartışılan bir mesele haline gelen "teknoloji nedenli tembelleşme" SSA'ların bir dezavantajı olarak kabul edilebilir. Barber (2015) "Can Artificial Intelligence Make Us Stupid? (Yapay Zekâ Bizi Aptallaştırabilir mi?)" başlıklı makalesinde Sanayi Devrimi'nden sonra insanların fiziksel olarak daha az aktif hale gelmesi ve kilo almaya başlaması gibi, dijitalleşmenin insanları daha az zeki yapmaya kadar varan tembelleşme yan etkileri olabileceğini dile getirmiştir.

Çalışmada öne çıkan bir başka bulgu ise SSA'ların engelli bireylerin hayatını kolaylaştırma yönünden faydalı teknolojiler olduğudur. Ancak böyle hayati bir kolaylığın sürdürülebilmesi için bu bireylerin veri mahremiyeti yönünden kayıplar yaşamaması gerekmektedir. Böylece bu teknolojileri endişe duymadan kullanabilmeleri söz konusu olabilir.

Katılımcıların SSA'ları tanımlarken olumlu ve SSA'ların avantajlarını vurgulayıcı tanımlamalar yapmış olması ve hiç olumsuz tanım yapılmamış olması,

katılımcıların bu teknolojileri kullanırken çoğunlukla memnuniyetlerinin yüksek olduğuna işaret etmektedir. Fakat büyük bir kısmı görüşmenin devamında mahremiyet endişeleri duyduklarını belirten görüşler dile getirmişlerdir. Katılımcıların büyük oranda dijital yerlileri temsil ettiği düşünüldüğünde, tüm katılımcıların daha önce çeşitli dijital araçları kullanırken mahremiyet ihlalini düşündürecek bir tecrübe yaşamış olması, dijital mecralarda kişisel bilgilerini paylaşmak konusunda olumlu ya da olumsuz bir fikir edinmiş olmaları olasıdır. Bazı araştırmalar göstermektedir ki, özellikle internet bağlantılı dijital teknolojilerin kullanımında sıkça rastlanan bir davranış olarak, kullanıcılar mahremiyetin az olduğu durumlarda veya mahremiyet belirsizliğine zamanla alıştıklarında, mahremiyet endişelerine neden olabilecek koşulları kabul etmeye daha yatkın olurlar (Vollan, 2017). Bireyler, mahremiyetlerinin ihlal edilmesiyle ilgili endişelerini dile getirirken bile, karşılığında kazanacakları bir şey olduğu sürece kişisel bilgilerini vermeye istek göstermişlerdir (Kokolakis, 2017). Literatürde “gizlilik paradoksu” olarak adlandırılan bu durum (Syverson, 2003) kullanıcıların internet ve dijital teknolojilerin yarattığı mahremiyet eksikliğine karşı ciddi endişeler duyduklarını dile getirmelerine rağmen, davranış bazında bu kaygıların tam tersini gösteren bir tutum sergilemeleri anlamına gelmektedir. Kullanıcılar SSA’ların kişisel verileri kaydediyor olmasını sunulan hizmetler karşılığında “küçük bir bedel” olarak görmektedir.

Çalışmanın en önemli bulgularından biri, katılımcıların veri gizliliği ve güvenliği konusunda ne tür bir bilgiye sahip oldukları sorulduğunda çoğunluğun bilgisi olmadığını belirtmesine karşın, veri ihlali konusunda da yine çoğunluğun SSA’ların veri gizliliğini ihlal ettiğini düşündüklerini belirtmesidir. Öncelikle, gizlilik politikalarına dair somut bilgileri olan katılımcı sayısının az olması beklenmedik bir bulgudur. Katılımcıların kendilerinden beklenildiği gibi aktif ve iyi derecede SSA kullandığı sonucu büyük oranda doğrulansa da veri gizliliği konusunda bilgisi olan katılımcı sayısının düşüklüğü, katılımcıların dijital mahremiyet farkındalığının düşük olduğuna kanıt gösterilebilir. Hem bilgilendirilmediğini hem de bilgilendirme metinlerini okumadığını dile getiren katılımcıların olması, bazı SSA kullanıcıların kişisel verinin güvenliğine dair bilgi edinmek, yapabiliyorsa kişisel önlemler almak gibi dijital çağda bir kullanıcının bilinçli internet kullanımı için alması gereken önlemleri ihmal ediyor olduğunu göstermektedir. Bilgilendirilme metnlerinin yeterliliği tartışmalıdır, hatta içerikleri yetersizdir ve doğal olarak kullanıcıda güvensizlik yaratabilir, kaldı ki bu metinlere ulaşmak kimi zaman zordur. Ancak bu metinleri kendi rızasıyla okumayı reddeden kullanıcıların bilgilendirilmediklerini düşünüyor olmaları, çevrimiçi

uygulamalarda gizlilik paradoksunun varlığının bir göstergesi olarak kabul edilebilir. Katılımcıların birçoğu bu metinleri okumanın bir fayda sağlamayacağına inanmaktadır ancak kişisel verilerinin güvende olmadığına da bilincindedir. Bu nedenle bu bulgu için direkt olarak “kullanıcı bilinçsizliği” denilememektedir ve bulgu daha çok gizlilik paradoksuna uygun bir örnektir.

Teknoloji kullanımının kaçınılmazlığı, sunulan hizmetlerden yararlanma arzusu gibi nedenlerin mahremiyet endişelerini büyük oranda baskıladığı görülmektedir. Daha doğrusu teknolojiden faydalanılmaya başlandığı anda memnuniyetin artıp endişenin azalması, katılımcıların gündelik yaşamlarında veri gizliliği ihlali, gizlilik politikaları gibi konular üzerine daha nadir düşünüyor olmalarına neden olmaktadır. Bu çalışmadaki veriler gizlilik paradoksunu doğrular niteliktedir. Syverson’un (2003, s.3) “Mahremiyetteki azalmanın da güvenlik açısından bir maliyeti vardır. Mahremiyetin azalmasının güvenliği artıracığı varsayılmaktadır. Bunun tersinin doğru olabileceğine dair ilk argümanları sağladık” dediği dönemden bu yana, dijital dünyada kişisel mahremiyet korumacılığının azalmasının daha fazla güvenlik açığı olarak geri döndüğü pek çok kere tecrübe edilmiştir.

Görüşmelerde birçok katılımcının aslında veri ihlaline dair kişisel bir tecrübe edinmediği görülmektedir, hatta birkaç katılımcı kendi deneyimleri sorulduğunda yakınlarının başından geçen bir olayı paylaşmışlardır. Kullanıcıların başkalarının yaşadığı tecrübelerle kanı sahibi olduğu görülmektedir. Buna sosyal medyada, haberlerde, sosyal ortamlarda duyulan olaylar da dahildir. Psikolojideki “paylaşılmış yaşam deneyimleri (shared life experiences) olarak adlandırılan bu gibi durumlarda kişi karşısındakinin olumsuz deneyimini empati yoluyla yaşamış ve anlayabilmiş gibi hissedebildiğini düşünür ancak araştırmalar göstermiştir ki bu gibi olumsuz deneyimler duyulduğunda beyin onu yaşamış gibi hissetmeye değil, baskılayıp görmezden gelmeye eğilimlidir (Israelashvili, Sauter ve Fischer, 2020). Katılımcıların ifadelerinde bu “görmezden gelme” durumu gözlemlenebilmektedir. Özellikle veri ihlali bizzat deneyimlememiş kullanıcıların mahremiyet endişesi bulunsu bile bu endişeler zayıftır.

Katılımcıların büyük oranda veri gizliliği riskleri karşısında bir önlem alma girişimi göstermemiş olması da mahremiyet risklerine karşı kabullenici ve boyun eğici bir davranış göstermiş olduklarını ortaya koymaktadır. Bu bulgular Sandra Petronio tarafından geliştirilen “İletişim Gizliliği Yönetimi Teorisi (Communication Privacy Management Theory)” ile çelişmektedir (Petronio, 1991). Teori, internet ve internet bağlantılı cihazları kullanan kişilerin bu mecralarda kişisel bilgilerini kontrol edebilme

gücüne sahip olduklarına inanma eğilimleri olduğunu iddia etmektedir (Petronio, 2019). Petronio'ya göre bireyler Petronio'nun "gizlilik sınırları (privacy boundaries)" olarak adlandırdığı, dijital ortamlarda sınırlarını kendilerinin belirledikleri özel alanları olduğunu düşünmektedirler (Petronio, 1991). Kişiler, bu alan içerisinde kişisel bilgilerini yönetebildiklerini ve bu bilgileri kimlerle paylaşacaklarını kontrol edebileceklerini düşünme eğilimindedir. Petronio'ya (1991) göre bu da bir yanılgıdır ancak günümüzde internet ve internet bağlantılı cihaz kullanıcılarının bu yanılgıya bile gerek kalmadan kişisel mahremiyetin yokluğunu kabul ettikleri görülmektedir. Görüşme katılımcılarının böyle bir özel alan hissiyatı yaşamadıkları, tam aksine SSA gibi mobil telefonlarda ve evlerde yer alan akıllı teknolojilerin yaygınlığının veri gizliliği adına kullanıcıya özel bir alan bırakmayacak şekilde etkili olduğunu düşündükleri sonucu ortaya çıkmaktadır. Görüşmecilerin ifadelerinde açık bir şekilde mahremiyet sınırlarının akıllı teknolojiler tarafından işgal edildiği düşüncesi hakimdir.

Bütün bu bulguların ışığında, dijital çağda mahremiyetin yok olduğu kabulünün önüne geçebilmek adına, bireysel mahremiyet ve veri gizliliği haklarına dair farkındalık sahibi olabilmek çok önemlidir. Katılımcıların İletişim Fakültesinde eğitim görmeleri faktörü göz önünde bulundurulduğunda, bilgisi olan öğrencilerin çoğunun bu bilgileri derslerden edindiğini söylemeleri beklenen bir bulgudur. Ancak yine de İletişim Fakültesi veya benzer sosyal bilimlere bağlı alanlarında öğrenci olmaksızın, mümkün olabildiğince her eğitim kurumunda, her yaştan ve kesimden internet ve IoT kullanıcılarına erişilebilecek online platformlarda, sosyal kuruluşlar, SSA geliştirici şirketler, eğitim kurumları ve hatta belediyelerce bu alanda çalışmalar yürütülmesi; eğitimler verilebilmesi dijital çağın bir gerekliliğidir. Dijital teknolojileri kullanan her birey bu alanda sahip olduğu yasal haklarını, hukuksal düzenlemeleri, kullandığı teknolojinin risklerini bilmesi gerekmektedir. Her bir akıllı cihaz farklı türde veri topluyor olabileceği gibi, kullanılan uygulamaların gizlilik politikalarına sık sık yeni güncellemeler gelmektedir. Bu gibi sebeplerle kullanıcıların verileri üzerindeki kontrolü ve açık rızası büyük önem kazanmaktadır. Her birey kişilik haklarının ve mahremiyetinin korunmasını koşulsuz ve doğuştan hak etmektedir ancak dijital çağın gerçeği, bilginin güç olduğudur. Çalışmanın en başında belirtildiği gibi mahremiyet bireyin kendini ve çevresinde olup bitenleri kontrol edebilme gücüdür. Bireyin yalnızca kendi istediği zamanlarda görünür olup kendi istediği zamanlarda anonim kalabilme hakkıdır. Kullanıcıların en temelde yapabilecekleri şey ise gizlilik politikalarını okumaktır. Bu bilgilendirme metinleri uzundur ve bu da elbette bir tür "politikadır".

Kullanıcıya tam anlamıyla güven vermeseler dahi, verilerin depolanması ve işlenmesi durumunda bunun hangi amaçlar doğrultusunda gerçekleştirileceğini bildirmenin yasal bir zorunluluk olduğu unutulmamalıdır. Böylece kullanıcı bu teknolojileri kullanırken kendisine sıradışı gelen ve kendini mağdur hissettiren durumlar yaşadığında bunu fark edebilecek, yargıya taşıyabilecek ve kullanıcı haklarını kullanabilmiş olacaktır.

Gizlilik politikaları kimi zaman ülkeden ülkeye farklılıklar gösterebilmektedir. Mahremiyetin ihlaline yol açabilecek her türlü veri güvenliği riskine karşı geliştirici şirketlerin aldığı önlemler, kullanıcısının vatandaşlığı ve ülkesindeki yasalardan bağımsız olarak eşit şekilde uygulanmalıdır. Bununla birlikte KVKK'da vurgulanan ve kişisel veriler işlenirken uygulanması yasal olarak zorunlu kabul edilmiş ilkelerin eksiksiz bir şekilde yerine getirilmesi çok büyük önem taşımaktadır. Mahremiyet ihlaline ilişkin her türlü tehdit göstermektedir ki, hassas verilerin bulunduğu tüm dijital ortamlar büyük bir dikkatle korunmalıdır. Bu verilere yetkili kişiler haricinde üçüncü kişilerin erişimi yasaklanmalıdır.

Uluslararası literatürde yaşlı yetişkinlerin (çoğunlukla 55-65 yaş ve üstü) SSA kullanımlarına ilişkin çalışmalar bulunmaktadır (Cowan, Neves ve Sayago, 2019; Pradhan, Lazar ve Findlater, 2020; Kim ve Choudhury, 2021). Bu çalışmanın örneklemini Y ve Z kuşağından öğrencilerle sınırlandırılmış olup, X kuşağı nispeten araştırma kapsamının dışında kalmıştır. X kuşağının mahremiyet algısı ve SSA kullanımları üzerine yapılacak bir çalışma da önemlidir. Bu çalışmada görüşülen katılımcı grubunun tümü SSA kullanıcılarından oluşmaktadır. Bu alanda yapılacak başka çalışmalarda SSA kullanıcısı olmayan, SSA kullanmayı tercih etmeyen kişilerle de görüşülerek bu kişilerin gerekçeleri, mahremiyet algıları ve SSA teknolojisine bakış açıları değerlendirilebilir.

KAYNAKÇA

- Abdi, N., Ramokapane M., Such J. M. (2019). More than Smart Speakers: Security and Privacy Perceptions of Smart Home Personal Assistants. Fifteenth Symposium on Usable Privacy and Security ({SOUPS}).
- Adams, C. (2021). Voice Assistants Don't Understand Us. They Should. <https://www.nytimes.com/2021/09/22/opinion/voice-assistants-accessibility-disability.html>
- Adobe Analytics (2019). State of Voice Technology for Brands. <https://www.slideshare.net/adobe/state-of-voice-technology-for-brands-145863065>
- Akıncı, A. N. (2019). Büyük Veri Uygulamalarında Kişisel Veri Mahremiyeti. (Uzmanlık Tezi). Sektörler ve Kamu Yatırımları Genel Müdürlüğü-Şubat 2019. <https://www.sbb.gov.tr/wp-content/uploads/2019/04/B%C3%Bcy%C3%Bck-Veri-Uygulamalar%C4%B1nda-Ki%C5%9Fisel-Veri-Mahremiyeti.pdf>
- Aktaş, C. (2007). Enformasyon Toplumu Bağlamında Türkiye. Selçuk İletişim, 4 (4), 181-193.
- Al Shamsi, J. H., Al-Emran, M., & Shaalan, K. (2022). Understanding key drivers affecting students' use of artificial intelligence-based voice assistants. Education and Information Technologies, s.1-21.
- All Things Digital Conference. (2010) <https://podcasts.apple.com/tr/podcast/steve-jobs-at-the-d-all-things-digital-conference-video/id529997900>
- Aloufi, R., Haddadi, H., & Boyle, D. (2019). Emotionless: Privacy-Preserving Speech Analysis for Voice Assistants. ArXiv, abs/1908.03632.
- Alptekin, G., Türkmen, D. ve Arslantaş, H. A. (2021). Baby boomers, x, y, z kuşaklarının sosyal medya kullanım düzeyleri ve tercihleri. Karadeniz Uluslararası Bilimsel Dergi, 1 (51), 253-278.
- Alston, M. (2020). "OK Google, I'm Feeling Really Down Today." <https://blog.myplanet.com/ok-google-im-feeling-really-down-today-e843c31120b4>
- Anders, D. (2021). Internet speed classifications: What is a good internet speed? <https://www.allconnect.com/blog/internet-speed-classifications-what-is-fast-internet>

- Andrew, O. (2018). The History and Evolution of the Smartphone: 1992-2018.
<https://www.textrequest.com/blog/history-evolution-smartphone/>
- Anyoha, R. (2017). Can Machines Think?
<http://sitn.hms.harvard.edu/flash/2017/history-artificial-intelligence/>
- Apple Privacy: <https://www.apple.com/legal/privacy/data/en/ask-siri-dictation/>
- Apple Support: iPhone’da Siri’ye sorma. <https://support.apple.com/tr-tr/guide/iphone/iph83aad8922/ios>
- Askım Kurt, A., Günüş, S., ve Ersoy, M. (2013). The current state of digitalization: Digital Native, Digital Immigrant and Digital Settler. Ankara University Journal of Faculty of Educational Sciences (JFES), 46 (1), 1-22.
- Asus (2021) Windows 10-Cortana nedir?
<https://www.asus.com/tr/support/FAQ/1014616/>
- Aydın, O., Baran G. (2010). Toplumsal Değişme Sürecinde Evlenme ve Boşanma Toplum ve Sosyal Hizmet Cilt 21, Sayı 2.
- Barber, N. (2015). Can Artificial Intelligence Make Us Stupid?
<https://www.psychologytoday.com/intl/blog/the-human-beast/201507/can-artificial-intelligence-make-us-stupid>
- Baruh L., Secinti E., Cemalcılar Z. (2017). Online Privacy Concerns and Privacy Management: A Meta-Analytical Review. Journal of Communication, Volume 67, Issue 1, February 2017, Pages 26–53.
- Bateman, R. (2021). Voice Assistants and Privacy Issues.
<https://www.termsfeed.com/blog/voice-assistants-privacy-issues/#:~:text=While%20voice%20assistant%20software%20providers,will%20require%20a%20Privacy%20Policy.>
- Bauman, Z., Lyon, D. (2013). Akışkan Gözetim. (E. Yılmaz, Çev.). İstanbul: Ayrıntı.
- Belk, R. W. (1988). Possessions and the Extended Self, Journal of Consumer Research, Volume 15, Issue 2, September 1988, Pages 139–168.
- Belk, R. W. (2013). Extended Self in a Digital World: Table 1. Journal of Consumer Research, 40(3), 477–500. doi:10.1086/671052
- Bennett, S., Maton, K., & Kervin, L. (2008). The “digital natives” debate: A critical review of the evidence. British Journal of Educational Technology, 39(5), 775–786.
- Berman, J. & Mulligan, D. (1999), “Privacy in the Digital Age: Work in Progress”, Nova Law Review, Vol. 23, No. 2.

- Berreby, D. (2017). Click to agree with what? No one reads terms of service, studies confirm. <https://www.theguardian.com/technology/2017/mar/03/terms-of-service-online-contracts-fine-print>
- Bilgiç, G. H., Duman, D. ve Seferoğlu, S. S. (2011). “Dijital Yerlilerin Özellikleri ve Çevrimiçi Ortamların Tasarlanmasındaki Etkileri”, İnönü Üniversitesi, Akademik Bilişim Konferansı Bildirileri, s. 257-263, İnönü Üniversitesi, Malatya.
- Boyd, D. ve Marwick, A. E. (2011). Social Privacy in Networked Publics: Teens’ Attitudes, Practices, and Strategies. A Decade in Internet Time: Symposium on the Dynamics of the Internet and Society.
- Boyd, D., Crawford, K. (2012). Critical questions for big data, Information, Communication & Society, 15:5, 662-679.
- Brill, T. M. (2015). Siri, Alexa, and Other Digital Assistants: A Study of Customer Satisfaction With Artificial Intelligence Applications. Electronic Dissertations & Teses. 1.
- Brown, J. S. (2000). Growing up digital: how the Web changes work, education, and the ways people learn. Change, March/April, 10–20.
- Canbek, G. N., Mutlu, M. (2016). Sayısal gelecekte yeni adım: akıllı kişisel yardımcılar. Açıköğretim Uygulamaları ve Araştırmaları Dergisi, 2 (1), 114-129.
- Castells, M., Cardoso G. (2005). The Network Society From Knowledge to Policy. Washington, DC: Johns Hopkins Center for Transatlantic Relations, 2005, ss.3-22.
- Chang, A. C. (2020). History of Artificial Intelligence. Intelligence-Based Medicine. Ss: 23–27. doi:10.1016/b978-0-12-823337-5.00002-0
- Chew, Y. J., Wong, K. S., Ooi, S. Y. (2018). Privacy protection in machine learning: The state-of-the-art for a private decision tree. In: Security and Authentication Editors: Ong Thian Song et al.
- Ching, C. C., Basham, J. D., ve Jang, E. (2005). The Legacy of the Digital Divide. Urban Education, 40(4), 394–411.
- Chivers, K. (2021). Digital generations: The technology gap between seniors, parents, and kids. <https://us.norton.com/internetsecurity-how-to-digital-generations.html>
- Cohen A., Graupe D. (1980). Speech recognition and control system for the severely disabled. Journal of Biomedical Engineering, Volume 2, Issue 2, Pages 97-107.
- Common Sense (2021). <https://privacy.commonsense.org/>

- Corden, J. (2017). A brief history of Cortana, Microsoft's trusty digital assistant. <https://www.windowscentral.com/history-cortana-microsofts-digital-assistant>
- Creighton, J. (2016). The Evolution of AI: Can Morality be Programmed? <https://futurism.com/the-evolution-of-ai-can-morality-be-programmed>
- Culkin, J. (1967). A schoolman's guide to Marshall McLuhan. *Saturday Review*, 51–53, 70–72.
- Dafoe, A. (2015). On Technological Determinism. *Science, Technology, & Human Values*, 40(6), 1047–1076.
- Dimock, M. (2019). Defining generations: Where Millennials end and Generation Z begins. <https://www.pewresearch.org/fact-tank/2019/01/17/where-millennials-end-and-generation-z-begins/>
- Dinler, E. ve Çalışkan, Z. (2019). Mülkiyetin tarihsel gelişimi üzerine bir deneme. *Sosyal Siyaset Konferansları Dergisi*, 77: 421-452.
- Duymaer van Twist, A. ve Newcombe, S., (2017) Strauss-Howe Generational Theory. In James Crossley and Alastair Lockhart (eds.) *Critical Dictionary of Apocalyptic and Millenarian Movements*.
- Easwara Moorthy A., Vu, K.L. (2014). Privacy Concerns for Use of Voice Activated Personal Assistant in the Public Space. *International Journal of Human-Computer Interaction* 31(4):307-335.
- Edu, J. S., Such, J. M., & Suarez-Tangil, G. (2021). Smart Home Personal Assistants. *ACM Computing Surveys*, 53(6), 1–36.
- Electronic Privacy Information Center (2022). Social Media Privacy. <https://epic.org/issues/consumer-privacy/social-media-privacy/>
- Emeç, A. S. (2019). CEYD-A Kullanıcılar Tarafından Da Geliştirilebiliyor. <https://turkiye.ai/ceyd-a-kullanicilar-tarafindan-da-gelistirilebiliyor/>
- Emre, İ. E. ve Erol Ç. S., (2017). “Veri Analizinde İstatistik mi Veri Madenciliği mi?”, *Bilişim Teknolojileri Dergisi*, 10(2), 161-167.
- Erdoğan, G. H. (2017). Bilgi Güvenliği, Kişisel Verilerin Korunması ve Biyometrik Verilerin İşlenmesine İlişkin Öneriler. (Yayımlanmış yüksek lisans tezi). İstanbul Teknik Üniversitesi Bilişim Enstitüsü.
- Eroğlu, Ş. (2018). Dijital Yaşamda Mahremiyet (Gizlilik) Kavramı ve Kişisel Veriler: Hacettepe Üniversitesi Bilgi ve Belge Yönetimi Bölümü Öğrencilerinin Mahremiyet ve Kişisel Veri Algılarının Analizi. *Hacettepe Üniversitesi Edebiyat Fakültesi Dergisi*, 35 (2), 130-153.

- Eşgi, N. (2013). Dijital Yerli Çocukların ve Dijital Göçmen Ebeveynlerinin İnternet Bağımlılığına İlişkin Algılarının Karşılaştırılması. Hacettepe Üniversitesi Eğitim Fakültesi Dergisi, 28 (28-3), 181-194.
- Eyüpoğlu, C, Aydın, M, Sertbaş, A, Zaim, A, Öneş, O. (2017). Büyük Veride Kişi Mahremiyetinin Korunması. Bilişim Teknolojileri Dergisi, 10 (2), 177-184.
- Federal Trade Commission (FTC) (2022): <https://consumer.ftc.gov/cfg-about-us>
- Ferenstein, G. (2015). The Birth And Death Of Privacy: 3,000 Years of History Told Through 46 Images. <https://medium.com/the-ferenstein-wire/the-birth-and-death-of-privacy-3-000-years-of-history-in-50-images-614c26059e>
- Forbes (2011). 5 Things People Buy Because Of Peer Pressure. <https://www.forbes.com/sites/investopedia/2011/11/16/5-things-people-buy-because-of-peer-pressure/?sh=58acff8a7ada>
- Forrest, C. (2018). Google Assistant gets multitasking skills and support for 30 languages. <https://www.techrepublic.com/article/google-assistant-gets-multitasking-skills-and-support-for-30-languages/>
- Fox, M. (2013). Alan F. Westin, Who Transformed Privacy Debate Before the Web Era, Dies at 83. <https://www.nytimes.com/2013/02/23/us/alan-f-westin-scholar-who-defined-right-to-privacy-dies-at-83.html>
- Freedman M. (2019). How Businesses Are Collecting Data (And What They're Doing With It) <https://www.businessnewsdaily.com/10625-businesses-collecting-data.html>
- Geambasu, R., Kohno T., Levy, A.A., Levy H.M. (2009). Vanish: Increasing Data Privacy with Self-Destructing Data. 18th USENIX Security Symposium. University of Washington.
- Gokhale, P., Bhat, O., Bhat, S. (2018). Introduction to IOT. International Advanced Research Journal in Science, Engineering and Technology.
- Gonsalves, T. (2018). The Summers and Winters of Artificial Intelligence. In M. Khosrow-Pour, D.B.A. (Eds.), Encyclopedia of Information Science and Technology, Fourth Edition (pp. 229-238). IGI Global. <http://doi:10.4018/978-1-5225-2255-3.ch021>
- Google Support: <https://support.google.com/assistant/?hl=en#topic=7546466>
- Google: Google Asistan, bilgilerinizi gizli ve güvende tutacak şekilde tasarlanmıştır. <https://safety.google/assistant/#:~:text=Choose%20a%20time%20limit%20for,aaccounthttps://safety.google/assistant/#:~:text=Choose%20a%20time%20limit%20for,account%20on%20an%20ongoing%20basis%20on%20an%20ongoing%20basis>

- Grustniy, L. (2019). Çaresi var: Çevrimiçi iz sürücülerden nasıl kurtulursunuz. <https://www.kaspersky.com.tr/blog/anti-tracking-tools/5896/>
- Guzman, A.L. (2017). Making AI safe for humans: A conversation with Siri. In R.W.Gehl & M. Bakardjieva (Eds.), *Socialbots and their friends: Digital media and the automation of sociality* (pp. 69-85). New York, NY: Routledge.
- Güzel, M. (2006). Küreselleşme, İnternet ve Gençlik Kültürü. *Küresel İletişim Dergisi*, 1(1), ss.1-16.
- Hall, C. (2022). What is Bixby? Samsung's smart assistant explained. <https://www.pocket-lint.com/phones/news/samsung/140128-what-is-bixby-samsungs-assistant-explained-and-how-to-use-it>
- Hall, P., Van Camp, J. (2021). The Best Smart Speakers With Alexa, Google Assistant, and Siri. <https://www.wired.com/story/best-smart-speakers/>
- Han, W., Zhang, H., Han, Y., & Duan, Z. (2020). Cognition-tracking-based strategies for diagnosis and treatment of minimal hepatic encephalopathy. *Metabolic Brain Disease*.
- Henley, J. (2013). Are teenagers really careless about online privacy?
- Herman, B. (2019). Gen Z and Privacy: They're Less Conflicted Than Other Generations.
- Hern, A. (2019). Apple contractors 'regularly hear confidential details' on Siri recordings. [https://www.theguardian.com/technology/2019/jul/26/apple-contractors-regularly-hear-confidential-details-on-siri-recordings](https://www.theguardian.com/technology/2019/jul/26/apple-contractors-regularly-hear-confidential-details-on-siri-recordings#:~:text=Apple%20contractors%20regularly%20hear%20confidential,assistant%20C%20the%20Guardian%20has%20learned.&text=Apple%20says%20the%20data%20confidential-details-on-siri-recordings#:~:text=Apple%20contractors%20regularly%20hear%20confidential,assistant%20C%20the%20Guardian%20has%20learned.&text=Apple%20says%20the%20data%20%E2%80%9Cis%20used%20to%20help%20Siri%20and%20dictation%20%E2%80%A6)
- Hoel and Chen (2018). *Research and Practice in Technology Enhanced Learning*.
- Holslin, P. (2021). Fastest Internet Providers 2022. [https://www.highspeedinternet.com/resources/fastest-internet-providers](https://www.highspeedinternet.com/resources/fastest-internet-providers#:~:text=Fiber%20is%20currently%20the%20fastest,and%20reliable%20over%20long%20distances)

- Holvast, J. (2009). History of Privacy. IFPI Advances in Information and Communication Technology, Vol. 298, pp.13-42.
- Hormby, T. (2013). The Story Behind Apple's Newton. <https://lowendmac.com/2013/the-story-behind-apples-newton/>
- Howe, N., ve Strauss, W. (1991). Generations: The History of America's Future, 1584 to 2069.
- Howe, N., ve Strauss, W. (1992). The new generation gap. ATLANTIC-BOSTON-, 270, 67-67.
- Hoy, M. B. (2018). Alexa, Siri, Cortana, and More: An Introduction to Voice Assistants. Medical Reference Services Quarterly, 37:1, 81-88.
<https://web.njit.edu/~ronkowit/eliza.html>
<https://www.bbc.com/future/article/20170214-the-machines-that-learned-to-listen>
<https://www.forbes.com/sites/cognitiveworld/2018/12/23/yes-chatbots-and-virtual-assistants-are-different/?sh=b1f5c836d7d2>
<https://www.itbusiness.ca/news/history-of-voice-recognition-from-audrey-to-siri/15008>
<https://www.storyblok.com/mp/best-use-cases-for-voice-technology>
<https://www.yapayzekatr.com/2019/04/30/akilli-asistan-sanal-asistan-nedir/>
- Hunt, V. D. (1986). Introduction to Artificial Intelligence and Expert Systems. Artificial Intelligence & Expert Systems Sourcebook, 1–39. doi:10.1007/978-1-4613-2261-0_1.
- Hurme, P. ve Jouhki, J. (2017). We shape our tools, and thereafter our tools shape us. Human Technology 13, 2: 145–148.
- IAPP: <https://iapp.org/about/what-is-privacy/Infosecurity> (2014). The Ponemon Institute: Most Organizations are Woefully Behind in Application Security. <https://www.infosecurity-magazine.com/news/the-ponemon-institute-most-organizations-are/>
- IBM (2020). Yapay zekâ. <https://www.ibm.com/tr-tr/cloud/learn/what-is-artificial-intelligence>.
- Ismail, K. (2021). The best use cases for voice technology.

- Israelashvili J., Sauter D. A., Fischer A. H. (2020). Different faces of empathy: Feelings of similarity disrupt recognition of negative emotions, *Journal of Experimental Social Psychology*, Volume 87, 103912.
- ITU (2021). Facts and Figures 2021: 2.9 billion people still offline. <https://www.itu.int/hub/2021/11/facts-and-figures-2021-2-9-billion-people-still-offline/>
- İçöz, T. (2020). Covid-19 etkisiyle chatbot kullanımı bankacılıkta 5 kat, e-ticarette 2 kat arttı. <https://webrazzi.com/2020/05/20/pandemi-etkisiyle-chatbot-kullanimi-bankacilikta-5-kat-e-ticarette-2-kat-artti/>
- İsmayılzade, L. (2017). Sanal Dünyada Sanal Dönüşüm. *Yeni Medya Elektronik Dergisi*, 1(3), 227-236.
- Jagadish, H.V. (2016). Data Science Ethics (History of Privacy), University of Michigan. <https://www.coursera.org/lecture/data-science-ethics/history-of-privacy-7e36E>
- Johnson D. G. (2021). Social Construction of Technology. *Encyclopedia of Science, Technology, and Ethics*.
- Joshi, N. (2018). Yes, Chatbots And Virtual Assistants Are Different!
- Kakırman Yıldız, A. (2012). Dijital Yerliler Gerçekten Yerli Mi Yoksa Dijital Melez Mi? .*The Journal of Academic Social Science Studies*.
- Karataş, Z. (2015). Sosyal Bilimlerde Nitel Araştırma Yöntemleri. *Manevi Temelli Sosyal Hizmet Araştırmaları Dergisi*, 1(1), 62-80.
- Kart, A. & Ketizmen, M. (2019). Kabahatler Kanunu'nun İctima Hükümleri Açısından Kişisel Verilerin Korunmasına İlişkin Suç ve Kabahatler ile Kurul'un İdari Ceza Kararlarına İlişkin Bir Değerlendirme. *Kişisel Verileri K. Dergisi*, 1 (2), 17-29.
- Kennedy, G., Krause, K., Judd, T., Churchward, A. & Gray, K. (2006). First year students' experiences with technology: are they really digital natives? Melbourne, Australia: University of Melbourne.
- Kim, S., & Choudhury, A. (2021). Exploring older adults' perception and use of smart speaker-based voice assistants: A longitudinal study. *Computers in Human Behavior*, 124, 106914.
- Klie, L. (2014). Neural Networks Reach into Virtual Assistants. Erişim Tarihi: 23 Aralık 2021. <https://www.destinationcrm.com/Articles/CRM-Insights/Insight/Neural-Networks-Reach-into-Virtual-Assistants-98749.aspx>

- Kline, R. (2011). Cybernetics, Automata Studies, and the Dartmouth Conference on Artificial Intelligence. *IEEE Annals of the History of Computing*, 33(4), 5–16. doi:10.1109/mahc.2010.44
- Kline, R. R. (2015). Technological Determinism. *International Encyclopedia of the Social & Behavioral Sciences*, 109–112.
- Knight, Y. (2009) Talkin’ ‘bout my generation: a brief introduction to generational theory, *Planet*, 21:1, 13-15.
- Knopp, C. (2019). Privacy Perception in Developing Countries. *Advanced Topics in Computer Security and Privacy*, Georg-August-University Gottingen, Germany.
- Koch, M. (2019). The Three Ps of Gen X Tech Use: Plugged In, (Social) Platforms and Privacy. <https://www.emarketer.com/content/the-three-p-s-of-gen-x-penetration-social-platforms-and-privacy>
- Koç Y. (2017). Sosyal Bilimlerde Örnekleme Kuramı. *Akademik Sosyal Araştırmalar Dergisi*, Yıl: 5, Sayı: 47, Haziran 2017, s. 480-495.
- Koene, A. (2016). Never read the terms and conditions? Here’s an idea that might protect your online privacy. <https://theconversation.com/never-read-the-terms-and-conditions-heres-an-idea-that-might-protect-your-online-privacy-62208>
- Koetsier, J. (2018). This AI Can Recognize Anger, Awe, Desire, Fear, Hate, Grief, Love By How You Touch Your Phone. <https://www.forbes.com/sites/johnkoetsier/2018/08/31/new-tech-could-help-siri-google-assistant-read-our-emotions-through-touch-screens/?sh=7d8173212132>
- Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & security*, 64, 122-134.
- Kondrats, J. (2018). Emotionally intelligent voice assistants, chatbots and the future. <https://www.linkedin.com/pulse/emotionally-intelligent-voice-assistants-chatbots-future-kondrats>
- Krakovsky, M. (2018). Artificial (emotional) intelligence. *Communications of the ACM*, 61(4), 1819.
- Kuckartz, U., Radiker, S. (2019). *Analyzing Qualitative Data with MAXQDA*. Cham: Springer.
- Kulshreshtha, N. (2020). How Does Voice Recognition Work: Secret Behind Your Voice Assistants. <https://fireflies.ai/blog/how-does-voice-recognition-work>

- Kurt, A., Günüş, S. & Ersoy, M. (2013). Dijitalleşmede son durum: Dijital yerli, dijital göçmen ve dijital göçebe. Ankara Üniversitesi Eğitim Bilimleri Fakültesi Dergisi, 46(1) 1–22.
- Kurtishi, R. (2018). Universal Design of Intelligent Personal Assistants. (Master Thesis) Department of Computer Science Faculty of Technology, Art and Design, Norway.
- Kümbetoğlu, B. (2012). Sosyolojide ve antropolojide niteliksel yöntem ve araştırma. (3. Basım). Ankara: Bağlam Yayıncılık
- Küzeci, E. (2010). Anayasal bir hak: Kişisel Verilerin Korunması. 2010 Bilişim Kurultayı
- KVKK, Kişisel Verilerin Korunması Kanunu, Kanun Numarası: 6698, Resmî Gazete Tarihi: 07.04.2016 Resmî Gazete Sayısı: 29677, Tertip: 5, Cilt: 57 <https://www.kvkk.gov.tr/Icerik/4186/6698-Sayili-Kanunda-Yer-Alan-Terimler>
- Laricchia, F. (2022). Number of digital voice assistants in use worldwide 2019-2024. <https://www.statista.com/statistics/973815/worldwide-digital-voice-assistant-in-use/>
<https://www.statista.com/statistics/973815/worldwide-digital-voice-assistant-in-use/>
 :~:text=In%202020%2C%20there%20will%20be,higher%20than%20the%20wo
 rld#:~:text=In%202020%2C%20there%20will%20be,higher%20than%20the%2
 0world'%20population.
- Laufer, R. S., Wolfe, M. (1977). Privacy as a concept and a social issue: A multidimensional developmental theory. Journal of Social Issues, 33(3), 22–42.
- Lavagnino, M. B. (2013). Information Privacy Revealed. <https://er.educause.edu/articles/2013/1/information-privacy-revealed>
- Liyanaarachchi, G. (2021). Managing privacy paradox through national culture: Reshaping online retailing strategy. Journal of Retailing and Consumer Services, 60, 102500.
- Long, W. RM., Raul, A. C., Blythe, F., Kara, D. (2021). The Privacy, Data Protection and Cybersecurity Law Review: EU Overview. <https://thelawreviews.co.uk/title/the-privacy-data-protection-and-cybersecurity-law-review/eu-overview>
- Lopatovska, I. (2019). Overview of the Intelligent Personal Assistants. Ukrainian Journal on Library and Information Science. Issue 3.

- LoupVentures. (2019). Smart Speaker Macro-Model Update. Retrieved from LoupVentures: <https://loupventures.com/smart-speaker-market-share-update/>
- Lowerre, B.T., Reddy, R. (1976). The HARP speech recognition system. Ph.D. Thesis Carnegie-Mellon Univ., Pittsburgh, PA. Dept. Of Computer Science.
- Lyon, D. (2013). Akışkan Gözetim. (E. Yılmaz, Çev.). İstanbul: Ayrıntı.
- Mannheim K. (1952). The Problem of Generations. Oxford University Press, Inc. *Psychoanalytic Review*, 57(3):378-404
- Martinez, D. (2021). Gen Z and the Data Security Paradox. <https://insights.viacomcbs.com/post/gen-z-and-the-data-security-paradox/>
- Mboyo, J.P. (2019). Reimagining Ubuntu in schools: A perspective from two primary school leaders in the Democratic Republic of Congo. *Educational Management Administration & Leadership*, 47, 206-223.
- McMillan, R. (2013). Apple Finally Reveals How Long Siri Keeps Your Data. <https://www.wired.com/2013/04/siri-two-years/>
- Medeiros, J. (2018). Voice Assistants are Changing How Users with Disabilities Get Things Done. <https://www.modev.com/blog/voice-assistants-are-changing-how-users-with-disabilities-get-things-done>
- Microsoft (2021). Azure Machine Learning'de derin öğrenme ve makine öğrenmesi karşılaştırması. <https://docs.microsoft.com/tr-tr/azure/machine-learning/concept-deep-learning-vs-machine-learning>
- Microsoft Support: <https://support.microsoft.com/en-us/topic/what-is-cortana-953e648d-5668-e017-1341-7f26f7d0f825>
- Mills, J. L., Harclerode, K. (2018). Privacy, Mass Intrusion and the Modern Data Breach, 69 Fla. L. Rev. 771.
- Mills, J. L. (2009). Privacy: The Lost Right. Published to Oxford Scholarship Online: January.
- Mooney, S. J., Pejaver, V. (2018), Big Data in Public Health: Terminology, Machine Learning, and Privacy, *Annual Review of Public Health*, 39, 95–112.
- Moskvitch, K. (2017). Voice recognition technology makes many aspects of modern life easier. The seeds were sown a lot further back than you might think.
- Nichinson D. (2020). The Smart Assistant Privacy-Performance Tradeoff. Leonard N. Stern School of Business, New York University, USA.

- Olinger N., Britz J.J., Olivier M.S. (2007). Western privacy and/or Ubuntu? Some critical comments on the influences in the forthcoming on Social Network Sites. In *Trust and Trustworthy Computing*, Berlin and Heidelberg: Springer, 2011, pp. 146–153.
- Öncü, G. A. (2019). Özel Yaşama ve Aile Yaşamına Saygı Hakkı Anayasa Mahkemesine Bireysel Başvuru El Kitapları Serisi – 8. Avrupa Konseyi Ankara Program Ofisi, Ankara.
- Park, J., Vance, A. (2021). Data Privacy in Higher Education: Yes, Students Care.
- Parker, K., & Igielnik, R. (2020, May 15). What we know about Gen Z so far. Pew Research Center's Social & Demographic Trends Project. <https://www.pewsocialtrends.org/essay/on-the-cusp-of-adulthood-and-facing-an-uncertain-future-what-we-know-about-gen-z-so-far/>
- Pasquier, T., Singh, J., Powles, J. et al. (2017). Data provenance to audit compliance with privacy policy in the Internet of Things. *Pers Ubiquit Comput* 22, 333–344 (2018).
- Pasztor, J., Bak, G. (2021). Digital Divide - A Technological Generation Gap. MEB-18th International Conference on Management, Enterprise, Benchmarking. Proceedings (MEB 2020) (pp.158-168).
- Patil, J., Shewale, A., Bhushan E., Fernandes A., Khartadkar R. (2021). A Voice Based Assistant Using Google Dialog flow and Machine Learning. *International Journal of Scientific Research in Science and Technology (IJSRST)*, Online ISSN :2395-602X, Print ISSN: 2395-6011, Volume 8 Issue 3, pp. 06-17, May-June 2021.
- Paw Research (2020). 18 statistics to explain The Rise of Voice Assistants. (Aynla, R.). <https://medium.com/the-open-manuel/18-statistics-to-explain-the-rise-of-voice-assistants-bdc8a71c07ab>
- Pehlivan, B. (2019). Akıllı asistan (Sanal Asistan) nedir?
- Petronio, S. (1991). Communication Boundary Management: A Theoretical Model of Managing Disclosure of Private Information Between Marital Couples. *Communication Theory*, 1(4), 311–335.
- Petronio, S., & Child, J. T. (2019). Conceptualization and Operationalization: Utility of Communication Privacy Management Theory. *Current Opinion in Psychology*.

- Pew Research Center (2019). Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information. <https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/>
- Pinola, M. (2011). History of voice recognition: from Audrey to Siri.
- Poibeau, T. (2017). The 1966 ALPAC Report and Its Consequences. in *Machine Translation*, MIT Press, 2017, pp.75-89.
- Poushneh, A. (2021). Humanizing voice assistant: The impact of voice assistant personality on consumers' attitudes and behaviors. *Journal of Retailing and Consumer Services*, 58, 102283.
- Pradhan, A., Lazar, A., & Findlater, L. (2020). Use of Intelligent Voice Assistants by Older Adults with Low Technology Use. *ACM Transactions on Computer-Human Interaction*, 27(4), 1– 27. doi:10.1145/3373759
- Prensky, M. (2001). Digital Natives, Digital Immigrants. *From On the Horizon* (MCB University Press, Vol. 9 No. 5, October.
- Rachels, J. (1975). Why privacy is important. *Philosophy & Public Affairs*, 323-333.
- Ramos, D. (2018). Voice Assistants: How Artificial Intelligence Assistants Are Changing Our Lives Every Day. <https://www.smartsheet.com/voice-assistants-artificial-intelligence>
- Richterich, A. (2018). *The Big Data Agenda: Data Ethics and Critical Data Studies*. Pp. 15–31. London: University of Westminster Press.
- Rollenhagen, L. (2021). Alan Westin is the father of modern data privacy law. <https://www.osano.com/articles/alan-westin>
- Romansky, R. (2017). A survey of digital world opportunities and challenges for user's privacy, *Int. J. Inform. Technol. Secur.*, 9, 97-112.
- Ronkowitz, K. (2017). ELIZA: a very basic Rogerian psychotherapist chatbot.
- Ryder, N. B. (1965). The Cohort as a Concept in the Study of Social Change. *American Sociological Review*, 30(6), 843–861.
- Salesforce (2018). Trends in Customer Trust https://c1.sfdcstatic.com/content/dam/web/en_us/www/documents/briefs/customer-trust-trends-salesforce-research.pdf
- Salesforce (2019) *State of the Connected Customer Report Outlines Changing Standards for Customer Engagement*. <https://www.salesforce.com/company/news-press/stories/2019/06/061219-g/>

- Sayago, S., Neves, B. B., & Cowan, B. R. (2019). Voice assistants and older people. Proceedings of the 1st International Conference on Conversational User Interfaces- CUI'19.
- Schuchmann, S. (2019). Analyzing the Prospect of an Approaching AI Winter. Master's.
- Shanbhag, A. (2020). Understanding The Difference Between A Chatbot And A Virtual Assistant. <https://botcore.ai/blog/chatbot-vs-virtual-assistants/>
- Shariff, A., Green, J., & Jettinghoff, W. (2021). The Privacy Mismatch: Evolved Intuitions in a Digital World. *Current Directions in Psychological Science*, 30(2), 159–166.
- Siri Team (2017). Hey Siri: An On-device DNN-powered Voice Trigger for Apple's Personal Assistant. <https://machinelearning.apple.com/research/hey-siri>
- Smartsheet. (2020). Voice Assistants: How Artificial Intelligence Assistants Are Changing Our Lives Every Day. <https://www.smartsheet.com/voice-assistants-artificial-intelligence>
- Solove, D. J. (2007). 'I've Got Nothing to Hide' and Other Misunderstandings of Privacy. *San Diego Law Review* 44: 745.
- Solove, D. J. (2008). *Understanding privacy*. Harvard University Press.
- Solove, D.J. (2006). A Brief History of Information Privacy Law. In Proskauer on Privacy.
- Srikanth, A. (2020). Virtual assistants vs Chatbots: What's the Difference & How to Choose the Right One? <https://freshdesk.com/customer-engagement/virtual-assistant-chatbot-blog/>
- Statista (2021). Global digital population as of January 2021. <https://www.statista.com/statistics/617136/digital-population-worldwide/>
- Statista Reseach Department, (2022). Number of voice assistant users in the United States from 2017 to 2022(in millions) <https://www.statista.com/statistics/1029573/us-voice-assistant-users/>
- Statista. (2020). Number of digital voice assistants in use worldwide from 2019 to 2024 (in billions) <https://www.statista.com/statistics/973815/worldwide-digital-voice-assistant-in-use/>
- Steele, C. (2021). Personal digital assistant (PDA). <https://searchmobilecomputing.techtarget.com/definition/personal-digital-assistant>

- Steeves, V., (2014). Young people online and the social value of privacy. *Journal of Information, Communication and Ethics in Society*, Vol. 12 Iss 4 pp. 298 – 313.
- Stengel, S. (2016). Newton MessagePad – 1993. <http://oldcomputers.net/apple-newton.html>
- Stepanova, O., Jechel P. (2021). The Privacy, Data Protection and Cybersecurity Law Review.
- Strauss, A. ve Corbin J. (1990). Basics of qualitative research: Grounded theory procedures and techniques. Newbury Park, CA: Sage.
- Strawn, G. (2014). Alan Turing. *IT Professional*, 16(1), 5–7. doi:10.1109/mitp.2014.2
- Sunumu, Bahçeşehir Üniversitesi Hukuk Fakültesi.
- Syverson, P. (2003). The Paradoxical Value of Privacy. Proceedings of the 2nd Annual Workshop on Economics and Information Security, May 29-30, University of Maryland, College Park, MD, USA.
- Taba, T. (2019). Personalized AI Assistant. (Thesis). Metropolia University of Applied Sciences, Finland.
- Tableau (2019). Staying cyber-secure while working from home. <https://public.tableau.com/ko-kr/gallery/staying-cyber-secure-while-working-home>
- Tapscott, D. (2008). Growing up digital: the rise of the Net generation. New York: McGraw-Hill.
- Tataroğlu, M. (2013). Mahremiyet Sorunlarının Önlenmesinde Mahremiyet Etki Değerlendirmesi (MED). *Yönetim ve Ekonomi: Celal Bayar Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*, 20(1), 263-289.
- TELUS International (2021). OK Google, how do voice assistants work? <https://www.telusinternational.com/articles/ok-google-how-does-alexa-work-voice-assistants-explained>
- Terzopoulos, G., Satratzemi, M. (2019). Voice Assistants and Artificial Intelligence in Education. BCI'19: Proceedings of the 9th Balkan Conference on Informatics. September 2019. Pages 1–6.
- The Smart Audio Report (2020). <https://www.nationalpublicmedia.com/insights/reports/smart-audio-report/>
- Thomson, R., Yuki, M., & Ito, N. (2015). A socio-ecological approach to national differences in online privacy concern: The role of relational mobility and trust., 51, p. 285-292.

- Tillman, M. (2021). What is Google Assistant and what can it do? <https://www.pocket-lint.com/apps/news/google/137722-what-is-google-assistant-how-does-it-work-and-which-devices-offer-it>
- Titlow, J. P. (2016). Siri and other voice assistants are leaving disabled users behind. <https://www.fastcompany.com/4008689/siri-and-other-voice-assistants-are-leaving-disabled-users-behind>
- Toplumsal Bilgi ve İletişim Derneği (TBİD) (2018). Avrupa Genel Veri Koruma Yönetmeliği (GDPR) Yürürlüğe Girdi. <https://www.tbid.org.tr/blog-tr/avrupa-genel-veri-koruma-yonetmeli-gdpr-yururluge-girdi/>
- Troksa, L.M. (2016). The Study of Generations: A Timeless Notion within a Contemporary Context.
- Tulshan, A. S., Dhage, S. N. (2019). Survey on Virtual Assistant: Google Assistant, Siri, Cortana, Alexa. *Advances in Signal Processing and Intelligent Recognition Systems*, 190–201. doi:10.1007/978-981-13-5758-9_17
- Turing, A. M. (1950). Computing Machinery and Intelligence. *Mind, New Series*, Vol. 59, No. 236 (Oct., 1950), pp. 433-460.
- Van Dijk, J. (2016). Ağ Toplumu. (Ö. Sakin, Çev.). İstanbul: Kafka.
- Varol, M., ve Varol, E. (2019). Kavram ve Kuramlarıyla Marshall McLuhan’a Bakış: Günümüzün Egemen Medya Araçları Ekseninde Bir Değerlendirme.
- ViaDialog (2021). Detection of human emotions by voice assistants: an industrial challenge. <https://viadialog.com/en/detection-emotions-assistants-vocaux/>
- Vyver, C., McDonald P. (2018). Improving Cyber Security Awareness among Generation X. Conference: 32nd IBIMA ConferenceAt: Seville, Spain.
- Walczak, S. (2018). Artificial Intelligence. In M. Khosrow-Pour, D.B.A. (Eds.), *Encyclopedia of Information Science and Technology*, Fourth Edition (pp.98-105).
- Wang, Q., Myers, M. D., & Sundaram, D. (2013). Digital Natives und Digital Immigrants. *Wirtschaftsinformatik*, 55(6), 409–420.
- Warren, S., Brandeis L. (1890). The Right to Privacy. *Harvard Law Review*, Vol. 4, No. 5. (Dec. 15, 1890), pp. 193-220.
- Warren, T. (2014). The story of Cortana, Microsoft's Siri killer. <https://www.theverge.com/2014/4/2/5570866/cortana-windows-phone-8-1-digital-assistant>

- Weaver, S. D., & Gahegan, M. (2007). Constructing, visualizing, and analyzing: A digital footprint. *Geographical Review*, 97(3), 324-350.
- Westin, A.F. (1967). *Privacy and Freedom*. New York: Atheneum.
- Westin, A.F. (1972). Data Banks in a Free Society. Records, Computers and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems, 24 Buff. L. Rev. 331.
- Wiggers, K. (2018a). Which voice assistant speaks the most languages, and why? <https://venturebeat.com/2019/02/02/which-voice-assistant-https://venturebeat.com/2019/02/02/which-voice-assistant-speaks-the-most-languages-and-speaks-the-most-languages-and-why/>
- Wiggers, K. (2018b). Samsung's Bixby assistant: 10 things worth trying. <https://venturebeat.com/2018/12/24/samsungs-bixby-assistant-10-things-worth-trying/>
- Wiggins III, R. H. (2004). Personal Digital Assistants. *Journal of Digital Imaging*, 17(1), 5-17.
- Wyatt, S. (2008). Technological determinism is dead; Long live technological determinism. *Science and technology studies*, 7, 165-180.
- Yıldırım A. ve Şimşek H. (2003). Sosyal bilimlerde nitel araştırma yöntemleri. Ankara: Seçkin.
- Yılmaz A., Özkoçak, L. (2010). Perception of Social Media in the Generations X, Y and Baby Boomers. Indonesia International Conference on Communication (IICC).
- Yoffie, David B., Wu, L., Sweitzer, J., Eden D., Ahuja, K. (2018). Voice War: Hey Google vs. Alexa vs. Siri. Harvard Business School Case 718-519, June 2018.
- 5237 sayılı Türk Ceza Kanunu. <https://www.mevzuat.gov.tr/mevzuatmetin/1.5.5237.pdf>