T.C.
SELÇUK ÜNİVERSİTESİ
SAĞLIK BİLİMLERİ ENSTİTÜSÜ

KİŞİSEL SAĞLIK VERİLERİ PAYLAŞMA NİYETİ İLE GİZLİLİK ENDİŞESİ VE ALGILANAN KONTROL ARASINDAKİ İLİŞKİDE ALGILANAN RİSK VE ALGILANAN FAYDANIN ARACI ROLÜ

HAVVA NUR ATALAY

YÜKSEK LİSANS TEZİ

SAĞLIK YÖNETİMİ ANABİLİM DALI

Danışman
Prof. Dr. Şebnem ASLAN

KONYA, 2022

T.C.
SELÇUK ÜNİVERSİTESİ
SAĞLIK BİLİMLERİ ENSTİTÜSÜ

KİŞİSEL SAĞLIK VERİLERİ PAYLAŞMA NİYETİ İLE GİZLİLİK ENDİŞESİ VE ALGILANAN KONTROL ARASINDAKİ İLİŞKİDE ALGILANAN RİSK VE ALGILANAN FAYDANIN ARACI ROLÜ

HAVVA NUR ATALAY

YÜKSEK LİSANS TEZİ

SAĞLIK YÖNETİMİ ANABİLİM DALI

Danışman
Prof. Dr. Şebnem ASLAN

KONYA,2022

ÖNSÖZ

Yüksek lisans eğitimim boyunca gerek ders döneminde gerekse tez döneminde beni bilimsel etik değerler doğrultusunda yönlendiren, bilgisini, zamanını ve sevgisini asla esirgemeyen ve bana her anlamda destek olan danışmanım Prof. Dr. Şebnem ASLAN'a,

Eğitim hayatımın her aşamasında olduğu gibi çalışma boyunca yanımda olan, maddi ve manevi desteklerini hiç esirgemeyen, sonsuz saygı ve minnet duyduğum babam Abdullah ATALAY'a, annem Kadriye ATALAY'a, ablam Ayşegül ATALAY'a ve kardeşim Mehmet ATALAY'a,

Çalışma boyunca varlıkları ile bana güç veren ve veri toplama aşamasında büyük katkı sağlayan Av. Nurdan CEYLAN'a, Hemşire Melike ÖZTÜRK'e, Cool Caliper CEO'su Hasan ULUDAĞ'a ve anketimi içtenlikle cevaplayan tüm katılımcılara

Teşekkkür ederim.

HAVVA NUR ATALAY

İÇİNDEKİLER

SİMGELER VE KISALTMALAR ..... Vİİİ

ÖZET ..... İX

SUMMARY X

1. GİRİŞ 1

1.1. Kişisel Veri ve Kişisel Sağlık Verisi Kavramları 3

1.1.1. Kişisel Veri Tanımı ve Kapsamı 3

1.1.2. Kişisel Veriler ile İlgili Uluslararası Düzenlemeler 5

1.1.3. Kişisel Veriler ile İlgili Ulusal Düzenlemeler 8

1.1.4. Kişisel Sağlık Verisi Tanımı ve Kapsamı 12

1.1.5. Kişisel Sağlık Verilerinin Önemi 14

1.2. Gizlilik Endişesi 16

1.2.1. Gizlilik, Bilgi Gizliliği ve Gizlilik Endişesi Kavramları 16

1.2.2. Gizlilik Endişesinin Ölçülebilirliği 17

1.2.3. Kişisel Sağlık Verileri ve Gizlilik Endişesi 18

1.3. Algılanan Kontrol 20

1.3.1. Kontrol ve Algılanan Kontrol Kavramları 20

1.3.2. Kişisel Sağlık Verileri ve Algılanan Kontrol 22

1.4. Algılanan Risk ve Algılanan Fayda 24

1.4.1. Algılanan Risk ve Algılanan Fayda Kavramları 24

1.4.2. Algılanan Risk Türleri 26

1.4.3. Gizlilik Hesabı Teorisi 29

1.4.4. Kişisel Sağlık Verileri, Algılanan Risk ve Algılanan Fayda 30

1.5. Veri Paylaşma Niyeti 32

1.5.1. Niyet ve Veri Paylaşma Niyeti 32

1.5.2. Kişisel Sağlık Verileri ve Veri Paylaşma Niyeti 33

2. GEREÇ VE YÖNTEM 35

2.1. Araştırmanın Amacı 35

2.2. Araştırmanın Önemi 35

2.3. Araştırmanın Türü 35

2.4. Araştırmada Kullanılan Ölçekler 36

2.4.1. Gizlilik Endişesi Ölçeği 36

2.4.2. Algılanan Kontrol Ölçeği 36

2.4.3. Algılanan Risk Ölçeği 37

2.4.4. Algılanan Fayda Ölçeği 37

2.4.5. Veri Paylaşma Niyeti Ölçeği 37

2.5. Araştırmanın Evreni ve Örneklemi 37

2.6. Araştırmanın Modeli 39

2.7. Araştırmanın Sınırlılıkları 39

2.8. Araştırma Verilerinin Toplanması 39

2.9. Araştırma Verilerinin Değerlendirilmesi 39

2.10. Araştırma Etiği 40

2.11. Araştırmanın Soruları ve Hipotezleri 40

3. BULGULAR 42

3.1. Katılımcılara Ait Tanımlayıcı-Betimleyici İstatistikler 42

3.2. Ölçek Maddelerine Ait Tanımlayıcı İstatistikler 46

3.3. Normal Dağılım Analizi 48

3.4. Ölçeklerin Geçerlik ve Güvenirliğine Ait Bulgular 48

3.4.1. Doğrulayıcı Faktör Analizi Sonuçları 50

3.4.2. Korelasyon Analizi Sonuçları 52

3.4.3. Yapısal Eşitlik Modeli 53

3.4.4. Hipotez Yorumları 56

4. TARTIŞMA 57

5. SONUÇ VE ÖNERİLER 59

5.1. Sosyo-demografik Verilere İlişkin Sonuçlar 59

5.2. Araştırmanın Hipotezlerine Ait Sonuçlar 59

5.3. Öneriler 61

6. KAYNAKLAR 62

7. EKLER 73

EK-A: Anket Formu 73

EK-A: Anket Formu (Devam) 74

EK-A: Anket Formu (Devam) 75

8. TURNİTİN RAPORU 76

ÇİZELGELER

Çizelge 2.1. Örneklem büyüklüğü belirleme. 38
Çizelge 3.1. Katılımcılara ait tanımlayıcı veriler. 42
Çizelge 3.2. Katılımcılara ait betimleyici istatistikler. 44
Çizelge 3.3. Modele ait doğrulayıcı faktör analizi sonuçları. 50
Çizelge 3.4. Korelasyon analizi. 52

ŞEKİLLER

Şekil 1.1. Kişisel sağlık verileri ile ilgili uluslararası düzenlemeler. 6
Şekil 1.2. Kişisel sağlık verileri ile ilgili ulusal düzenlemeler. 9
Şekil 1.3. Kişisel sağlık verilerinin paylaşıldığı kurumlar ve sebepleri. 15
Şekil 1.4. Kontrol duygusunun öncülleri ve sonuçları. 23
Şekil 1.5. Güvenlik açığının ve risk algısının bileşenleri. 25
Şekil 2.1. Araştırmanın modeli. 39
Şekil 3.1. Doğrulayıcı faktör analizi modeli. 51
Şekil 3.2. Gizlilik endişesi ve veri paylaşma niyeti ilişkisine yönelik yol analizi ilk aşama. 53
Şekil 3.3. Algılanan kontrol ve veri paylaşma niyeti ilişkisine yönelik yol analizi ilk aşama. 53
Şekil 3.4. Gizlilik endişesi ve algılanan kontrol ile veri paylaşma niyeti arasındaki ilişkide algılanan fayda ve algılanan riskin aracı rolünü incelemeye ilişkin yol (path) analizi sonuç modeli. 54
Şekil 3.5. Oluşturulan yeni yol modeli 55

SİMGELER VE KISALTMALAR

AB	Avrupa Birliği
BM	Birleşmiş Milletler
CFIP	Bilgi Gizliliği Endişesi Ölçeği
GDPR	Genel Veri Koruma Tüzüğü
HIPC	Sağlık Bilgileri Gizliliği Endişesi Ölçeği
IUIPC	Bilgi Gizliliği Endişesi Ölçeği
KVKK	Kişisek Verileri Koruma Kanunu
md.	Madde
N	Örneklem Sayısı
SS	Standart Sapma
TCK	Türk Ceza Kanunu
TMK	Türk Medeni Kanunu
$\bar{x}$	Ortalama

ÖZET

T.C.
SELÇUK ÜNİVERSİTESİ
SAĞLIK BİLİMLERİ ENSTİTÜSÜ

Kişisel Sağlık Verileri Paylaşma Niyeti ile Gizlilik Endişesi ve Algılanan Kontrol Arasındaki İlişkide Algılanan Risk ve Algılanan Faydanın Aracı Rolü

Havva Nur ATALAY

Sağlık Yönetimi Anabilim Dalı

YÜKSEK LİSANS TEZİ / KONYA-2022

Çalışma, bireylerin kişisel sağlık verileri paylaşma niyeti ile gizlilik endişesi ve algılanan kontrol arasındaki ilişkide algılanan risk ve algılanan faydanın aracılık rollerinin olup olmadığını araştırmak amacıyla yapılmıştır.

Çalışmanın evrenini Türkiye'nin İzmir, Konya ve Adana illerinde yaşamakta olan bireyler oluşturmaktadır. Örneklem büyüklüğü 600 olarak belirlenmiştir. Çalışmaya hangi ilden en az kaç kişinin katılması gerektiğini belirlemek için tabakalı örnekleme yöntemi kullanılmıştır. Bu doğrultuda çalışmaya İzmir'den 302, Konya'dan 183, Adana'dan 150 kişi katılmıştır.

Çalışmada Sun ve ark (2019) tarafından geliştirilen Gizlilik Endişesi Ölçeği, Li ve ark (2017) tarafından geliştirilen Algılanan Kontrol Ölçeği, Xu ve ark (2011) tarafından geliştirilen Algılanan Risk, Algılanan Fayda ve Veri Paylaşma Niyeti ölçekleri kullanılmıştır.

Araştırma verilerinin istatistiksel analizi için SPSS 26.0 programı kullanılmıştır. Güvenirlik analizi için Cronbach Alpha ve AVE değeri hesaplanmış ve geçerlik analizi için AMOS Graphics programı ile doğrulayıcı faktör analizi uygulanmıştır. Hipotezlerin test edilmesi için AMOS Graphics programı kullanılarak yapısal eşitlik modeliyle yol (path) analizi yapılmıştır.

Yapılan analizler sonucunda bireylerin kişisel sağlık verilerini paylaşma niyeti ile gizlilik endişesi arasında negatif yönlü anlamlı bir ilişki tespit edilmiştir. Fakat bu ilişkide algılanan risk ve algılanan faydanın aracılık rolünün olmadığı görülmüştür. Ayrıca bireylerin kişisel sağlık verilerini paylaşma niyeti ile algılanan kontrol arasında pozitif yönlü anlamlı bir ilişki tespit edilmiştir. Bu ilişkide algılanan risk ve algılanan faydanın aracılık rolü olduğu görülmüştür.

Anahtar Sözcükler: Algılanan fayda; algılanan kontrol; algılanan risk; gizlilik endişesi; kişisel sağlık verisi.

SUMMARY

REPUBLIC OF TURKEY

SELÇUK UNIVERSITY

HEALTH SCIENCES INSTITUTE

The Mediating Role of Perceived Risk and Perceived Benefit in the Relationship Between Intention to Share Personal Health Data, Privacy Concern, and Perceived Control

Havva Nur ATALAY

Department Of Healthcare Management

MASTER THESİS / KONYA-2022

The study was conducted to investigate whether perceived risk and perceived benefit have mediating roles in the relationship between individuals' intention to share personal health data, privacy concerns, and perceived control.

The population of the study consists of individuals living in İzmir, Konya and Adana provinces of Turkey. The sample size was determined as 600. Stratified random sampling method was used to determine at least how many people from which city should participate in the study. In this direction, 302 people from İzmir, 183 people from Konya and 150 people from Adana participated in the study.

In the study, Privacy Concern Scale developed by Sun et al (2019), Perceived Control Scale developed by Li et al (2017), Perceived Risk, Perceived Benefit and Data Sharing Intention scales developed by Xu et al (2011) were used.

SPSS 26.0 program was used for statistical analysis of research data. Cronbach Alpha and AVE values were calculated for reliability analysis and confirmatory factor analysis was applied with AMOS Graphics program for validity analysis. In order to test the hypotheses, path analysis was performed with the structural equation model using the AMOS Graphics program.

As a result of the analysis, a negative significant relationship was found between the intention of individuals to share their personal health data and privacy concerns. However, it was seen that the perceived risk and perceived benefit did not have a mediating role in this relationship. In addition, a positive and significant relationship was found between the individuals' intention to share their personal health data and perceived control. It was seen that perceived risk and perceived benefit played a mediating role in this relationship.

Keywords: Perceived benefit; perceived control; perceived risk; privacy concern; personal health data.

1. GİRİŞ

Sınırları tam olarak çizilemeyen (Dülger 2016), yönetilmesi hem bireye hem kanunlar aracılığıyla devlete ait olan (Chaudhry ve ark 2015) kişisel veriler, bireye ait olan ve bireyi tanımlayan bilgilerdir. Kişisel sağlık verileri ise bu bilgiler içerisinde özel nitelikli veriler olarak ele alınmaktadır. Bireyin bireysel sağlığı ile ilgili elde edilen bilgiler kişisel sağlık verilerini oluşturmaktadır. Bu veriler hem fiziki arşivlerde hem de elektronik ortamlarda toplanmaktadır (Bezirgan Gözmener, 2019). Tele sağlık, giyilebilir cihazlar, kişisel sağlık kaydı uygulamaları gibi birçok girişim de kişisel sağlık verilerinin toplanmasını kolaylaştırmaktadır. Ayrıca kişisel sağlık kayıtlarının elektronik ortama geçirilmesi için de günden güne daha fazla çalışma yapılmaktadır (Ibraimi ve ark 2009).

Kişisel sağlık verileri ticari değer taşıdığı için birçok sektörde pazarlamacılar, kimlik hırsızları ve birçok kuruluş için cazip bir hedef olmaktadır (Li 2015). Dolayısıyla kişisel sağlık verilerinin elektronik ortamlarda çevrimiçi olarak paylaşılması, siber saldırılar, kötü niyetli yazılımcılar, maddi kazanç elde etmek isteyen kişi veya kurumların varlığı gibi birçok sebeple riskli olarak görülmektedir (Youn 2009). Bansal ve ark'a göre (2010) sağlık hizmetleri bağlamında, kişisel sağlık bilgileri çevrimiçi olarak paylaşıldığında, kötüye kullanılabilmekte veya izinsiz olarak erişilebilmektedir. Ayrıca, hastaneler tarafından kişisel ve klinik bilgiler toplanırken, kullanılırken ve depolanırken oluşabilecek bilgi sızıntısı, mahremiyet ve güvenliğin ihlal edilmesi riskleri oldukça önemli bir konudur (Mehraeen ve ark 2016).

Bansal ve ark'a (2010) göre bireyler, kişisel sağlık verilerinin nasıl kullanıldığı, aktarıldığı, korunduğu ve bu bilgilerin paylaşılması aşamasında ne kadar kontrole sahip oldukları konularında gizlilik endişesi duymaktadır. Bu nedenle gizliliğin korunması ve klinik verilere yetkisiz erişimin önlenmesi gibi konular, veri girişi, saklama, kullanım ve aktarımın tüm aşamalarında yeterli dikkat gösterilmesi gereken temel konular arasındadır (Abouelmehdi ve ark 2018, Mehraeen ve ark 2016).

Gizlilik, sosyal bilimlerin neredeyse tüm alanlarında, özellikle de hukuk, ekonomi, psikoloji, yönetim, pazarlama ve yönetim bilgi sistemleri olmak üzere 100

yıldan fazla bir süredir incelenmektedir (Dinev ve ark 2013). Bu incelemeler sonucunda gizlilik "çok boyutlu, esnek, konuma bağlı ve yaşam deneyimine göre değişmesi anlamında" dinamik bir kavram olarak ele alınmaktadır (Xu ve ark 2011). Bilgi gizliliği endişesi ise bilginin kontrolünde olmak, bilgi alışverişinin güvenliği ve bu bilgiyi toplayanın kurallara uygun davranıp davranmayacağı olarak ele alınmaktadır (Bansal ve ark 2010). Dolayısıyla gizliliğin ana faktörlerinden biri algılanan kontrol düzeyidir (Princi ve Kramer 2020).

Algılanan kontrol, çevredeki değişikliklerin kişinin eylemlerine, çabalarına ve seçimlerine bağlı olduğu inancı olarak tanımlanmaktadır (Infurna ve ark 2011). Diğer bir deyişle, kişinin belirli bir eylemi sonuçlandırma düzeyi hakkındaki inançları algılanan kontrolü oluşturmaktadır (Alonso-Ferres ve ark 2020). Teknolojinin gelişmesi bilgiye erişimi kolaylaşmaktadır. Bilgiye daha kolay erişimle ilgili bu tür algılar, kullanıcıların kişisel bilgiler üzerindeki algılanan kontrolünü azaltmakta ve bu da öznel olarak daha yüksek gizlilik riskine yol açabilmektedir (Hoadley ve ark 2010). 2015 yılındaki bilgi güvenliği ihlallerine ilişkin istatistiklere göre kaybedilen verilerin %43'ünün kamu kurumlarında ve %19'unun sağlık hizmetlerinde olduğu (Henkoğlu 2017) ve 2020 yılındaki veri güvenliği ihlallerine ilişkin istatistiklere göre (Veri İhlali İstatistiği: Kapsamlı Rehber 2020) 2017 yılından 2019 yılına kadar sağlık verileri ihlallerinden etkilenenlerin sayısının %80 artttığı görülmektedir.

Algılanan gizlilik riskleri, kişiye ait olan her türlü verinin kötü niyetli olarak kullanılması sonucunda oluşacak belirsizlikle ilgilidir (Sun ve ark 2015). Veri paylaşma niyetinde risk algısının en az fayda algısının ise çok olması beklenmektedir (Choi ve ark 2013). Algılanan faydalar bireylerin verileri paylaştıktan sonra oluşacak yararlarla ilgilidir. Algılanan risklerin ve faydaların bir arada ele alınması gizlilik hesabı teorisini oluşturmaktadır. Bu modele göre bireyler, algılanan risklerin minimum, algılanan faydaların maksimum olduğu durumlarda veri paylaşımı gerçekleştirmektedir (Dinev ve ark 2013).

Dolayısıyla bu çalışmada, kişisel sağlık verileri paylaşım niyeti ile gizlilik endişesi ve algılanan kontrol ilişkisinde algılanan risk ve algılanan faydanın aracı rolü araştırılmıştır. Araştırma kapsamında kişisel veri, kişisel sağlık verisi, gizlilik endişesi, algılanan kontrol, algılanan risk ve algılanan fayda kavramları ayrıntılı olarak ele alınmaktadır.

1.1. Kişisel Veri ve Kişisel Sağlık Verisi Kavramları

Bu bölümde kişisel veri ve kişisel sağlık verisi kavramlarının tanımları ve kapsamları belirlenerek kişisel sağlık verilerinin önemi üzerinde durulmuştur.

1.1.1. Kişisel Veri Tanımı ve Kapsamı

Kişisel veri kavramı literatürde gerek direkt olarak tanımlanmış gerekse kapsamı belirlenerek hangi verilerin kişisel nitelikte olduğu üzerinde durulmuştur. Kişisel veri kavramı tanımlanmadan önce kişilik ve veri kavramlarının açıklanması kişisel verinin ne olduğunu anlamak açısından oldukça önemlidir.

Canlı doğum gerçekleşmesi şartı ile ana rahmine düşülen an ile başlayan (Türk Medeni Kanunu m. 28) ve ölümle sonuçlanan süreç kişilik kavramını oluşturmaktadır (Yücedağ 2017). Kişilik kavramında Türk Medeni Kanunu (TMK)'na göre gerçek ve tüzel kişiler şeklinde ayrım yapılmaktadır (Türkmen 2019). İnsan gerçek kişiliktir. TMK'nin 8. maddesinde tüm insanların hak ehliyetinin bulunduğu belirtilmiştir. Bu doğrultuda insanların her biri kişi kavramını oluşturur ve her bir kişi eşit haklara sahiptir (Özkan 2020). Kendilerine farklı bir kişilik atfedilmiş olan ürünlerin/malların veya bir/birçok kişinin bir araya gelmesi tüzel kişilik olarak tanımlanmaktadır (Dural ve Öğüz). Bu noktada söylenmelidir ki tüzel kişilerin verileri 6698 sayılı Kanun ile korunmamaktadır (Kişisel Verileri Koruma Kurumu 2020). Dolayısıyla bu çalışmada yer alan kişisel kavramı "gerçek kişiye ait olan" şeklindeele alınacaktır.

Veri; gözlemlerin, oluşumların veya çeşitli durumların her türlü gösterimidir (Kılınç 2012). Literatürde "veri" kavramı "bilgi" kavramı ile aynı anlamda kullanılmaktadır. Fakat "enformasyon (information)" olarak kullanılan bilgi ile "knowledge" olarak kullanılan bilgi kavramları birbirlerinin yerini tutmamaktadır (Başar 2019). Knowledge olarak ele alınan bilgi, enformasyonların bir araya getirilmesi sonucu oluşan bir bütünü ele alır. Bilgi sürecinin temelinde ise veri vardır. Bu süreç bir piramit olarak düşünülürse tabanında verinin olduğu sonrasında enformasyonun geldiği ve bilginin oluştuğu söylenebilir (Alkan 2003, Yılmaz 2009, Başar 2019). Fakat hem ulusal hem uluslararası düzenlemelerde kafa karıştırıcı olmaması adına bu ayrımların üzerinde durulmadığı görülmektedir. Bu sebeple bu çalışmada veri kavramı bilgi olarak ele alınmıştır.

Kişi ve veri kavramlarının tanımları yapılıp kapsamları belirlendikten sonra düzenlemelerde yer alan kişisel veri kavramını incelemek gerekmektedir çünkü gerek ulusal gerekse uluslararası yapılan düzenlemelerde kişisel veri kavramı genel hatlarıyla açıklanmıştır. Bu sebeple hem ulusal hem uluslararası düzenlemelerdeki tanımlara aşağıda yer verilmiştir.

Ulusal düzenlemelerden biri olarak ele alınan 6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK)'nda ve 2019 yılında yürürlüğe giren Kişisel Sağlık Verileri Hakkında Yönetmelik'te kişisel veri kavramı *"Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin(ait) her türlü bilgi"* şeklinde tanımlanmıştır (Dülger 2015a).Benzer bir şekilde Anayasa Mahkemesi tarafındankişisel veri,*"belirli veya kimliği belirlenebilir olmak şartıyla, bir kişiye ilişkin bütün bilgiler"*olarak ele alınmaktadır (Çelik 2017).

Uluslararası alanda kişisel veri, 1980 yılında Avrupa Birliği (AB)' nin yayımlamış olduğu 95/46/EC sayılı "Bireylerin Kişisel Verilerinin İşlenmesi ve Serbestçe Dolaşımı Karşısında Korunmasına İlişkin Direktif" md. 2/a' da; Avrupa Konseyi tarafından 1981 yılında imzaya açılan 108 sayılı Sözleşme md. 2(a)' da; İktisadi İşbirliği ve Kalkınma Teşkilatıtarafından kabul edilmiş olan ve uluslararası alanda ilk resmi belge niteliğinde olan "Kişisel Verilerin Sınır Aşan Trafiği ve Verilerin Korunmasına İlişkin Rehber İlkeleri" md. 1/b' de *"belirli veya belirlenebilir bir gerçek kişiye ilişkin tüm bilgiler"*olarak tanımlanmıştır (Akgül 2013, Ağıralan 2015, Avcı 2019).

Ulusal ve uluslararası düzenlemelerde yapılan tanımlamalardan yola çıkarak, bir verinin kişisel veri sayılabilmesi için gerçek bir kişi ve bu kişinin doğrudan veya dolaylı olarak tanımlanmasını sağlayan bir bilgi olması gerektiği söylenebilmektedir. Diğer bir deyişle kişisel veri, gerçek bir kişiye ait olmalı ve gerçek kişi bu veri ile tanımlanabilir, belirlenebilir ve nitelenebilir olmalıdır (Kişisel Verileri Koruma Kurumu 2018a). Sonuç olarak kişisel verinin nasıl tanımlandığı, ne anlam taşıdığı ve ne tür verilerin kişisel veri kapsamına girdiğinin net ve sınırlı bir yanıtı olmamakla birlikte bir bireyi tanımlamaya yönelik her çeşit "bilgi" o bireyin kişisel verisini oluşturmaktadır (Dülger 2019a). Bu noktada belirtilmelidir ki, kişisel veriler sadece isim, soy isim, doğum yeri ve doğum tarihi gibi bilgiler olarak sınırlandırılmamakta

aynı zamanda o kişinin fiziki özellikleri, sosyoekonomik durumu, ailevi durumu gibi özellikleri ile ilgili bilgileri de kapsamaktadır (Çelik 2017).

Geniş kapsama sahip kişisel veriler veri sahibinin hak ve özgürlüklerine ilişkin potansiyel riskleri nedeniyle (Orel ve Bernik 2018) özel nitelikli ve genel nitelikli olmak üzere 2' ye ayrılmaktadır. Özel nitelikli kişisel veriler literatürde "özel koruma gerektiren veri", "hassas veri" gibi farklı isimlerle ele alınmaktadır. 1998 yılında İngiltere'de yayımlanan Kişisel Verilerin Korunması Kanunu' nda "sensitive personal data - hassas kişisel veri", Hollanda Kişisel Verilerin Korunması Kanunu' nda ise "special personal data - özel kişisel veri" olarak ele alınmıştır (Korkmaz 2016). Ayrıca Türkiye'de 2016 yılında yayımlanan 6698 sayılı KVKK'da da bu ayrım "özel nitelikli kişisel veriler" şeklinde yapılmıştır (Kişisel Verileri Koruma Kurumu 2018). KVKK md. 6/1'de özel nitelikli kişisel veriler *"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 verileri"* şeklinde belirtilmiştir (Bayındır 2019, Kişisel Verileri Koruma Kurumu 2016). Bu veriler bireylerin özel alanını, temel özgürlüklerini ve mahrem alanlarını ilgilendirdiği için özel koruma gerektirmekte ve dolayısıyla diğer verilerden ayrı başlık altında incelenmektedir. Avrupa İnsan Hakları Mahkemesi de bu ayrımın yapılmasının gerekliliğini dile getirmekte olup alınan tedbirlerin artırılmasını uygun görmektedir (Korkmaz 2016). Sayılan tüm bu verilerin dışında kalan veriler ise genel nitelikli olarak ele alınmaktadır. Böylece verilerin işlenmesi, aktarılması, depolanması ve korunması hususunda öncelik veya ayrıcalık belirlenmektedir.

1.1.2. Kişisel Veriler ile İlgili Uluslararası Düzenlemeler

Büyük miktarda kişisel bilgi değiş tokuş edildiğinden, saklandığından ve paylaşıldığından, kişisel gizlilik kamuoyu gözetimi altındadır (Li ve ark 2011b). Aynı zamanda kişisel veriler üzerinde yetkisiz erişim, amaç dışı kullanım ve yanlış işleme gibi risk oluşturacak durumların varlığı ulusal bilgi güvenliği sistemini ve ulusal/uluslararası yönetmeliklerin gerekliliğini vurgulamaktadır (Olca ve Can 2014). Ayrıca kişisel sağlık bilgilerinin gizliliği ve güvenliği ilkelerinin belirlenmesinin amacı, bireylerin mevcut sağlık verilerinin, sağlığın iyileştirilmesine ve zararın azaltılmasına hizmet etmek için kullanılmasını sağlamaktır. Bu hedef doğrultusunda

bireysel ve kamu haklarını korumak için politikalar, prosedürler ve teknik yöntemler geliştirilmektedir (Beck ve ark 2016).Düzenleyici bakış açısından bu politikaların, prosedürlerin ve önlemlerin önemli katkısı vardır: yasalar hem gizliliği korumakta hem de hassas (özel nitelikli) kişisel verilerin toplanmasını ve kullanılmasını kısıtlamaktadır (Žliobait ve Custers 2016).

Gerek özel nitelikli gerekse genel nitelikli kişisel veriler Avrupa Konseyi, Birleşmiş Milletler (BM) vb. tarafından yapılan uluslararası düzenlemelere konu olmuştur. Yapılan bu düzenlemeler şekil 1.1.' de verilmiştir.



Şekil 1.1. Kişisel sağlık verileri ile ilgili uluslararası düzenlemeler.
Kaynak: Kişisel Verileri Koruma Kurumu 2021.

1960'lı yıllardan bu yana sağlık bilgi teknolojisindeki artışların etkiyle birlikte Avrupa Konseyi, Avrupa İnsan Hakları Sözleşmesi md. 8'e dayanarak kişisel verilerin korunması ile ilgili çeşitli düzenlemeleri kabul etmiştir (Warner 2005). İmzaya açılma tarihi 1981 ve yürürlüğe girme tarihi 1985 olan kişisel verilerin korunmasına yönelik ilk uluslararası hukuki düzenleme olan ''108 sayılı Kişisel Nitelikteki Verilerin Otomatik İşleme Tabi Tutulması Karşısında Kişilerin Korunmasına Dair Sözleşme" bu düzenlemeler içerisinde en önemli metindir (Kutlu ve Kahraman 2017). İlgili Sözleşmenin "Özel Veri Kategorileri" altında yer alan md.

6'ya göre bireylerin kökeni, dini inancı, adli sicilleri, siyasi görüşleri, cinsel yaşamları ve sağlıkları ile ilişkili verilerinin iç hukukta gerekli düzenlemeler yapılmadığı sürece işlenemeyeceği yer almaktadır (Korkmaz 2016). Bu doğrultuda 28 Ocak 1981'de ilk imzalayan ülkelerden olan Türkiye, uzun bir müddet kişisel verilerin korunması noktasında ayrıntılı bir kanun oluşturmaması sebebiyle Sözleşmeyi imzalamış ama onaylamamış tek ülke konumunda olmuştur (Kişisel Verileri Koruma Kurumu 2018b, Korkmaz 2016). Nihayetinde Türkiye ilgili sözleşmeyi iç hukukuna 17 Mart 2016 tarihinde 29656 sayılı Resmi Gazete'de yayımlayarak dâhil etmiştir. Bu sözleşmenin asıl hedefi üye olan tüm ülkelerde, kökeni ya da yaşadığı yer ayırt etmeksizin bireylerin kendileriyle alakalı kişisel özellikte olan verilerinin otomatik bilgi işleme noktasında temel hak ve özgürlükleri çerçevesinde korunmasını sağlamaktır (Kişisel Verileri Koruma Kurumu 2018b).

Küresel iletişim ağı olarak anılan internete bireylerin daha kolay erişim sağlaması, BM tarafından hem küresel kalkınmada bir araç hem de temel özgürlükleri sağlamaya yönelik bir hak şeklinde ele alınmaktadır. BM tavsiye niteliği taşısa da 1990'da kişisel verilerin korunması noktasında hazırlanan "Bilgisayarla İşlenmiş Kişisel Veri Dosyalarına İlişkin Rehber İlkeleri" kabul etmiştir (Arslan 2011, Kılınç 2012, Çalık 2016, Akçalı Gür 2019). İlgili belgede kişisel verilerin korunması noktasında uyulması gereken ilkeler yer almakta ve aşağıdaki gibi sıralanmaktadır (Kılınç 2012):

1.Yasallık ve dürüstlük
2. Doğruluk
3. Amacın belirli ve haklı olması
4. İlgili kişilerin erişme hakkı,
5. Ayrımcılıktan kaçınma
6. İstisna koyma yetkisi
7. Güvenlik
8. Denetim ve yaptırım
9. Sınır ötesi veri transferi

Avrupa Birliği (AB)'nde ise kişisel veri alanında ilk önemli düzenleme, 1995 yılında 95/46/EC sayılı Direktif ile yapılmıştır (Dülger 2019c). Direktifin esas amacı,

AB'ye üye olan ülkeler arasında kişisel verilerin korunması ile ilgili düzenlemelerin birliğinin sağlanmasıdır.

95/46/EC sayılı Direktif sonrasında AB, Özel verilerin kapsamlı bir şekilde toplanmasına yönelik direktifler sağlamak ve asgari standartları tanımlamak ve bireylerin mahremiyetini korumak için Genel Veri Koruma Tüzüğü (GDPR)'nü kabul etti (Princi ve Kramer 2020).

GDPR, AB'ye üye olan ülkelerde yaşayan kişilerin, mahremiyet ve gizlilik konusunda güvencelerini sağlamak adına oluşturulmuştur. Eksiksiz bir şekilde hazırlanmaya çalışılan bu yönergeye göre bireylerin verileri şeffaf ve anlaşılabilir onam olmadan kamuya sunulamaz ve kullanılamaz (Beyan ve ark 2020). Bu doğrultuda 25 Mayıs 2018 tarihinden beri AB üye ülkelerinde yürürlükte olan Yönetmelik, yeni dijital çağda mahremiyet hakkının güçlendirilmesini sağlamaktadır (Pintiliuc 2018).

1.1.3. Kişisel Veriler ile İlgili Ulusal Düzenlemeler

Çalışmanın uluslararası düzenlemeler başlığı altında da yer verilen, sınır ötesi verilerin nasıl paylaşılması gerektiği ve bu veriler ile ilgili alınması gereken önlemlerin yer aldığı 108 sayılı Sözleşme, 1981 yılında imzaya açılmış olup Türkiye tarafından da imzalanarak (Altundiş 2016, Hatipoğlu 2019) 17 Mart 2016 tarihinde iç hukuka dâhil edilmiştir (KVKK Uygulama Rehberi 2018, Gökçay ve Arda 2019). Ayrıca 2010'da Türkiye Cumhuriyeti Anayasası'na kişisel verilerin işlenmesi, düzeltilmesi ve silinmesini içeren bir hakkın mevcudiyeti ve kişisel verilerin korunması noktasındaki usul ve esasların kanunla belirlendiği hükümleri eklenmiştir (Gürsel ve Düğmeci 2018). Şekil 1.2'de kişisel verilerin korunması ile ilgili yapılan ulusal düzenlemeler verilmiştir (Kişisel Verilerin Korunması Kanununa İlişkin Uygulama Rehberi 2018):



Şekil 1.2. Kişisel sağlık verileri ile ilgili ulusal düzenlemeler.
Kaynak: Kişisel Verilerin Korunması Kanununa İlişkin Uygulama Rehberi 2018.

Günümüzde teknolojilerdeki gelişmelere paralel olarak bilişim alanında da ilerlemeler gerçekleşmiş olup elektronik ortamlarda veri paylaşımı sık kullanılır hale gelmiştir. Bu durum bilişim alanında ağlar aracılığıyla paylaşımı gerçekleşen kişisel veriler üzerinde siber saldırıların artmasına da sebep olmuştur. Verilere yapılan bu ihlaller birer suç niteliğinde sayılmaya başlanmış ve siber saldırıların bulunduğu bu noktada kamu tarafından kişisel verilerin güvenliğinin sağlanması için politika ve planlamaların yapılmasını mecburi kılmıştır (Kutlu ve Kahraman 2017).

Kişisel verilere ve kişisel sağlık verilerine ilişkin pek çok özel düzenleme her ne kadar veri koruma mevzuatında yer almaktaysa da bunların anayasa hukuku, ticaret hukuku, medenî hukuk, ceza hukuku ve hukukun diğer pek çok alanıyla irtibatı bulunmaktadır (Akkurt 2020). Bu doğrultuda da mevzuata yönelik olarak yeniden derleme yoluyla 2005 yılında 5237 sayılı Türk Ceza Kanunu (TCK) çıkarılmıştır. İlgili Kanun'un 135.-139. maddelerince kişisel verilerin ihlali durumunda oluşan suçlar hüküm altına alınmıştır. Suç tipleri düzenlenmiş olan

TCK'nın ikinci kitabında "kişilere karşı suçlar" başlığı altında ikinci kısmın dokuzuncu bölümü olan "özel hayata ve hayatın gizli alanına karşı suçlar" başlığı altında kişisel veriler ile ilgili suç tipleri ele alınmıştır (Dülger 2016). Bu maddeler ile genel olarak internet ve elektronik araçlar ile bireylerin verilerinin açık rıza olmadan edinilmesi ve paylaşılması gibi hususlarda düzenleme yoluna gidilmiştir (Kutlu ve Kahraman 2017, Sınar 2020). Yine sözü edilen ilgili Kanunda bu düzenlemeler verilerin toplanmasını, korunmasını ve özel hayatın gizliliğini de içermektedir (Kılınç 2012).

Kişisel verilerin korunması üzerine TCK'de düzenlenen ilk suç ''Kişisel verilerin (hukuka uygun olmadan) kayıt altına alınması" suçudur. Genel anlamda nitelik olarak ayrım yapılmadan kişisel verilerin hukuka uygun olmadan kayıt altına alınması, TCK md. 135'te hüküm altına alınan suçu oluşturmaktadır (Kart ve Ketizmen 2019). Ayrıca ilgili maddenin ikinci fıkrasında; kayıt altına alınan verilerin bireyin dini ve siyasi görüşlerine, ırkına, cinsel hayatına ve "*Sağlık Durumuna"* ilişkin olması halinde cezanın yarı oranında artırılacağı hüküm altına alınmıştır (Korkmaz 2016, Yılmaz 2018). 136. md. kayıt altına alınan verilerin hukuka uygun olmadan paylaşılması veya edinilmesi suçunu, 137. md. işlenen bu suçların nitelikli durumlarını, 138. md. verilerin silinmemesi suçunu ve son olarak 140. md. ise bu suçlarla ilgili olarak tüzel kişilikler üzerine uygulanması gereken güvenlik önlemlerini içermektedir (Dülger 2016).

Kanunda yer alan 135. ve 136. md. ile ortak hukuksal değerler korunmaktadır. Yani veriler hukuka uygun olmadan kaydedilir veya işlenilir ise kişinin özel hayatı ve bireysel korunma alanı dolayısıyla ''Kişisel Verileri'' bu maddeler ile korunmaktadır (Dülger 2015b).

KVKK m. 11/1/ğ 'de bireyin kişisel verilerinin ihlali durumunda karşılaştığı zararın giderilmesini talep etmek hakkı tanınmaktadır. Bu doğrultuda KVKK m. 14/3'te bireylerin kişisel verilerinin ihlali sonucu uğradığı zarar karşılığında genel hükümler aracılığıyla tazminat hakkına sahip olduğu yer almaktadır. Burada "genel hükümler" kavramı ile TMK ve Türk Borçlar Kanunu gibi düzenlemelerle kişilik hakkının korunması belirtilmektedir (Özkan 2020). Buradan da görülmektedir ki KVKK, TMK' ya atıf yapmaktadır.

TMK md. 2'de kişisel verilerin işlenmesi konusundaki ihlali, dürüstlük kuralı çerçevesinde ele alınmaktadır. Burada ele alınan dürüstlük kavramı, veri işleme sürecinde görevi kötüye kullanmama ilkesine uyma davranışıdır (Kişisel Verileri Koruma Kurumu 2018c).

TMK md. 24'te kişisel hak ihlalinde, kişilik hakkı zarar görmüş bireylerin rızası dâhilinde özel veya kamusal faydanın gözetilmesi ve kanun tarafından elde edilen yetkinin kullanılması durumunda hukuka aykırılık bulunmayacağı düzenlenmiştir (Türkmen 2019).

Yukarıdaki maddeler incelendiğinde, TMK bireylere kişisel veriler ile ilgili oluşan veya oluşabilecek her türlü ihlal durumunda dava açabilme hakkı tanımaktadır. Fakat koruma amaçlı açılacak olan dava, uygulama ve hukuki teknikler yönünden uygun bir çözüm yolu olarak görülmemektedir (Oğuz 2018).

Türkiye Cumhuriyeti Devleti, kişisel verilerin korunmasına yönelik olarak kanun tasarısı hazırlığı ile 1989 yılında ilk çalışmasına başlamıştır. 2006 yılına kadar yapılan tasarı çalışmaları devam etmiş ve 2008'de Türkiye Büyük Millet Meclisi'ne gönderilmiş ancak yasalaşma aşamasına geçmeden geçersiz sayılmıştır (Tataroğlu 2009). 2012 yılında tasarı başbakanlığa tekrar gönderilmiş ve 6698 sayılı Kişisel Verilerin Korunması Kanunu 7 Nisan 2016 tarihinde yayımlanmıştır (Çetin 2014, Dülger 2019b).

20 Ekim 2016'da 6698 sayılı Kanun'dan birkaç ay sonra "Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetinin Sağlanması Hakkında Yönetmelik" yayımlanmıştır (Zeybek Ünsal ve Örnek Büken 2018). Yayımlanan yönetmelik, 6698 sayılı Kanun'un henüz yeni olması, kişisel sağlık verilerini kapsayan bir yönetmeliğin çıkarılması için yeterli sayıda uzman görüşünün olmaması ve mevzuata uygunluk taşımadığı gerekçeleri ile eleştirilmiş ve yönetmeliğin durdurulması için dava açılmıştır (Dülger 2019b). Bu dava sonucunda 6 Temmuz 2017 tarihinde Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetinin Sağlanması Hakkında Yönetmelik'in yürütmesi Danıştay kararı ile durdurulmuştur (Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetinin Sağlanması Hakkında Yönetmelik (mülga), 2017). Bu karar sonrasında, söz konusu Yönetmelik 24 Kasım 2017 tarihinde eleştiriler doğrultusunda düzenlenerek 30250 sayılı Resmi Gazete'de Kişisel Sağlık

Verilerinin İşlenmesi ve Mahremiyetinin Sağlanması Hakkında Yönetmelikte Değişiklik Yapılmasına Dair Yönetmelik yayımlanmıştır (Dülger 2015a). Düzeltmeler her ne kadar eleştiriler göz önüne alınarak yapılmış da olsa *"Yürütmesi daha önceden durdurulmuş olan yönetmelik üzerinde değişiklik yapılamayacağı ve yürütmesi durdurulmuş olan yönetmeliği tekrar yürürlüğe koyma amacı taşıdığı için"* hukuka aykırılık taşıması gerekçesiyle bu Yönetmelik de Türk Tabipleri Birliği ve Türk Diş Hekimleri Birliği tarafından yargıya taşınmıştır (Dülger 2019b, Eke ve ark 2018, İmançlı 2019, Nalbantoğlu 2018,). Söz konusu Yönetmelik hakkında da 9 Ekim 2018 tarihinde yürütmenin durdurulması kararı alınmıştır. Son olarak Kişisel Sağlık Verileri Hakkında Yönetmelik 21 Haziran 2019 tarihinde 30808 sayılı Resmi Gazete'de yayımlanmış ve önceki Yönetmelik yürürlükten kaldırılmıştır (Dülger 2019b).

1.1.4. Kişisel Sağlık Verisi Tanımı ve Kapsamı

Özel nitelikli kişisel veriler içerisinde yer alan kişisel sağlık verileri 2019 yılında çıkarılan Kişisel Sağlık Verileri Hakkında Yönetmelik md.4/1'de, fiziksel ve ruhsal sağlıkla ilgili veriler, alınan sağlık hizmetleriyle ilgili oluşturulan bilgiler bütünü şeklinde tanımlanmaktadır. Farklı bir tanıma göre, paylaşım noktasında belirli kişilerin bulunduğu yalnızca seçilen kişilerle paylaşıldığı, paylaşılmaması gereken durumlarda hastanın makul bir nedeninin ve bu doğrultuda korunmaya değer bir faydanın olduğu bütün veri türleri olarak ele alınmaktadır (Başar 2019). Diğer bir deyişle bireyin yaptırdığı tahliller, kullandığı ilaçlar veya geçirdiği tüm hastalıklar kişisel sağlık verileri olarak ele alınmaktadır (Kişisel verileri Koruma Kurumu 2018). Aynı zamanda kişisel sağlık verileri, hastanın tıbbi durumları ve geçmişleri, ilaçları, akıl sağlığı, genetik yapısı, cinsel davranışı, yaşam tarzı, inançları ve alışkanlıkları hakkında bilgi içerebilmektedir (Li 2015). Ayrıca 108 sayılı Sözleşme'de sağlıkla ilgili olan veriler, bireyin şu anki, geçmiş ve gelecekteki ruhsal veya fiziksel sağlığı ile ilişkili bilgiler şeklinde tanımlanmıştır (Alp ve Gürsel 2020). Sonuç olarak bir kişinin sağlık durumunu belirten her türlü bilgi kişisel sağlık verisi olarak ele alınmaktadır (İmançlı 2019). Kişisel sağlık verileri özel nitelikli kişisel veriler arasında yer aldığından işlenmesinde açık rıza alınması şartı yer almaktadır.

Kişisel sağlık verilerinde açık rıza

Sağlık hizmetleri alanında gittikçe artan veri toplulukları oluşturulmakta ve bu veriler sağlık hizmeti sunumunu ve yaşam biçimini iyileştirmek için potansiyel bilgileri içermektedir (Beyan ve ark 2020). Bu bilgiler hem elektronik ortamda sanal olarak, hem arşivde fiziki olarak işlenip saklanmaktadır (Bezirgan Gözmener 2019). Kişisel sağlık verilerinin toplanması, işlenmesi ve paylaşımı üçlü bir döngü olarak görülebilmektedir. Bu döngünün etik ve ahlaki olarak devam edebilmesi noktasında hastanın açık rızasının alınması büyük önem taşımaktadır (Yıldırım 2019).

KVKK md.5 ile kişisel verilerin kişinin açık rızası alınmadan işlenemeyeceği kanuna bağlanmakta ve bireylere verilerinin üzerinde kontrol yetkisi vermektedir (Gökçay ve Arda 2019, Öksüzoğlu 2019). Aynı zamanda ilgili Kanunda kişisel sağlık verilerinin özel nitelikli veriler olarak gerekli görüldüğü takdirde açık rıza aranmaksızın işlenebileceği de yer almaktadır (Durmuş 2021).

Kişisel sağlık verilerinde veri sorumlusu ve veri işleyen

Kişisel sağlık verilerinin işlenmesi, kaydedilmesi, depolanması ve aktarımı aşamalarında veri işleyen ve veri sorumlusu kavramlarının farklarının bilinmesi gerekmektedir. Kişisel Sağlık Verileri Hakkında Yönetmelik'te veri sorumlusu *"Kişisel sağlık verilerinin işlenme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönelmesinden sorumlu olan gerçek veya tüzel kişi"* olarak; veri işleyen ise "*veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişi"* olarak tanımlanmaktadır (Kişisel Verileri Koruma Kurumu, 2018).

Baran ve Şener'e (2019) göre veri sorumlusunun yükümlülükleri; hastaya ait verilere ulaşımın güvenliğini ve bilgi gizliliğini sağlamak, verilere hukuka aykırı olarak erişilmesini engellemek ve bu doğrultuda gerekli olan teknik ve idari tedbirleri almaktır. Dolayısıyla veri sorumlusu, bulunduğu kurumdaki kanuna uygunluk denetimlerini yapmak ve yaptırmakla yükümlüdür (Baran ve Şener 2019).*"GDPR md.28'de veri işleyen tarafından işleme faaliyetinin gerçekleştirilmesinin, veri işleyen ile veri sorumlusu arasında veri işlenmesine ilişkin bir sözleşme ya da hukuki işlemin yapılmasıyla mümkün olabileceğine işaret edilmiş ve işlemin içeriğinin asgari şartları belirtilmiştir"* (Başara 2020).

Buradan hareketle veri işleyen kişinin veri sorumlusu doğrultusunda hareket ettiği ve veri sorumlusunun da işleme eyleminin yapılma sebebini ve yöntemini belirttiği sonucuna ulaşılabilmektedir.

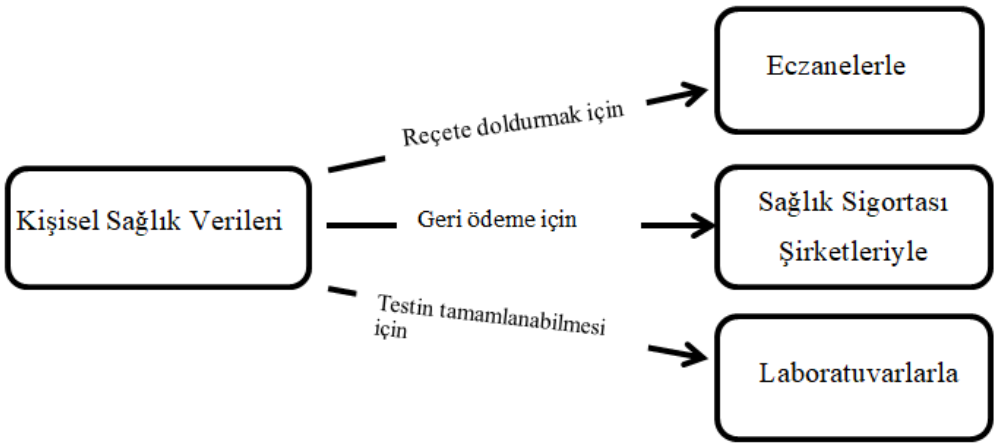
Kişisel sağlık verilerinin anonimleştirilmesi

Kişisel sağlık verilerinin kapsamı noktasında ele alınması gereken bir diğer husus da anonimleştirmedir (Yıldırım 2019). Veri sorumlusu, kaydedilen verilerin araştırma yapmak gibi amaçlar için kullanılması durumunda bireylerin gizliliğini koruyarak verileri anonimleştirme sürecine geçmektedir (Dankar ve El Emam 2012). Bu süreçler mevzuatlar neticesinde güvenilir olarak nitelendirilmekte olup gerek kamu gerek özel sektör veri anonimleştirme yoluna giderek veri paylaşımı noktasında teşvik edilmektedir (Gözüküçük 2014).

Anonimleştirme aşamasında; bireylerin ad, soyad ve Türkiye Cumhuriyeti kimlik numaraları gibi tanımlayıcı bilgiler silinmekte ardından kişiyi doğrudan veya dolaylı yoldan tanımlayan bilgi kategorileri değiştirilmektedir. Sonuç olarak kişisel verilerin paylaşılması noktasında anonimleştirme sayesinde veri gizliliği sağlanmaktadır (Ohm 2009). Gerek anonimleştirilerek bir çalışmada kullanılsın gerekse tedavi sürecinde yol gösterici olarak kullanılsın kişisel sağlık verilerinin önemi tartışılmazdır.

1.1.5. Kişisel Sağlık Verilerinin Önemi

Bilginin kapsamlı olarak yönetimi, kaliteli hizmet sunumu için bir gerekliliktir. Sağlık hizmetlerinde de kişisel sağlık verileri olarak ele alınan tüm bilgilerin planlı ve kapsamlı olarak elde edilmesi etkin yönetimi gerçekleştirmektedir (Baran ve Şener 2019). Dolayısıyla sağlık hizmetleri, bilgileri işlemekte, toplamakta, kullanmakta ve depolamakta olan bir sistem olarak ele alınmaktadır (Baran ve Şener 2019). Sistemde yer alan bütün bilgiler doğrudan hastanın adı ve diğer kişisel tanımlayıcılarla (ör. adres, sağlık sigortası, numarası vb.) bağlantılıdır. Bu bilgilerin genel olarak hangi amaçla ve kimlerle paylaşıldığı Şekil 1.3'te yer almaktadır.



Şekil 1.3. Kişisel sağlık verilerinin paylaşıldığı kurumlar ve sebepleri.
Kaynak: O'Doherty ve ark (2016) kaynağından yararlanılarak oluşturulmuştur.

Bir birey ile bir sağlık hizmeti sağlayıcısı arasındaki her etkileşim hastanın tanısı, sağlık geçmişi ve kullandığı ilaçlar hakkında bilgilerin kaydedilmesine yol açmaktadır. Bu bilgileri toplamanın temel amacı, bireyler ve topluluklar için en uygun sağlık hizmetini sağlamaktır (O'Doherty ve ark 2016). Beck ve ark (2016)'a göre ise kişisel sağlık verilerini toplamanın genel olarak iki nedeni vardır. Bunlar (Beck ve ark 2016):

- Hasta yönetimini optimize etmek ve bu hizmetlerin kullanımının bir sonucu olarak araştırmaların, müdahalelerin ve sağlık durumundaki değişikliklerin sonuçlarını belgelemek için doğru ve uzunlamasına tıbbi kayıtlar oluşturmak ve
- Sağlık hizmetlerinin kurumlarda, ulusal düzeylerde kullanımını, maliyetini, sonucunu ve etkisini izlemek ve değerlendirmek için sözde anonimleştirilmiş veya kimliksizleştirilmiş kişisel sağlık bilgilerini kullanarak araştırmalar yapmaktır.

Sonuç olarak kişisel sağlık verilerinin ilk toplanma amacından farklı olarak, sağlık hizmetlerinin iyileştirilmesi ve geliştirilmesi amacıyla kullanılması sıklıkla karşılaşılan bir durumdur. Bu amaçlar için yeniden kullanılabilecek kişisel verilere erişim, bilimsel araştırmalar için önemli bir faaliyet oluşturduğundan, bu tür işlemeye izin vermek oldukça önemlidir (Orel ve Bernik 2018).

1.2. Gizlilik Endişesi

Bu bölümde gizlilik, bilgi gizliliği vegizlilik endişesi kavramları tanımlanarak gizlilik endişesinin ölçülebilirliğine yer verilmiş ve kişisel sağlık verilerinin paylaşımında gizlilik endişesi incelenmiştir.

1.2.1. Gizlilik, Bilgi Gizliliği ve Gizlilik Endişesi Kavramları

Bireyler kendilerine ait olan verilerin korunmasını isteme hakkına sahiptir. Diğer bir deyişle bireyler, kişisel verilerinin kimlerle paylaşıp kimlerle paylaşılmayacağı konusunda karar verici konumunda olabilmektedir. Bu noktada ortaya çıkan unsur gizlilik olarak adlandırılmaktadır. Gizlilik, her türlü bilgilerin yetkisi olmayan kişiler tarafından elde edilmesinin engellenmesi ve bu bilgilerin korunması olarak tanımlanabilmektedir. Diğer bir deyişle gerek saklanıldığı/depolandığı ortamlarda gerekse aktarım sürecinde bilgiye yetkisiz kişilerin erişiminin engellenmesi şeklinde ele alınabilmektedir (Yüksel 2018, Baran ve Şener 2019).

Gizlilik kavramı kişiliğin korunması hakkı ile ilgili olarak *"Bireyin yalnız kalma özgürlüğü"* şeklinde ele alınmaktadır (Takçı ve Canbay 2017). Yaygın olarak kullanılan bir tanım, gizliliği kişinin kendisiyle ilgili bilgilere erişimini kontrol etmesi olarak tanımlar. Bu tanım, gizliliği açıklamaya yönelik kapsamlı bir girişimi temsil eder ve bireylerin bilgilerini tam olarak kontrol edemediklerini, ancak daha fazla kontrol istediklerini kabul eder (Kenny ve Collony 2016).

Bireyin kişisel bilgilerinin başkalarına ne zaman, nasıl ve ne ölçüde iletileceğini kontrol edebilme yeteneği olarak tanımlanan bilgi gizliliği, bilgi çağının en önemli etik, yasal, sosyal ve politik konularından biridir (Hong ve Thong 2013).

Dünyanın bilgi toplumu haline gelmesi bireylerde, bilgilerin kullanımı ve paylaşılması ile ilgili birçok endişenin oluşmasına sebep olmaktadır. Çünkü bu bilgiler yalnızca ürünlerle ilgili olmayıp direkt olarak bireylerle de ilgilidir (Buchanan ve ark 2007). Ayrıca teknolojinin gelişmesi verilerin ağ tabanlı uygulamalarda işlenmesini, aktarılmasını ve depolanmasını da beraberinde getirmektedir. Günümüzün elektronik dünyasında, rekabet stratejileri giderek artan bir şekilde büyük miktarda işlenen veriye bağlıdır. Kuruluşlara değer sağlayan bu

verilerin işlendiği bilgi uygulamaları, bireyler için gizlilik endişeleri yaratmaktadır (Culnan ve Armstrong 1999, Lee ve Kwon 2015). Diğer bir deyişle kablolu ve kablosuz ağ platformunun bağlanabilirliği veri kaynaklarında bir genişlemeye ve kişisel bilgilere daha kolay erişime yol açmıştır (Li ve ark 2011a) ve bu doğrultuda bireylerin gizlilik endişesi artmıştır.

Gizlilik endişesi kurumların bilgi gizliliği uygulamaları ile ilgili bireylerin kaygısıdır. Gizlilik endişesi, algılanan gizlilik ihlali olasılığını ve gizlilik ihlalleri sırasında oluşması beklenen kayıplara bireylerin tepkilerini yansıtır (Borena ve ark 2013). Gizlilik endişesi, istenmeyen iletişime ve kişisel bilgilerin kötüye kullanımına karşı korunma ihtiyacı olarak tanımlanmaktadır. Bu doğrultuda kişisel bilgi alışverişi esnasında bilgi güvenliğinin kontrol altında olması ve bilginin paylaşıldığı kişinin bunu uygun şekilde kullanıp kullanmayacağı ile ilgilidir (Dhagarra ve ark 2020).

Tüketicilerin iki tür gizlilik endişesi vardır. İlk olarak, ikincil kullanım riskinden, yani kişisel verilerinin, tüketicinin kişisel verilerini ilişkilendirdiği işlemin parçası olmayan üçüncü taraflarla paylaşma gibi, rızaları olmaksızın ilgisiz amaçlarla yeniden kullanılması riskinden endişe duymaktadırlar. İkincisi, tüketiciler, güvenlik ihlalleri veya iç kontrollerin eksikliği nedeniyle kişisel verilere yetkisiz erişim konusunda endişelidir (Gupta ve Dubey 2016, Dhillon ve Moores 2001, Bessen 1993). Bu noktada bilgi gizliliği endişesinin ölçülebilirliği ve en aza indirilmesi için çalışmalar yürütülmesi oldukça önemli hale gelmektedir.

1.2.2. Gizlilik Endişesinin Ölçülebilirliği

Gizliliği tek başına ölçebilmek neredeyse imkansızdırve ilişkiler iktisadi olarak değerlendirilmekten çok bireyin algı ve biliş düzeyi ile ilgili olduğundan gizlilik endişe düzeyini ölçebilmek için araştırmacılar inanç, tutum ve algı gibi ölçütler kullanmaktadır (Smith ve ark 2011). Bireylerin kişisel bilgi sağlama istekliliğini etkileyen faktörleri anlamak, hem hizmet sunucuları açısından hem de hizmet sunumunu geliştirmesi gereken kişiler açısından önemlidir (Li ve ark 2011a). Bu nedenle, bireylerin bilgilerinin üçüncü kişilerle paylaşılmasına ilişkin gizlilik endişelerini ve bunları etkileyen faktörleri anlamak büyük önem taşımaktadır (Sun ve ark 2019).

Literatürde gizlilik endişelerini ayrıntılı olarak ölçülebilir hale getiren birkaç çalışma mevcuttur. Bunlardan ilki Bilgi Gizliliği Endişesi Ölçeği (CFIP)' dir. Bu ölçek Smith ve ark (1996) tarafından geliştirilmiş ve ölçekte gizlilik endişelerinin veri ile ilgili dört boyutu belirlenmiştir. Bunlar; toplama, hata, ikincil kullanım ve bilgiye yetkisiz erişimdir (Osatuyi 2015). Elde edilen bu boyutlar daha sonra Stewart ve Segars (2002) tarafından yeniden doğrulanmıştır. O zamandan beri bu boyutlar, bireylerin kurumsal gizlilik uygulamalarına yönelik endişelerini ölçmek için güvenilir ölçeklerden biri olarak ele alınmaktadır.

Malhotra ve ark (2004) tarafından ise e-ticaret üzerinden alışveriş yapan ve internet üzerinden bilgilerini paylaşan bireylerin endişelerini ölçmek için İnternet Kullanıcılarının Bilgi Gizliliği Endişesi Ölçeği (IUIPC) geliştirilmiştir. Toplama, kontrol ve farkındalık olmak üzere üç alt boyuttan oluşan ölçek Smith ve ark (1996) tarafından geliştirilen ölçekten yararlanılarak oluşturulmuştur.

Sağlık bilgi teknolojileriyle ilgili gizlilik endişelerini açıkça ele almak için ise Kenny ve Connoly (2016) Sağlık Bilgileri Gizliliği Endişeleri Modelini (HIPC) geliştirdi. Bu model, Toplama, Yetkisiz İkincil Kullanım, Uygunsuz Erişim, Hatalar, Kontrol ve Farkındalık olmak üzere altı alt boyuttan oluşmaktadır. Modelin ilk dört boyutu daha önce açıklanmış olan CFIP ölçeği ile son iki boyut olan kontrol ve farkındalık ise IUIPC ölçeğinden yararlanılarak oluşturulmuştur (Becker 2018).

1.2.3. Kişisel Sağlık Verileri ve Gizlilik Endişesi

Sağlık hizmeti bağlamında gizlilik, hastaların tıbbi kayıtlarının, rıza sağlanması yoluyla nasıl kullanılacağı üzerinde kontrol sahibi olmaları gerektiği anlamına gelir (Bani Issa ve ark 2020). Diğer bir deyişle sağlık hizmetlerinde gizlilik, genellikle kişisel sağlık verileri hakkındaki hassas bilgileri koruma yeteneğine sahip olmak olarak tanımlanmaktadır (Abouelmehdi ve ark 2018).

Kişisel sağlık verilerinin gizli tutulması uygulaması, sağlık mahremiyetinin bir boyutunu oluşturmaktadır. Çünkü hasta mahremiyetine bağlılığı korurken elektronik tıbbi kayıtların paylaşılması ve yayılması, tıbbi bilişimin ve genel olarak toplumun karşılaştığı en büyük zorluklardan biridir (Devi ve Prasad 2017). Sağlık kurum ve kuruluşları, sağlık tehditlerini belirlemek, sağlık hizmetlerini değerlendirmek ve iyileştirme konusundaki yasal yükümlülüklerini yerine getirmek

için kişisel sağlık verilerini toplar, depolar ve kullanır. Bu sağlık verilerinin toplanmasının temeli, hassas bilgilerin gizliliğini ve güvenliğini korumayı gerektiren kamu güvenidir (Lee ve Gostin 2009).

Gizlilik, mahremiyetin bir uzantısıdır ve esas olarak bilgilerin, özellikle hassas klinik verilerin korunmasını belirtir. Bu noktada gizlilik, sağlık hizmeti sağlayıcıları ve hastalar arasındaki güvenilir iletişim veya anlaşma boyutuna atıfta bulunarak mahremiyetten ayrılır (Bani Issa ve ark 2020). Tıpta gizlilik, hastaların hekimlere güvenerek paylaştığı bilgilerin üçüncü kişilerle paylaşılmamasını ifade etmektedir (Yüksel 2018). Başka bir tanıma göre kişisel sağlık verilerinin gizliliği, hasta ile hekim arasında aktarılan bilgilere yönelik paylaşım iznini sınırlayan bir dizi kural anlamına gelmektedir. Ayrıca sağlık bilgilerinde gizlilik, bireyin sağlık bilgilerinin paylaşılmasını önleme hakkıdır (George ve Bhila 2019).

Kişisel sağlık verilerinin toplanması aynı zamanda bu verilere yetkisiz kişilerin erişim sağlaması ile belirli mahremiyet sorunlarına neden olabilmektedir. Bu sebeple bireylerin çoğu sağlık verilerinin toplanmasını kabul etmemektedir. Bu durum, sağlık hizmetlerinin geliştirilmesi için büyük bir engel teşkil etmektedir (Kim ve ark 2018). Ayrıca sağlık bilgilerinin gizliliği endişesi, bireylerin hassas alanlarda sağlık hizmetlerinden kaçınmasına bile neden olabilir (Bansal ve ark 2010).

Kişisel sağlık verilerinin paylaşımında gizlilik ihlallerinin olması bireylerin sağlık çalışanlarına güvenini de sarsmaktadır. Bu güvensizlik durumu ise hastalar ve sağlık çalışanları arasındaki iletişime ve tedavi süreçlerine yansımaktadır (Maraş ve Ceyhan 2021).Yüksel'e (2018) göre de bu durum şu şekilde ele alınmaktadır:

> *"Bireyin, sağlık verilerinin yeterli düzeyde korunmadığına yönelik şüphesi, sağlık hizmetlerinden faydalanmaktan kaçınması sonucunu doğuracak ve bu durum hem bireysel hem de toplumsal düzeyde oldukça ağır zararlara yol açabilecektir. Zira hasta ile hekim arasındaki güven bağı hem teşhis, hem de tedavi sürecinde büyük önem taşır"* (Yüksel 2018).

Sonuç olarak hasta bilgileri hem son derece hassas olduğu için güvenli ve gizli tutulması gerekir, hem de farklı sağlık hizmeti sağlayıcılarının bunlara erişmesi gerekebilmektedir (Mehraeen ve ark 2016). Bu sebeple, hastaların uygun tıbbi bakımı alabilmeleri için bu verilerin bir kısmı paylaşılmalıdır, ancak aksi takdirde

izinsiz paylaşılması hastaya zarar verebileceğinden tüm veriler gizli kalmalıdır (Li 2015). Verilerin paylaşılması gerektiği durumlarda ise veriler anonimleştirilip bireyi tanımlayacak bilgi bütünü olmadan aktarılmalıdır. Altman (1975) gizliliği tanımlarken bireye ve ona ait bilgilere erişimde seçici kontrol uygulanmasına odaklanmıştır. Bu tanımda gizlilik ile ilgili olarak bilgi kontrolü vurgulanmaktadır. Diğer bir deyişle kontrol boyutu, bireyin kendi kişisel sağlık verileri üzerinde yeterli kontrole sahip olmadığına dair endişelerini kapsar (Becker 2018). Bu nedenle gizlilik endişesi ile birlikte algılanan kontrol kavramı da ele alınmalıdır.

1.3. Algılanan Kontrol

Bu bölümde kontrol ve algılanan kontrol kavramları tanımlanarak kişisel sağlık verileri paylaşımında algılanan kontrol incelenmiştir.

1.3.1. Kontrol ve Algılanan Kontrol Kavramları

Kontrol, genellikle psikolojik bir kavram olarak davranış bilimlerinde kullanılmıştır. Bu açıdan tanımlanan kontrol, insanların karşılaştıkları olaylarda önemli sonuçlar oluşturacak faaliyetlerin, durumların ve davranışların farkındalığı ve seçimi ile ilgili inançlarının tümüdür (Skinner ve Connell 1986). Diğer bir deyişle kontrol kavramı bir kişinin bir durumu önemli ölçüde değiştirme ve tahmin etme inancını belirtmekte ve bir kişinin yaşamı üzerindeki etkisine ilişkin inançlarının kapsamını tanımlamaktadır (Hajli ve Lin 2014).

Kişisel veriler söz konusu olduğunda kontrol kavramı gizlilik durumunu belirleyen faktörlerden biri olarak ele alınabilmektedir (Xu 2007). Malhotra ve ark (2004) da kontrolü, bilgi gizliliğinin aktif bir bileşeni olarak görmektedir. Bu sebeple yapılan çoğu çalışmada kontrol kavramı gizliliği tanımlamada oldukça yardımcı olmuştur. Örneğin; Bennett (1967) gizliliği bilginin seçici kontrolü olarak tanımlamıştır. Jourard (1966) gizliliği, insanların mevcut deneyimleri hakkında belirli bilgileri başkalarından saklamasının bir sonucu olarak görmektedir. Bu tanımda, verileri diğer bireylerden saklama eylemindeki kontrol düzeyi dikkat çekmektedir. Westin (1967) ise *"Bireyin kendisi hakkında hangi bilgilerin başkalarına ve hangi koşullar altında iletileceğine karar verme/koşulları kontrol etme hakkı"* olarak tanımlamıştır. Bu görüşün merkezinde üç kilit unsur vardır: karar vermenin özerkliği, kişinin kendisi hakkındaki bilgi ve bu bilgiyi iletme sürecindeki

bireyin kontrol düzeyi (Yao ve ark 2007). Goodwin (1991) ise tüketici gizliliğini, bireyin verilerine izinsiz fiziksel erişim üzerindeki kontrol ve bilgi paylaşımı üzerindeki kontrol olmak üzere iki farklı kontrol boyutu ileele almaktadır. Bu tanımlamalardan da yola çıkarak kişisel verilerdeki kontrolün, gizlilikle ilişkili ancak ayrı bir yapı olduğu anlaşılmaktadır (Dinev ve Hart 2006, Dinev ve ark 2013). Laufer ve Wolfe (1977) da yalnızca bireyin bir durumda kontrolü algılaması üzerine gizliliğin oluşmayacağını vurgulayarak kontrolü, gizlilik sisteminde arabulucu bir değişken olarak kavramsallaştırmıştır.

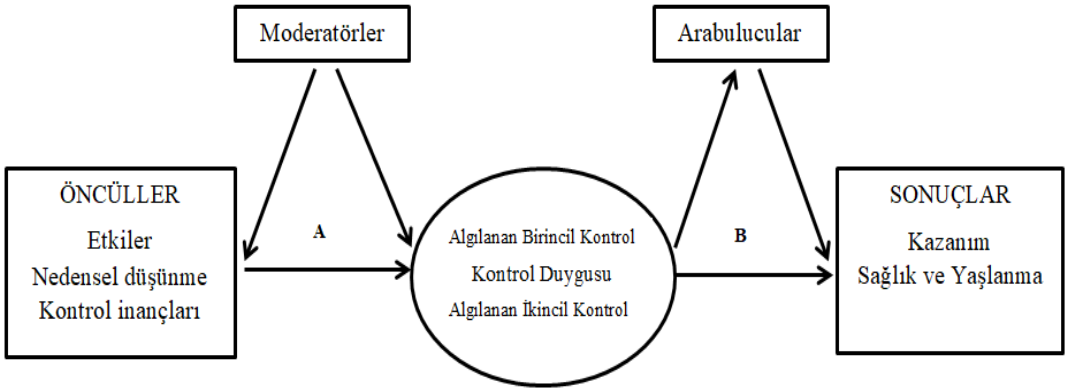
Algılanan kontrol, bilimsel araştırma alanı olarak 20.yy ortalarında gerçekleşen "Bilimsel Devrim" anlayışıyla oluşmuştur. Zamanla davranış ve motivasyon teorilerinde ele alınmıştır. Kontrol Değeri Teorisi, Sağlık İnanç Modeli, Koruma Motivasyon Teorisi ve Planlı Davranış teorisine uyarlanan Gerekçeli Eylem Teorisi algılanan kontrol üzerinde yapılan ve sağlık alanında da onaylanan çalışmalara örnek gösterilmektedir (Chipperfield ve ark 2012). Ayrıca Conner ve Armitage (1998), öz-yeterlik ve algılanan kontrol arasında ayrımın daima göz önünde tutulması gerektiğine dikkat çekmiştir. Sonuç olarak algılanan kontrol, genellikle kontrol odağı, öz yetkinlik ve öz yeterlik gibi belirli kontrol teorilerini açıklamak için kullanılmaktadır (Connell 1985, Weisz ve Stipek 1982).

Bilgi kontrolünün çeşitli kullanımları, tüketicilerin gizliliklerinin ihlali konusundaki endişelerini azaltabilir (Wang ve ark 2016). Bireyler, gizliliği artıran (sağlayan) teknoloji aracılığıyla kişisel kontrol uyguladıklarında, çevreleri üzerinde birincil kontrol elde etmek için çabalarlar (Xu ve ark 2011). Li ve ark (2011a)'a göre veriler üzerinde algılanan yüksek kontrole sahip bireyler, kişisel bilgilerinin paylaşılması ve daha sonra kullanılması üzerinde daha fazla kontrol algılamakta, yüksek gizlilik riski inançlarına sahip olanlar ise kişisel bilgileri üzerindeki potansiyel kontrol kaybına karşı daha ihtiyatlı davranmaktadır. Das ve Teng (1998), kontrolün katılımcı taraflar arasında işbirliğine dayalı davranışta güven oluşturmada önemli bir mekanizma olarak görülebileceğini ileri sürmektedir. Bu şekilde ele alınan algılanan kontrol, bir platformda güven atmosferinin yayılmasına yardımcı olmaktadır (Krasnova ve ark 2010). Böylece bireylerin yüksek bilgi kontrolü algısı, algılanan riskleri hafifletmekte ve veri paylaşma niyetini olumlu yönde artırmaktadır (Hajli ve Lin 2014).

1.3.2. Kişisel Sağlık Verileri ve Algılanan Kontrol

Kontrol kavramının odak noktası tüketicilerin ne kadar bilgiyi paylaşacaklarına, başkalarının bunları nasıl algılamasını istediklerine veya kendilerini nasıl paylaşmaları gerektiğine karar vermeleridir (Wang ve ark 2016). Bu noktada kontrol duygusu, bireyin sonuçları ele alma kapasitesini ve yeterliliğini artıran bir faktör olabilmektedir (Robinson ve Lachman 2017, Alonso-Ferres ve ark 2020, Hofmann ve ark 2014). Bu şekilde ele alındığında algılanan kontrol bireylerin sonuçlar üzerinde bir değişime sebep olabileceklerine inandıklarında ortaya çıktığı görülebilmektedir (Eryılmaz ve Ercan 2010). Aynı zamanda bireyin sahip olduğu kaynaklar arttıkça ve karşılaştığı engeller azaldıkça algılanan kontrol düzeyi artmaktadır (Kocagöz ve Dursun 2010). Verilerin ödeme aracı olduğu ve bu bilgilerin elde edilmesinde şirketlerin ve diğer kurumların büyük bir çıkara sahip olduğu dijital bilgi çağında, özel veriler üzerinde kontrol her zamankinden daha önemli hale gelmiştir (Princi ve Kramer 2020).

Chipperfield ve ark (2012) algılanan kontrolde ele alınan bu ilişkiyi sağlık alanında öncüller ve sonuçlar arasındaki ilişki şeklinde açıklamaktadır. Herhangi bir alanda bireyin kendine inancı ve hareketleri üzerinde kontrolü olduğu sürece sonucu değiştirebildiği bilinmektedir. Fakat sağlık alanında bu kontrolün sonucu bireysel değil toplumsaldır. Örneğin bir sınava hazırlanmak ve yüksek almak bireyin kendi kontrolü sonucu oluşurken, sağlıklı beslenmesine ve egzersiz yapmasına rağmen toplumun geneline yayılmış bir salgın hastalığa yakalanmak bireysel algılanan kontrolün dışında gerçekleşmektedir. Ayrıca bireysel algılanan kontrol çerçevesinde kriptolu olarak korunan ve verilere bir saldırı sonucu ulaşılması bireyin kontrolü dışında gerçekleşmektedir. Bu ilişki şekil 1.4'te yer almaktadır.



Şekil 1.4. Kontrol duygusunun öncülleri ve sonuçları.
Kaynak: Chipperfield ve ark (2012) kaynağından uyarlanmıştır.

Bireyin çevredeki olay veya durumları etkileyebilme kabiliyeti olarak görülen algılanan kontrolün sağlık alanıyla yüksek bir ilişkisinin olduğu bilinmektedir (Chipperfield ve Greenslade 1999). Bireyler sağlık sorunları yaşadıklarında, sunulan sağlık hizmetlerine kolay erişim, tanı ve tedavi aşamalarında kendisine ait olan tüm bilgileri sağlık personelleri ile güvenerek paylaşır ve bu paylaşım esnasındaki tüm verilerin gizliliğinin korunacağına inanır (Şenyürek 2017). Veriler, meşru sağlık amaçları için kullanılması koşuluyla kuruluşlar arasında paylaşılabilir. Verileri alan kuruluşun gizlilik ve güvenlik önlemlerinin, verileri toplayanlarla eşdeğer olması gerekir (Beck ve ark 2016). Bu noktada kontrol bir güvenlik duygusu oluşturarak risklerin olmadığı bir güven duygusu oluşturur (Princi ve Kramer 2020). Güven, bir tarafın, diğer taraf için önemli olan belirli bir eylemi gerçekleştireceği beklentisine dayanarak, diğer tarafı izleme veya kontrol etme kabiliyetine bakılmaksızın, başka bir tarafın eylemlerine karşı kontrolünün bulunmaması olarak tanımlanır (Hong 2015). Sağlık hizmetlerindeki güven durumu bilgi asimetrisinden dolayı yüksektir. Hekim-hasta arasındaki bu ilişki esnasında elde edilen kişisel bilgiler, hastanın kendisine ait bilgilerin paylaşımı durumundan haberdar olmadıkça başkaları ile paylaşılmamalıdır (Than Win 2005).

Algılanan kontrol aynı zamanda planlı davranış teorisinin temel taşlarından birini oluşturmaktadır (Ajzen 1991). Bu teoriye göre bireylerin eyleme geçmesine algılanan sosyal normlar ve algılanan kontrol düzeyleri etki etmektedir. Gerçek ve algılanan kontrol arasında ayrım yapılması gerekmektedir. Özellikle e-sağlık uygulamalarında gerçek kontrol, teknik ayarlar ve izinler aracılığıyla kurulabilir

(Princi ve Kramer 2020). Ayrıca burada bulunan kişisel sağlık verileri, aktarımdan önce yerel olarak anonimleştirilebilir (Clarke ve Steele 2015). Fakat kan alma sırasında verilen kontrol miktarının bireysel olarak algılanan kontrolden farklı olabileceği de görülmektedir (Bugental ve ark. 1989).

1.4. Algılanan Risk ve Algılanan Fayda

Bu bölümde risk kavramı, algılanan risk kavramı, algılanan risk türleri ve kişisel sağlık verileri ve algılanan risk başlıklarına yer verilmiştir.

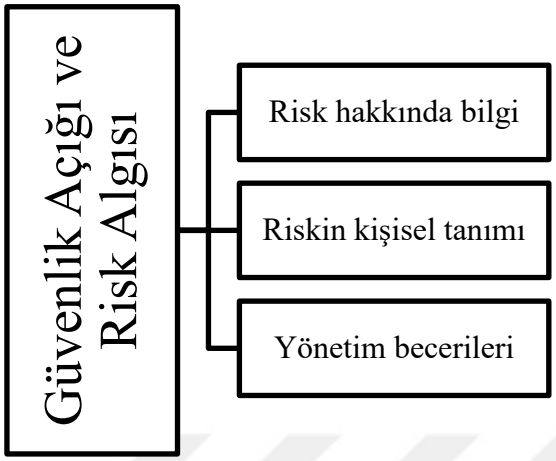
1.4.1. Algılanan Risk ve Algılanan Fayda Kavramları

Risk, genel olarak olumsuz bir sonuç potansiyelinden kaynaklanan belirsizlik ve diğer tarafın kayıplarla sonuçlanabilecek fırsatçı davranışlarının olasılığı olarak tanımlanmıştır (Xu ve ark 2008). Başka bir tanıma göre ise risk, bir olayın istenmeyen ve olumsuz sonuçlarının gerçekleşme potansiyelidir (Beldad ve ark 2011). Risk eğilimi (bireyin genel risk alma istekliliği olarak tanımlanır) bireyler arasında farklılık göstermektedir ve risk algıları da arzu edilen bir sonucun izlenmesinden kaynaklanan bir kayıp olasılığına dair öznel bir inanç olarak adlandırılmaktadır (Beldad ve ark 2011). Bireyler, özellikle işleme amaçları hakkında bilgilendirilmedikleri zaman, kişisel verilerinin tam kullanımıyla ilgili olası risklerin çoğu zaman farkında olmazlar (Fabiano 2019). Bu durum da algılanan risk kavramının ele alınması gerekliliğini vurgulamaktadır.

Algılanan risk kavramı 1960'lı yıllarda gelişmeye başlamış olup ilk olarak Raymond Bauer tarafından tanımlanmıştır. Bu tanıma göre algılanan risk, tüketicilerin davranış ve tutumlarını açıklamak için kullanılmakta ve belirsizliğin olduğu durumlarda bireyin tavrını belirtmektedir (Deniz ve Erçiş 2008, Türkmendağ ve Uygur 2020). Bauer, tüketicilerin belirli bir mal ve hizmeti satın alma eyleminin sonuçlarının belirsizliği ve yönlendirilememesi sebebiyle risk barındırdığını ileri sürmüştür (Deniz ve Erciş 2008).

Bireylerin olayları gözlemlemeleri ve değerlendirmeleri bir risk algısını oluşturmaktadır (Ercan ve ark 2020). Bu risk algısı güvenlik açığının oluştuğu durumlarda meydana gelmektedir. Şekil 1.5'te güvenlik açığı ve risk algısının bileşenleri üç farklı faktör olarak verilmiştir. Bu üç faktörde, nesnel bilgi (bilgi),

öznel bilgi (sezgi), ilgi alanları (kişisel değerler ve motivasyonlar) ve inançlar (fikirler veya onaylanmamış bilgi) rol oynamaktadır. (Zambrano-Cruz ve ark 2018).



Şekil 1.5. Güvenlik açığının ve risk algısının bileşenleri.
Kaynak: Zambrano-Cruz ve ark (2018) kaynağından yararlanılarak oluşturulmuştur.

Algılanan risk, bir davranışın olası sonuçları hakkındaki belirsizliğin ve bu sonuçların olası zararlarının bir birleşimi olarak düşünülebilir (Forsythe ve Shi 2003). Dolayısıyla algılanan risk, kişilerin ya da firmaların müşterilerinin şahsi bilgilerine üçüncü şahısların erişim sağlaması sonucunda ortaya çıkması muhtemel sorunlar ile ilgilidir (Malhotra ve ark 2004, Wang ve ark 2016). Yani risk kavramı farklı alanlarda hem olumlu hem olumsuz sonuçlarda incelenirken, tüketicilerin tutum ve davranışlarının söz konusu olduğu pazarlama alanında yalnızca olumsuz sonuçlarda incelenmektedir (Ada ve Aksoy 2020). Bu düşünceyi destekleyen Boshoff ve ark (2011)' a göre algılanan riskler, bir davranışın potansiyel sonuçları hakkındaki belirsizliğin ve bu sonuçların muhtemel olumsuzluğunun bir aracı olarak görülmektedir. Aynı zamanda kişisel verilerin paylaşımı durumunda bireylerin bilgilerine gerek firmalar aracılığı gerekse siber saldırılar ile üçüncü kişiler tarafından ulaşılabilme riski de algılanan riski oluşturmaktadır (Malhotra ve ark 2004, Wang ve ark 2016). Buna bağlı olarak, gizlilik riskleri, kişisel verilerin kötüye kullanılması olasılığının neden olduğu belirsizlikle ilgilidir (Sun ve ark 2015).

Fayda ise çok temel bir tanım ile "yarar" olarak ele alınmaktadır. Diğer bir deyişle, fonksiyonellik ve işlevsellik şeklinde tanımlanmaktadır (Tanrıkulu ve Bakır 2021). Literatürde değer ve fayda kavramları aynı anlamda kullanılmaktadır. Ancak

fayda ve değer kavramlarının birbirinden farklı kavramlar olduğu belirtilmelidir (Başaran ve Aksoy 2015, Zeithaml 1988). Algılanan değer, bireyin paylaşım aşamasında neyin alındığına ve neyin verildiğine ilişkin algılarına dayalı olarak veri paylaşımının kendisi için oluşturduğu faydasına ilişkin genel değerlendirmesidir (Park ve ark 2004, Zeithaml 1988). Ayrıca algılanan değer, algılanan faydaların katlanılan maliyetlere karşı psikolojik ve zihinsel değerlendirme sonucudur, yani bireyler kişisel verileri paylaştıklarında nelere katlanmaları gerektiğini bilişsel olarak fark ettiğinde değer kavramından söz edilmektedir (Wu ve ark 2008). Chen ve Dubinsky (2003) de algılanan değeri, bireylerin istenen sonuçların oluşmasında katlanılan maliyet karşılığında elde edilen algılanan net fayda şeklinde tanımlamıştır.

Algılanan faydalar, bireylerin ihtiyaç ve isteklerini karşılayan avantajlarının ve memnuniyetlerinin toplamıdır. Bu, bireylerin verileri paylaştıktan sonra ne kazandığına dair algıdır (Tanadi ve ark 2015). Aynı zamanda algılanan fayda, bireyin seçimlerinin temel bir parçasını oluşturmaktadır (Choi ve ark 2013). Genel olarak algılanan fayda, bireylerin verilerini paylaştıklarında elde edecekleri kazancın bilincinde olmaktır (Xu ve ark 2011, Smith ve ark 2011).

1.4.2. Algılanan Risk Türleri

Pazarlamada risk, tüketicilerin ürün/hizmet satın aldıklarında veya satın alma sürecindeki satıcı üzerinde algıladıkları belirsizliği ifade etmektedir. Dolayısıyla bu belirsizlik durumlarını temel kaynaklara göre kategorize etmek ve tüketicilerde belirsizlik oluşturan durumları incelemek sonucunda algılanan risk kavramının türleri ortaya çıkmaktadır (Çakar ve Can 2019). Algılanan risk kavramının tanımlanmasından itibaren bu kavramı ölçmeye yarayan faktörlerin belirlenmesi üzerinde literatürde birçok çalışma yapılmıştır. Bu çalışmalara Tablo 5.1'de yer verilmiştir. Xu ve ark (2009)'a göre algılanan riskin performans, zaman, güvenlik, psikolojik, sosyal ve finansal kayıp gibi birtakım türleri mevcuttur ve tüm risk unsurları performans riskinden kaynaklanmaktadır.

Tablo 5.1. Algılanan Risk Türleri.

	Risk Türleri
Cox (1967)	Finansal ve sosyo-psikolojik
Jacoby ve Kaplan (1972)	Finansal, ürün performansı, fiziksel, sosyal ve psikolojik
Taylor (1974)	Sosyal / psikolojik ve işlevsel / ekonomik kayıp
Peter ve Ryan (1976)	Finansal, ürün performansı, fiziksel, sosyal, psikolojik ve zaman / kolaylık
Stone ve Gronhaug (1993)	Ekonomik, işlevsel, fiziksel, sosyal ve psikolojik
Schiffman ve Kanuk (1994)	Finansal, güvenlik, işlevsel, sosyal, psikolojik ve zaman kaybı
Jarvenpaa ve Todd (1996)	Finansal, performans, sosyal ve gizlilik
Kurtz ve Clow (1997)	Sosyal, psikolojik, finansal ve ürün performansı
Tan ve Toe (2000)	Finansal ve gizlilik
Cases (2002)	Finansal, fiziksel, ürün performansı, psikolojik, sosyal ve zaman kaybı
Laroche ve ark (2003)	Finansal, performans, psikolojik, sosyal ve zaman kaybı
Deniz ve Erciş (2008)	Finansal, fiziksel, performansı, psikolojik, sosyal, ve zaman kaybı
Zhao ve Li (2012)	Finansal, fiziksel, ürün performansı, psikolojik, sosyal ve zaman kaybı
Cöddü (2015)	Finansal, fiziksel, ürün performansı, psikolojik, sosyal, zaman kaybı ve gizlilik
Yaka (2018)	Fiziksel, ürün performansı, psikolojik, sosyal ve zaman kaybı

Kaynak: Cox(1967), Jacoby ve Kaplan(1972), Taylor(1974), Peter ve Ryan(1976), Stone ve Gronhaug(1993), Schiffman ve Kanuk(1994), Jarvenpaa ve Todd(1996), Kurtz, Clow(1997), Tan ve Toe(2000), Cases(2002), Laroche ve ark(2004), Chen ve Chang(2005), Deniz ve Erciş(2008), Boshoff ve ark(2011), Zhao ve Li(2012), Cöddü(2015), Yaka(2018) kaynaklarından yararlanmıştır.

Literatürde yer alan yerli ve yabancı çalışmaların incelenmesi sonucu algılanan risk türleri; finansal, ürün performansı, fiziksel, sosyal, psikolojik, güvenlik, zaman kaybı ve gizlilik şeklinde sıralanabilmektedir. Bireylerin bir ürün

veya hizmeti satın alma kararı için "genel risk" yukarıda bahsedilen risk türlerinden herhangi birini içerebilmekte ve algılanan riskin çok boyutlu bir yapı olduğu sonucuna varılmaktadır (Boshoff ve ark 2011).

Finansal Risk: Bir ürünün satın alınması sürecinde parasal kayıp olasılığı ve bireyin gizli finansal bilgilerinin diğer bireyler tarafından kötüye kullanılma olasılığı şeklinde tanımlanmaktadır (Boshoff ve ark 2011, Huang ve ark 2004).

Ürün performansı: Algılanan performans riski, satın alınan mal veya hizmetlerin tüketicinin beklentilerini karşılayamama ihtimalidir. Algılanan riskin bu boyutu, ürünlerin kullanışlılığı veya işlevselliği ile benzerlik göstermektedir (Lim 2003).

Fiziksel risk: Bireylerin gizlilik inançlarını şekillendirmekte duruma özgü faktörlerin etkisini inceleyen Laufer ve Wolfe (1977), kişilerin fiziksel alan nitelikleri, uygun davranışın tanımı, tahmin edilen riskler ve faydalar gibi somut duruma özgü faktörleri değerlendirerek gizlilik inançlarının şekillendirilebileceğini öne sürmektedir (Li ve ark 2011a).

Sosyal Risk: Birey, sosyal statüsünü yükseltmek ve sosyal açıdan toplumda kabul edilebilirlik sağlamak için ürün veya hizmetleri satın alır. Satın aldığı ürünün bireyin bu yöndeki beklentilerini karşılamaması sosyal risk faktörünü oluşturmaktadır (Ada ve Aksoy 2020). Sosyal risk, ürün veya hizmetin oluşturduğu kötü durumun birey üzerinde arkadaşları ve ailesi tarafından yaşanılan hayal kırıklığının etkisini de yansıtmaktadır (Ueltschy ve ark 2004).

Psikolojik Risk: Algılanan riskin bu boyutu, yaptığı seçimin kötü olmasının kişide oluşturduğu hayal kırıklığı ve diğer psikolojik sorunlar (kaygı, stres, üzüntü vb) ile ilgilidir (Deniz ve Erciş 2008).

Güvenlik Riski: Bu tür riskler bireylerin bilgilerinin izinsiz kullanılması, çalınma ihtimali ve gizliliğine yöneliktir (Ercan ve ark 2020). Kişiye ait özel verilerin çalınması, izinsiz erişim sağlanması ve dolayısıyla gizliliğinin korunamaması bu risk türünü oluşturmaktadır (Hong ve Yi 2012).

Zaman kaybı riski: Zaman riski, bir ürün veya hizmetin satın alınma sürecinde oluşan zaman kaybı olasılığı şeklinde ifade edilmektedir (Chen ve He 2003).

Gizlilik riski: Gizlilik riski, müşterinin kişisel verileri üzerindeki potansiyel kontrol kaybı ile ilgilidir. Pek çok yetkisiz kişi, bilgileri açık rıza olmadan kullanmakta ve bilgi verilerinin kötüye kullanılmasına yol açmaktadır bu durum da gizlilik riskini oluşturmaktadır (Tanadi ve ark 2015).

1.4.3. Gizlilik Hesabı Teorisi

Bireylerin kişisel verilerini paylaşma niyetlerini ölçmenin iki yöntemi vardır; bu yollardan ilki algılanan faydanın boyutunu belirlemek ikincisi algılanan risklerin boyutunu belirlemektir (Wang ve ark 2016). Tıp teknolojilerinde bazı durumlarda, riskler ve faydalar uygulama olarak ayrı veya bağımsız değildir. Örneğin; bir kaza sonucu bilinç kaybı durumunda verilerin bireyin onamı alınmadan mecburi paylaşılması risk olarak, bu paylaşım sonucu hayatının kurtulması ise fayda olarak görülebilmektedir. İlişkilerde genel olarak değişkenlik olsa da, algılanan risk ne kadar yüksekse, algılanan fayda o kadar düşük olur ve bunun tersi de geçerlidir (Alhakami ve Slovic 1994).

Gizlilik paradoksunun en temel dayanaklarından biri "homo economicus (ekonomik insan)" terimidir. Ekonomide bu terim kararları ve eylemlerinin tümü faydalarını en üst düzeye çıkarma girişimiyle yönlendirilen bir tüketici olan ekonomik insanı varlığını ifade eder (Rittenberg ve Trigarthen 2012, Flender ve Müller 2012). Ekonomik insan kavramı gizlilik açısından uyarlandığı zaman; bir tüketicinin bilgisini paylaşmasından elde edebileceği faydaları, paylaştığı zaman oluşacak risklere tercih etmesi beklenir (Lee ve Kwon 2015). Bu görüşe göre, bireyler, tamamen bilgili olarak ele alınmakta veya kararlarını olasılıklara dayandıran ileriye dönük algılanan faydaları maksimize etmek için çabaladıkları varsayılmaktadır (Acquisti ve Grossklags 2005). Yapılan araştırmalar, bireylerin faydalara ilişkin algısının riske aracılık eden bir faktör olarak işlev görebileceğini göstermiştir. Bireyler verilerini paylaşırken ekonomik insan anlayışının zıttına faydayı en üst düzeye çıkarmaktan ziyade kayıpları önlemek için daha çok motive

olmakta ve dolayısıyla algılanan risk bireylerin davranışını açıklamada daha önemli hale gelmektedir (Gerber ve ark 2014, Ghamari ve Mellbin 2015, Lim 2003).

Culnan ve Armstrong (1999) verinin paylaşılması sürecinde bireyler tarafından algılanan faydalar ve algılanan riskler arasındaki dengenin hesaplanması ile gizliliğin ölçülebileceğini (privacy calculus) ifade eder. Bu teori; gizlilik endişeleri, algılanan riskler, algılanan faydalar ve veri paylaşma niyetinden oluşur (Sun ve ark 2019). Gizlilik hesabı teorisi, tüketicilerin ürün veya hizmet sağlayıcıların kişisel bilgilerine erişmelerine izin verdiklerinde, bilgilerin paylaşılmasını sağlayan ve engelleyen motivasyon faktörlerinin maliyet (risk) - fayda analizini gerçekleştireceklerini ileri sürmektedir (Wang ve ark 2016, Sheehan ve Hoy 2000).

Verilerin paylaşılmasından algılanan faydaların algılanan risklerden daha ağır basması beklerlenirse, bireylerin gönüllü olarak kişisel sağlık verileri paylaşma isteklerini analiz etmek için öncelikle gizlilik hesabı teorisi kullanılır (Becker 2018). Bu model algılanan faydalar ile gizlilik riskleri arasındaki değiş tokuşun sonuçlarının çok önemli bir rol oynadığını öne sürmesine rağmen, literatürdeki çalışmalar algılanan risklerin ve algılanan faydaların ana etkilerine odaklanmış ancak bu iki faktör arasındaki etkileşimi değerlendirmemiştir (Dinev ve Hart 2006, Xu ve ark 2009, Zhao ve ark 2012). Ayrıca uygulamada tazminat, sektör özdenetim ve hükümet düzenlemeleri yoluyla dağıtıcı ve prosedürel adalet hükümlerinin, bilgi paylaşımının algılanan yararlarını ve risklerini etkilediği varsayılmaktadır (Xu ve ark 2009).

1.4.4. Kişisel Sağlık Verileri, Algılanan Risk ve Algılanan Fayda

Kişisel sağlık kayıtları bağlamında hastanın bilgi güvenliğine yönelik riskler, bireylere çeşitli derecelerde zarar veren hatalara yol açan teknik (yazılım ve donanım bileşenleri) ve teknik olmayan (insanla ilgili) faktörler arasındaki etkileşimlerden kaynaklanabilmektedir (Bani Issa ve ark 2020). Teknik olmayan yani insanla ilgili olan faktörlere örnek olarak; bireylerin mobil sağlık uygulamalarını kullanırken şifrelerini yetkisiz kişilerle paylaşmaları ve yetkili kişilerin ticari amaçlarla verileri üçüncü kişilere aktarmaları gibi durumlar verilebilmektedir (Eke ve ark 2018). Sağlık teknolojilerine bağlı olarak bilgi uygulamalarının da gelişmesi bireyin sağlık durumunun daha görünür olmasına ve böylece veri madenciliği ve haritalanması ile

verilerin yetkisiz kişilere aktarılmasına sebep olmaktadır.Bu noktada ise yazılım ve donanım kaynaklı teknik hatalar ve riskler oluşmaktadır (Becker 2018).

Sağlık hizmetlerinin teşhis, tetkik ve tedavi aşamalarında kaydedilen kişisel sağlık verileri kolayca analiz edilebilmekte, dağıtılabilmekte ve yeniden kullanılabilmektedir. Bu nedenle bireyler bu kolaylığın olumlu sonuçlarının yanında kendi bilgisi veya rızası olmadan ilgisiz amaçlarla kullanılması konusunda nispeten yüksek bir risk algılamaktadır (Becker 2018). Örneğin bulut hizmeti sağlayıcıları, verileri üçüncü taraflara satmak için kötüye kullanabilmektedir. Bu tür gizlilik saldırıları, kullanıcıların güvenini etkilemekte ve hassas veri depolama konusunda onları şüpheci hale getirmektedir (Thilakanathan ve ark 2016). Bir sağlık kayıt sistemi, çeşitli yaygın saldırılar altında olabilir. Bu tehditlerden bazılarına aşağıda yer verilmiştir (Win ve ark 2006):

Maskeleme: Bir varlığın başka bir varlıkmış gibi davranması.

Kaynakların yetkisiz kullanımı: Bu, hem ağlardaki kaynaklara hem de bir bilgisayar sistemine yetkisiz erişimi içerir.

Yetkisiz ifşa ve bilgi akışı: Bu tehdit, ağ bağlantılı bir sistemde depolanan, işlenen veya aktarılan bilgilerin hem iç hem de dış kullanıcı kuruluşlara yetkisiz ifşasını ve yasa dışı akışını içerir.

Kaynakların ve bilgilerin yetkisiz olarak değiştirilmesi: Bilgilerin yetkisiz olarak değiştirilmesi hem bir sistem içinde (belleğe yazarak) hem de ağ üzerinden (aktif dinleme yoluyla) gerçekleşebilir.

Eylemlerin reddi: Bu, kuruluşlarda hesap verebilirliğe yönelik bir tehdittir.

Yetkisiz hizmet reddi: Burada, saldırgan, bunları kullanma yetkisi olan varlıklara kaynak veya hizmetleri reddetmek için hareket eder.

Sağlık kuruluşlarındaki yöneticiler ve liderler kişisel sağlık verileri paylaşımındaki algılnaan faydayı artırmak için aşağıdaki anahtar stratejileri takip etmelidir (Ceccato ve Price 2019):

- *Personel için gizlilik ve güvenlik eğitimi ve uygulamaları da dâhil olmak üzere "altın veri" kültürüne öncülük etmek,*
- *Özelleştirilmiş veri rollerinin değerini anlamak ve doğru kişilerle doğru rollere yatırım yapılmasını sağlamak. Örneğin, sağlık bilişimi profesyonelleri, veri gereksinimlerini tanımlayıp haritalamak için ve veri analistleri verileri analiz etmek ve yorumlamak için,*
- *Bir gizlilik görevlisinin varlığından emin olmak ve verilerin anonimleştirilmesi, uygun erişim haklarının sağlanması ve verilerin toplanması, saklanması ve yok edilmesi için politikaların uygulanması,*
- *Verilerin sağlık hizmeti sunumu ve sonuçları üzerindeki etkisi hakkında halk eğitimi ve bilgi paylaşımı ile daha geniş bir topluluğu bilgilendirmek,*
- *Veri analitiği ve uygulamaları için fırsatlardan yararlanmak için akademik topluluklar ile ortaklıklar kurmak,*
- *Veri bilgi sistemlerinin güvenliği ve gizliliğinin dış denetimlerini sağlamak,*
- *Büyük verinin yeni dünyasında rıza konuları etrafındaki tartışmaları yönetmektir.*

1.5. Veri Paylaşma Niyeti

Bu bölümde niyet ve veri paylaşma niyeti tanımlandıktan sonra kişisel sağlık verileri ve veri paylaşma niyeti ele alınmıştır.

1.5.1. Niyet ve Veri Paylaşma Niyeti

Niyet, belirli bir davranışta bulunma motivasyonu veya arzusunun gücünü ifade eder (Ajzen, 1991). Veri paylaşma niyeti ise bireyin kendine ait bilgileri kendisi dışında bir kişiye veya bir platforma aktarma ihtimalinin olup olmaması durumudur (Xu ve ark 2011). Veri paylaşımı ile ilgili bireysel karar süreci, birçok faktörden etkilenir veya engellenir. Bunlar arasında, eksik bilgi, sınırlı rasyonellik ve rasyonaliteden sistematik psikolojik sapmalar, mükemmel rasyonalite varsayımının bir bireyin gizliliğe duyarlı davranışının nüanslarını yeterince yakalayamayabileceğini göstermektedir (Acquisti ve Grossklags 2005).

Tüketicilerin kişisel bilgi paylaşım davranışı, bilgi ifşası kavramı ile açıklanmaktadır. İş bağlamında bilgi ifşası, tüketicilerin biyografik ve demografik özellikleri, yaşam tarzı, alışveriş alışkanlıkları, tüketim tercihleri gibi kişisel

bilgilerinin şirketlerle paylaşılması anlamına gelir. Tüketiciler, kişiselleştirilmiş hizmetler, çeşitli ayrıcalıklar, ödüller, indirimler ve finansal avantajlar elde etmek için kişisel bilgilerini paylaşabilmektedir (Özkan 2018).

1.5.2. Kişisel Sağlık Verileri ve Veri Paylaşma Niyeti

Kişisel veri paylaşımı ile ilgili hangi alanda olursa olsun geçmişten günümüze kadar yapılan çalışmalar bir bireyin bilgi gizliliği konusunda endişelenme eğilimi olarak tanımlanan, tüketicilerin genel gizlilik endişesine odaklanmıştır (Buchanan ve ark 2007, Malhotra ve ark 2004, Smith ve ark 1996, Yao ve ark 2007). Chen (2013) tarafından yapılan bir araştırmada, bireylerin gizlilik endişelerinin artmasının kişisel bilgileri paylaşma niyetini azalttığı sonucuna ulaşılmıştır. Aynı zamanda Zlatolas ve ark (2019) tarafından yapılan bir diğer çalışmada algılanan faydaların ve gizlilik endişelerinin bireylerin kişisel verileri paylaşma niyetleri üzerinde doğrudan bir etkisi olduğu ileri sürülmüştür. Beyan ve ark (2020)'a göre halkın, kişisel verilerin işlenmesi, korunması ve depolanması üzerindeki bilinç düzeyi giderek artmaktadır ve bu da bireylerin veri paylaşma konusundaki niyetlerini etkilemektedir. Mevcut düşünceler sağlık verilerinin açık rıza ve onam alınmadan başkaları ile paylaşılıp bireyin temel özgürlük hakkına zarar veren bir gizlilik ihlalinin bulunduğu yönündedir. Yetkili kişilere erişim izni verilen bilgilerin etik kullanımı belirsizdir. Bireyler firmaların etik olmayan davranışlarından, bu veri paylaşımının sonuçlarından ve erişim izni verilmeyen verilere dahi ulaşım sağlanabilmesinden endişelenmektedir (Wang ve ark 2016).

Kişisel bilgilerin adil veya sorumlu bir şekilde kullanılmaması, bir bireyin kişisel bilgilerin kullanımını kontrol edememesinden kaynaklanan iki tür bilgi gizliliği endişesi ortaya çıkarabilir (Culnan ve Armstrong 1999):

- ➔ İlk olarak, bir güvenlik ihlali veya uygun dâhili kontrollerin bulunmaması sonucunda kişisel bilgilere yetkisiz erişim elde edilirse, bir kişinin gizliliği ihlal edilebilir.

- ➔ İkincisi, bilgisayara aktarılmış bilgiler kolaylıkla kopyalanabileceği ve paylaşılabileceği için ikincil kullanım riski vardır, yani bir amaç için sağlanan bilgiler, bireyin bilgisi veya rızası olmadan ilgisiz amaçlar için yeniden kullanılabilir.

Pahalı, karmaşık ve evrensel olarak kullanılan bir hizmet olan sağlık, aynı zamanda en kişiselleştirilmiş hizmetlerden biridir. Güven oluşturmak ve sürdürmek ve mahremiyetin sağlanması, hastaların bir sağlık hizmeti sunum sistemine sürekli katılımı için esastır (Dhaggarra ve ark 2020).

Eksik bilgi, dışsallıklar, bilgi asimetrileri, risk ve belirsizlikler bireylerin kişisel sağlık verilerini paylaşma niyetlerini etkilemektedir (Acquisti ve Grossklags 2005).

2. GEREÇ VE YÖNTEM

2.1. Araştırmanın Amacı

Çalışmanın amacı,kişisel sağlık verileri paylaşım niyeti ile gizlilik endişesi ve algılanan kontrol ilişkisinde algılanan risk ve algılanan faydanın aracı rolünü araştırmaktır.

2.2. Araştırmanın Önemi

Kişisel verilerin güvenliği konusunda üzerinde en çok durulması gereken kavram, kişisel sağlık verileridir. Bireyler artık hastaneye gitmeden de e-nabız gibi belirli uygulamalar ve giyilebilir sağlık teknolojileri ile kişisel sağlık verilerini paylaşmaktadır. Paylaşılan bu verilerin işlenmesi, depolanması, aktarılması, korunması ve gizliliğinin sağlanması gerekli kanunlarla güvence altına alınmış olsa da yüksek düzeyde endişe ve belirsizlik içermektedir. Literatüre bakıldığı zaman kişisel sağlık verilerinin korunması noktasında birçok hukuki bakış açısı kazandırıldığı gözlemlenmiştir. Fakat bireylerin bu konuda gizlilik endişesini, güven durumunu, algılanan risk ve algılanan fayda düzeylerini dolayısıyla veri paylaşma niyetlerini inceleyen çalışmaya rastlanmamıştır. Bu açıdan çalışmanın özgün nitelikte olduğu düşünülmektedir. Çalışma özellikle farklı bölgelerdeki bireylerin sağlık verileri paylaşımındaki görüşlerine yer verdiği için literatüre bu açıdan da katkı sağlayacaktır.

Çalışmada kullanılan tüm ölçeklerin geçerlilik ve güvenilirlikleri yapılmış ve bu kapsamda doğrulayıcı faktör analizi sonuçlarına yer verilmiştir. Dolayısıyla daha sonra bu ölçeklerden birini ya da birkaçını kullanmak isteyen araştırmacılara katkı sağlaması beklenmektedir.

2.3. Araştırmanın Türü

Araştırma; bireylerin kişisel sağlık verileri paylaşımında gizlilik endişesi, algılanan kontrol, algılanan risk, algılanan fayda düzeyleri ve veri paylaşma niyetleri arasındaki ilişkiyi inceleyen nicel bir çalışmadır.

2.4. Araştırmada Kullanılan Ölçekler

Araştırmada kullanılan anket formu iki bölümden oluşmaktadır. İlk bölüm yaş, cinsiyet, öğrenim durumu, annenin öğrenim durumu, babanın öğrenim durumu, yaşanılan şehir, aylık gelir düzeyi, meslek, bir günde internette geçirilen süre, e-nabız kullanma durumu gibi demografik bilgileri içeren 23 sorudan oluşmaktadır. İkinci bölümde bireylerin gizlilik endişelerini ölçmeye yönelik dört ifade, algılanan kontrol düzeylerini ölçmeye yönelik üç ifade, kişisel sağlık verisi paylaşımında mevcut olan riskleri algılama düzeylerine yönelik üç ifade, mevcut olan faydaları algılama düzeylerini ölçmeye yönelik üç ifade ve son olarak kişisel sağlık verilerini paylaşma niyetini ölçmeye yönelik üç ifade yer almaktadır. Dolayısıyla 23 demografik veri ve 16 ölçek ifadesinin yer aldığı anket formu katılımcılara yönetilmiştir.

Çalışmada; gizlilik endişesi, algılanan kontrol, algılanan risk, algılanan fayda ve veri paylaşma niyeti ölçekleri kullanılmıştır. Ölçekler hakkındaki bilgiler aşağıda yer almaktadır.

2.4.1. Gizlilik Endişesi Ölçeği

Gizlilik Endişesi Ölçeği, Sun ve ark (2019) tarafından geliştirilip geçerlilik ve güvenilirlik testleri yapılmış olan "Gizlilik ve Bilgi Paylaşma Niyeti" ölçeğinin alt ölçeğidir. Ölçek 3 maddeden oluşmaktadır. İfadeler 1-hiç katılmıyorum' dan 5-kesinlikle katılıyorum' a kadar olan beş basamaklı Likert ölçeği üzerinden cevaplandırılmıştır. Ölçeğin iç tutarlılık katsayısı (Cronbach Alpha) 0,90 olarak yüksek güvenilirlikte bulunmuştur.

2.4.2. Algılanan Kontrol Ölçeği

Li ve ark (2017) tarafından geliştirilen ve geçerlilik güvenilirlik testleri yapılmış olan "Çok Boyutlu Gelişim Ölçeği" nin alt boyutu olan Algılanan Kontrol Ölçeği 3 maddeden oluşmaktadır. İfadeler 1-Kesinlikle Katılmıyorum' dan 5-Kesinlikle Katılıyorum'a kadar olan 5 basamaklı Likert Ölçeği üzerinden cevaplandırılmıştır. Ölçeğin iç tutarlılık katsayısı (Cronbach Alpha) 0,92 olarak yüksek güvenilirlikte bulunmuştur.

2.4.3. Algılanan Risk Ölçeği

Xu ve ark (2011) tarafından Konuma Duyarlı Pazarlama Ölçümü için geliştirilen ve geçerlilik güvenilirlik testleri yapılmış olan ölçeğin alt boyutunu oluşturan Algılanan Risk ölçeği 3 maddeden oluşmaktadır. 1-Hiç Katılmıyorum'dan 7-Kesinlikle Katılıyorum'a kadar 7'li Likert tipinde olan ölçeğin iç tutarlılık katsayısı (Cronbach Alpha) 0,94 olarak yüksek güvenilirliktedir.

2.4.4. Algılanan Fayda Ölçeği

Xu ve ark (2011) tarafından Konuma Duyarlı Pazarlama Ölçümü için geliştirilen ve geçerlilik güvenilirlik testleri yapılmış olan ölçeğin alt boyutunu oluşturan Algılanan Fayda Ölçeği 3 maddeden oluşmaktadır. 1-Hiç Katılmıyorum'dan 7-Kesinlikle Katılıyorum'a kadar 7'li Likert tipinde olan ölçeğin iç tutarlılık katsayısı (Cronbach Alpha) 0,91 olarak yüksek güvenilirliktedir.

2.4.5. Veri Paylaşma Niyeti Ölçeği

Bireylerin veri paylaşma niyetini ölçmek için Xu ve ark (2011) tarafından Konuma Duyarlı Pazarlama Ölçümü için geliştirilen ve geçerlilik güvenilirlik testleri yapılmış olan ölçeğin alt boyutunu oluşturan Veri Paylaşma Niyeti Ölçeği kullanılmıştır. Ölçek 3 maddeden oluşmaktadır. İfadeler 1-Hiç Katılmıyorum'dan 7-Kesinlikle Katılıyorum'a kadar olan 7 basamaklı Likert ölçeği üzerinden cevaplandırılmıştır. Ölçeğin iç tutarlılık katsayısı (Cronbach Alpha) 0,86 olarak yüksek güvenilirlikte bulunmuştur.

2.5. Araştırmanın Evreni ve Örneklemi

Araştırma, rastgele örnekleme yöntemiyle seçilen İç Anadolu Bölgesi'nden Konya ilinde, Ege Bölgesi'nden İzmir ilinde ve Akdeniz Bölgesinden Adana ilinde yapılmıştır. Rastgele örnekleme yöntemine göre ana kütledeki bütün birimler homojen olmalı (Karagöz, 2021, s.233) ve bir kişinin seçilmesi diğerinin seçilme olasılığını etkilememelidir (Coşkun ve ark, 2015, s. 139).

Çalışmada hangi şehirden kaç bireye ulaşılması gerektiği tabakalı örnekleme yöntemi kullanılarak belirlenmiştir. Bu yöntemde evren; yaş, cinsiyet, yaşanılan yer gibi gruplara ayrılır ve gruplardan kota (oran) kadar birey seçilir (Aslan 2018). Bu

çalışmada evren nüfusa göre gruplara ayrılmıştır. Nüfus bilgileri tez verilerinin toplandığı 2019 yılına ait verilerden oluşmaktadır. Sonuçlar Çizelge 2.1'de yer almaktadır.

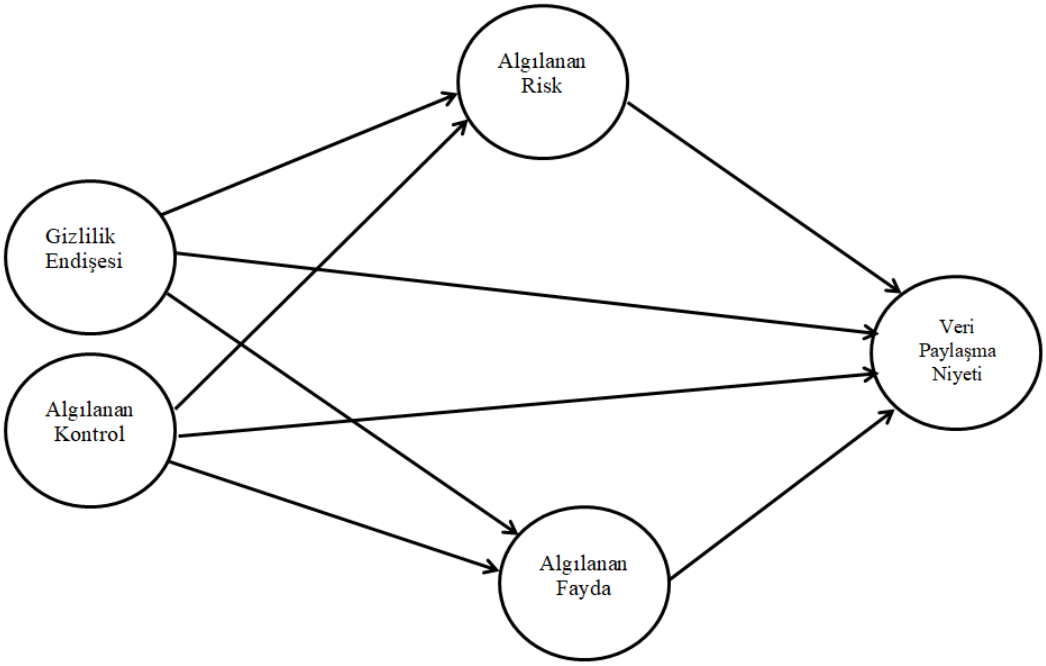
Çizelge 2.1. Örneklem büyüklüğü belirleme.

İl	**2019 Yılı Nüfus Miktarı**	**Kota Oranları**		**KOTA**
İzmir	4 367 251	4 367 251/8 837 565= 0,50	%50	600*%50=300 kişi
Konya	2 232 374	2 232 374/8 837 565=0,25	%25	600*%25=150 kişi
Adana	2.237 940	2 237 940/8 837 565=0,25	%25	600*%25=150 kişi
Toplam	**8 837 565**		**%100**	**600**

Kaynak: İlgili nüfus verileri Türkiye İstatistik Kurumu nüfus sayım bilgilerinden alınmıştır (https://cip.tuik.gov.tr/).

Yukarıdaki çizelgede görüldüğü gibi illerin nüfus miktarının bu üç ilin toplam nüfus miktarına bölünmesi ile kota oranları belirlenmiştir. Daha sonra 600 kişi olarak belirlenen örnek büyüklüğünden her ilden kaç kişinin (kota) çalışmaya dâhil edileceğine karar verilmiştir. Çalışma bu örneklem üzerinden yürütülmüştür. Sonrasında ***rastgele örnekleme yöntemi*** kullanılarak bireylere çevrimiçi olarak ulaşılmıştır. Anket Google Formlar üzerinde düzenlenip çeşitli **sosyal platformlar** (twitter, instagram, facebook, whatsapp, LinkedİN) yoluyla katılımcılara ulaştırılmıştır.

2.6. Araştırmanın Modeli



Şekil 2.1. Araştırmanın modeli.

Araştırmanın modeli Şekil 2.1'de yer almaktadır.

2.7. Araştırmanın Sınırlılıkları

Araştırma Ege Bölgesinden İzmir, İç Anadolu Bölgesinden Konya ve Akdeniz Bölgesinden Adana illeri ile sınırlıdır. Aynı zamanda çalışmanın bulguları, bireylerin kendilerine yöneltilen sorulara verdikleri yanıtlar ile sınırlıdır.

2.8. Araştırma Verilerinin Toplanması

Araştırmayı yapabilmek için ilk olarak Selçuk Üniversitesi Sağlık Bilimleri Fakültesi Etik Kurulundan izin alınmıştır. Daha sonrasında çeşitli sosyal platformlar (twitter, instagram, facebook, whatsapp, LinkedİN) aracılığıyla bireylere çevrimiçi anket uygulanmıştır.

2.9. Araştırma Verilerinin Değerlendirilmesi

Araştırma verilerinin istatistiksel analiz edilmesi için SPSS 26.0 programı ile tanımlayıcı istatistikler (Standart Sapma, Ortalama), güvenilirlik analizi için

Cronbach Alpha ve geçerlilik analizi için AMOS Graphics programı ile doğrulayıcı faktör analizi uygulanmıştır.

2.10. Araştırma Etiği

Araştırma öncesi Selçuk Üniversitesi Sağlık Bilimleri Fakültesi Girişimsel Olmayan Klinik Araştırmalar Etik Kurulundan etik kurul izni (EK-B) alınmıştır. Araştırma izni alındıktan sonra çalışma yürütülmeye başlanmıştır.

Çalışmaya katılım gönüllülük ile gerçekleşmektedir. Bireyler çalışmanın amacı hakkında bilgilendirildikten sonra kendilerinden gönüllü olduklarına dair onam alınmıştır (Ek-C).

2.11. Araştırmanın Soruları ve Hipotezleri

Araştırmanın soruları aşağıda maddeler halinde sunulmuştur.

1. Kişisel sağlık verileri paylaşımında gizlilik endişesi, veri paylaşma niyeti ile negatif yönlü ilişkili midir?
2. Kişisel sağlık verileri paylaşımında gizlilik endişesi ve veri paylaşma niyeti ilişkisinde algılanan risk aracılık rolüne sahip midir?
3. Kişisel sağlık verileri paylaşımında gizlilik endişesi ve veri paylaşma niyeti ilişkisinde algılanan fayda aracılık rolüne sahip midir?
4. Kişisel sağlık verileri paylaşımında algılanan kontrol, veri paylaşma niyeti ile pozitif yönlü ilişkili midir?
5. Kişisel sağlık verileri paylaşımında algılanan kontrol ve veri paylaşma niyeti ilişkisinde algılanan risk aracılık rolüne sahip midir?
6. Kişisel sağlık verileri paylaşımında algılanan kontrol ve veri paylaşma niyeti ilişkisinde algılanan fayda aracılık rolüne sahip midir?

Bu çalışma soruları doğrultusunda oluşturulan araştırma hipotezleri aşağıda verilmiştir;

Hipotez 1. Kişisel sağlık verileri paylaşımında gizlilik endişesi, veri paylaşma niyeti ile negatif yönlü ilişkilidir.

Hipotez 2. Kişisel sağlık verileri paylaşımında gizlilik endişesi ve veri paylaşma niyeti ilişkisinde algılanan risk aracılık rolüne sahiptir.

Hipotez 3. Kişisel sağlık verileri paylaşımında gizlilik endişesi ve veri paylaşma niyeti ilişkisinde algılanan fayda aracılık rolüne sahiptir.

Hipotez 4. Kişisel sağlık verileri paylaşımında algılanan kontrol, veri paylaşma niyeti ile pozitif yönlü ilişkilidir.

Hipotez 5. Kişisel sağlık verileri paylaşımında algılanan kontrol ve veri paylaşma niyeti ilişkisinde algılanan risk aracılık rolüne sahiptir.

Hipotez 6. Kişisel sağlık verileri paylaşımında algılanan kontrol ve veri paylaşma niyeti ilişkisinde algılanan fayda aracılık rolüne sahiptir.

3. BULGULAR

Bu bölümde çalışma kapsamında yapılan analizlerin sonuçlarına ait bulgulara yer verilmiştir.

3.1. Katılımcılara Ait Tanımlayıcı-Betimleyici İstatistikler

Çizelge 3.1. Katılımcılara ait tanımlayıcı veriler.

	Sayı (n)	**Yüzde (%)**
Cinsiyet		
Kadın	274	43,1
Erkek	361	56,9
Yaş Aralığı		
22ve altı	165	26
23-30	245	38,6
31 ve üstü	225	35,4
Öğrenim Düzeyi		
İlköğretim	42	6,6
Lise	128	20,2
Üniversite	354	55,7
Lisansüstü	111	17,5
Annenin Öğrenim Düzeyi		
Okuryazar değil	45	7,1
İlköğretim	416	65,5
Lise	96	15,1
Üniversite	67	10,6
Lisansüstü	11	1,7
Babanın Öğrenim Düzeyi		
Okuryazar değil	28	4,4
İlköğretim	342	53,9
Lise	141	22,2
Üniversite	111	17,5
Lisansüstü	13	2
Yaşanılan Şehir		
İzmir	302	47,6
Konya	183	28,8
Adana	150	23,6
Toplam	**635**	**100**

Araştırmaya katılan bireylere ait demografik veriler Çizelge3.1'de yer almaktadır. Buna göre katılımcıların %43,1(274)'i kadın %56,9(361)'u erkektir. Yaş açısından bakıldığında çalışmaya en çok %38,6(245) ile 22 yaş ve altı bireyler katılmıştır. Bunu takiben %35,4(225) ile 31 yaş ve üstü bireyler ve %26(165) ile 22 yaş ve altı bireyler gelmektedir.

Çalışmaya katılan bireylerin çoğunluğu %55,7 (354) ile üniversite mezunu iken %20,2(128)'si lise, %17,5(111) lisansüstü ve %6,6(42)'sı ise ilköğretim mezunudur. Katılımcıların annelerinin öğrenim düzeyine bakıldığında; %65,5(416) ile çoğunluk ilköğretim mezunu, %15,1(96) ile lise mezunu, %10,6(67) ile üniversite mezunu ve %1,7(11) ile lisansüstü eğitim mezunudur. Ayrıca katılımcılarının anneleri %7,1(45) ile okuryazar değildir.

Katılımcıların babalarının öğrenim düzeyine bakıldığında, annelerin öğrenim düzeyine benzer bir sonuç çıkmaktadır. Bu doğrultuda katılımcıların babaları %53,9(342) ile ilköğretim mezunu, %22,2(141) ile lise mezunu, %17,5(111) üniversite mezunu, %4,4(28) ile okuryazar değil ve %2(13) ile lisansüstü eğitim mezunudur.

Çizelge 3.2. Katılımcılara ait betimleyici istatistikler.

	Sayı(n)	**Yüzde(%)**
E-Nabız Uygulamasını Kullanma Durumu		
Evet	412	64,9
Hayır	223	35,1
Bir Yılda Hastaneye Ortalama Gidiş Sayısı		
Hiç	64	10,1
1-2 kez	245	38,6
3-4 kez	168	26,5
5 kez ve üstü	158	24,9
Hastaneye Parmak İzi Verme Durumu		
Evet	255	40,2
Hayır	380	59,8
Randevu Alırken Kullanılan Yöntem		
182'yi ararım	174	27,4
MHRS- Merkezi Hekim Randevu Sistemi'ne girerim.	296	46,6
Hastaneyi arayarak randevu alırım.	85	13,4
Sağlık kuruluşunun çevrimiçi randevu uygulamasından randevu alırım.	80	12,6
Bir Günde İnternette Geçirilen Süre		
3 saat ve altı	209	32,9
4-6 saat	261	41,1
7 saat ve üstü	165	26
Hastalık Geçmişini Her Sağlık Kuruluşundaki Hekimin Görmesinin Veri Açığı Olup Olmamasına Dair Görüş		
Evet	131	20,6
Hayır	333	52,4
Kararsızım	171	26,9
Toplam	**635**	**100**

Bireylere ait betimleyici istatistikler Çizelge3.2'de yer almaktadır. Buna göre çalışmaya katılan bireylerin %64,9(412)'u e nabız uygulamasını kullanırken %35,1'i kullanmamaktadır. Bir yılda hastaneye gidiş sayısına bakıldığında, katılımcılar sırasıyla %38,6(245) ile en çok 1-2 kez, %26,5(168) ile 3-4 kez, %24,9(158) ile 5 kez ve üstü hastane gitmektedir. Ayrıca katılımcıların %10,1(64)'i bir yılda hastaneye hiç gitmemektedir.

Katılımcıların %59,8(380)'i herhangi bir hastaneye parmak izi vermemişken %40,2(255)'si parmak izi vermiştir. Randevu alırken kullanılan yönteme

bakıldığında, katılımcıların %46,6(296)'sı MHRS-Merkezi Hekim Randevu Sistemi'ne girmekte, %27,4(174)'ü 182'yi aramakta, %13,4(85)'ü hastaneyi aramakta ve %12,6(80)'sı sağlık kuruluşunun çevrimiçi randevu sitesine girmektedir.

Araştırmaya katılan bireyler bir günde internette en az %26(165) ile 7 saat ve üstü, en çok %41,1(261) ile 4-6 saat arasında vakit geçirmektedir. Ayrıca katılımcıların %32,9(209)'u bir günde internette 3 saat ve altı vakit geçirmektedir. Hastalık geçmişini her sağlık kuruluşundaki hekimin görmesinin veri açığı olup olmamasına dair görüşe bakıldığında, katılımcıların %52,4(333)'ü hayır, %26,9(171)'ü kararsızım ve %20,6(131)'sı evet cevabını vermiştir.

3.2. Ölçek Maddelerine Ait Tanımlayıcı İstatistikler

Tablo 3.1. Ölçek maddelerine ait tanımlayıcı istatistikler.

Gizlilik Endişesi Ölçeği	$\bar{x}$	*ss*
Sağlık kuruluşlarında kişisel bilgilerimi paylaşmam noktasında belirsizlikler mevcuttur.	3,01	1,13
Sağlık kuruluşlarında kişisel bilgilerimin paylaşım esnasında kaybolma ihtimali yüksektir.	3,01	1,22
Sağlık kuruluşları ile paylaştığım kişisel bilgilerimin kötüye kullanılma ihtimali vardır.	2,89	1,24
Sağlık kuruluşlarında paylaşılan bilgiler siber saldırılar gibi birçok sorun içermektedir.	3,12	1,25
Algılanan Kontrol Ölçeği	$\bar{x}$	*ss*
Sağlık kuruluşlarında sağlık personeli ile teşhis ve tedavi işlemleri sırasında paylaşılacak bilgilerin neler olduğunun farkındayım.	3,84	1,06
Sağlık personeli ile iletişimim sırasında toplanan bilgilerimin sağlık personeli tarafından nasıl kullanılacağını kontrol ettiğime inanıyorum.	3,31	1,19
Tedavi sürecinde verdiğim bilgileri daha sonra doğrulayabileceğime yani veriyi paylaştıktan sonra düzeltebileceğime inanıyorum.	3,51	1,16
Algılanan Risk Ölçeği	$\bar{x}$	*ss*
Kişisel bilgilerimin e-nabız gibi mobil uygulamalarla paylaşılması beklenmedik problemleri beraberinde getirebilir.	3,86	1,66
Kişisel bilgilerimi e-nabız gibi mobil uygulamalarda paylaşmak üçüncü kişilerin erişimi açısından risk içermektedir.	4,20	1,80
Kişisel bilgilerimin veri aktarımı sürecindeki kayıp potansiyeli yüksektir.	3,89	1,73
Algılanan Fayda Ölçeği	$\bar{x}$	*ss*
Sağlık personeli ile veri paylaşmak ve e-sağlık uygulamalarını kullanmak, ihtiyacım olan sağlık bilgilerimi bulmak için arama süremi kısaltır.	5,42	1,51
Sağlık personeli ile veri paylaşmak ve e-sağlık uygulamalarını kullanmak ihtiyaç duyduğum sağlık bilgilerime anında ulaşma kolaylığı sağlar.	5,61	1,38
Genel olarak, sağlık personeli ile veri paylaşmanın ve e-sağlık uygulamalarını kullanmanın faydalı olduğunu düşünüyorum.	5,43	1,42
Veri Paylaşma Niyeti Ölçeği	$\bar{x}$	*ss*
Sağlık personeli ile kişisel bilgilerimi paylaşma ihtimalim var.	5,04	1,62
Sağlık personeli ile kişisel bilgilerimi paylaşırım.	4,92	1,76
Sağlık personeli ile ürün ve hizmet gelişimi için kişisel bilgilerimin paylaşılması benim için genellikle mümkündür.	4,82	1,70

Tablo 3.1'de görüldüğü gibi Sun ve ark(2019) gizlilik endişesi ölçeği 4 sorudan, Li ve ark(2017) algılanan kontrol ölçeği 3 sorudan, Xu ve ark(2011) algılanan risk ölçeği 3 sorudan, Xu ve ark(2011) algılanan fayda ölçeği 3 sorudan ve Xu ve ark(2011) veri paylaşma niyeti ölçeği 3 sorudan oluşmaktadır. Tabloya göre gizlilik endişesi ölçeğinde en yüksek puan "Sağlık kuruluşlarında paylaşılan bilgiler siber saldırılar gibi birçok sorun içermektedir." (3,12±1,25) ifadesine; en düşük puan ise "Sağlık kuruluşlarında kişisel bilgilerimi paylaşmam noktasında belirsizlikler mevcuttur."(3,01±1,22) ifadesine aittir.

Algılanan kontrol ölçeğine göre en yüksek puan "Sağlık kuruluşlarında sağlık personeli ile teşhis ve tedavi işlemleri sırasında paylaşılacak bilgilerin neler olduğunun farkındayım." (3,84±1,06) ifadesine; en düşük puan "Sağlık personeli ile iletişimim sırasında toplanan bilgilerimin sağlık personeli tarafından nasıl kullanılacağını kontrol ettiğime inanıyorum." (3,31±1,19) ifadesine aittir.

Algılanan risk ölçeğine bakıldığında, "Kişisel bilgilerimi e-nabız gibi mobil uygulamalarda paylaşmak üçüncü kişilerin erişimi açısından risk içermektedir." (4,20±1,80) ifadesi en yüksek; "Kişisel bilgilerimin e-nabız gibi mobil uygulamalarla paylaşılması beklenmedik problemleri beraberinde getirebilir." (3,86±1,66) ifadesi en düşük puana sahiptir.

Algılanan fayda ölçeğinde en yüksek puan "Sağlık personeli ile veri paylaşmak ve e-sağlık uygulamalarını kullanmak ihtiyaç duyduğum sağlık bilgilerime anında ulaşma kolaylığı sağlar." (5,61±1,38) ifadesine; en düşük puan "Sağlık personeli ile veri paylaşmak ve e-sağlık uygulamalarını kullanmak, ihtiyacım olan sağlık bilgilerimi bulmak için arama süremi kısaltır." (5,42±1,51) ifadesine aittir.

Son olarak veri paylaşma niyeti ölçeğine bakıldığında ise en yüksek puan "Sağlık personeli ile kişisel bilgilerimi paylaşma ihtimalim var." (5,04±1,62) ifadesine; en düşük puan "Sağlık personeli ile ürün ve hizmet gelişimi için kişisel bilgilerimin paylaşılması benim için genellikle mümkündür." (4,82±1,70) ifadesine aittir.

3.3. Normal Dağılım Analizi

Çalışmada ölçeklerin normal dağılıma uygun olup olmadığı araştırılmıştır. Elde edilen veriler tablo 3.2'de gösterilmektedir.

Tablo 3.2. Ölçeklerin normal dağılım değerleri

	Skewness	**Kurtosis**
Gizlilik Endişesi Ölçeği	0,05	-0,56
Algılanan Kontrol Ölçeği	-0,32	-0,24
Algılanan Risk Ölçeği	-0,02	-0,72
Algılanan Fayda Ölçeği	-0,60	-0,12
Veri Paylaşma Niyeti Ölçeği	-0,49	-0,35

Normal dağılıma uygunluğun belirlenebilmesi için Skewness ve Kurtosis değerleri incelenmiştir. Bu değerler -1 ve +1 arasında yer alıyorsa eğer normal dağılıma uyduğu söylenebilmektedir (Hair ve ark 2013). Bu doğrultuda Tablo 3.2'ye bakıldığında ölçeklerin normal dağılıma uygunluk gösterdiği görülmektedir.

3.4. Ölçeklerin Geçerlik ve Güvenirliğine Ait Bulgular

Araştırmada kullanılan ölçeklerin geçerlik ve güvenirlikleri doğrulayıcı faktör analizi ile incelenmiştir.

Yapılan doğrulayıcı faktör analizi sonucunda $\chi 2/df$ oranı, RMSEA, GFI, AGFI, CFI ve NFI indeksleri elde edilmiştir. Elde edilen bu indekslere bakılarak ölçeğin kabul edilebilir değerlere sahip olup olmadığı belirlenebilmektedir. Sonuçlara göre eğer ölçek kabul edilebilir uyum değerlerine sahip değilse düzeltme indeksi veren sorular ölçekten silinmektedir veya modification indices önerilerine göre işlem yapılmaktadır. Gerekli sorular silindikten ve modifikasyonlar yapıldıktan sonra kalan sorular tekrar analize tabi tutulmakta ve bu işlem kabul edilebilir uyum değerlerini elde edene kadar devam etmektedir.

Literatürde; $\chi 2/df$ oranının <5 olması durumunda kabul edilebilir olduğu, < 3 olması durumunda ise iyi uyum olduğu belirtilmektedir. RMSEA değeri $0 \leq RMSEA \leq 0,05$ arasında iyi uyum, $0,05 < RMSEA \leq 0,10$ arasında kabul edilebilir uyum

göstermektedir (Bagozzi 1981; Browne ve Cudeck 1993). GFI değerinin 0,90 ≤ GFI ≤ 1,00 aralığı iyi uyumu, 0,85 ≤ GFI < 0,90 aralığı kabul edilebilir uyumu temsil etmektedir (Li ve ark 2005, Hooper ve ark 2008). AGFI değeri 0,90 ≤ AGFI ≤1,00 arasında iyi uyum, 0,85 ≤ AGFI < 0,90 arasında ise kabul edilebilir uyum olarak ifade edilmektedir (Hooper ve ark 2008). CFI değeri için 0,97 ≤ CFI ≤ 1,00 arasında iyi uyum ve 0,95 ≤ CFI < 0,97 değerleri kabul edilebilir uyum göstermektedir (Steiger 2007). NFI değeri 0,95 ≤ NFI ≤ 1,00 arasında iyi uyum, 0,90 ≤ NFI < 0,95 kabul edilebilir uyum olarak ifade edilmektedir (Bentler 1990). Özetle aşağıdaki Tablo 3.3'te verilmiştir.

Tablo 3.3. Doğrulayıcı faktör analizi kabul edilebilir uyum ve iyi uyum değer aralıkları.

Model Uyum Kriteri	**İyi Uyum**	**Kabul Edilebilir Uyum**
CMIN/df	X^2/sd < 3	X^2/sd < 5
RMSEA	0 ≤ RMSEA≤ 0,05	0,05 < RMSEA ≤ 0,10
GFI	0.90 ≤ GFI ≤ 1.00	0,85 ≤ GFI < 0,90
AGFI	0.90 ≤ AGFI ≤1.00	0,85 ≤ AGFI < 0,90
CFI	0,97 ≤ CFI ≤ 1.00	0,95 ≤ CFI < 0,97
NFI	0,95 ≤ NFI ≤ 1.00	0,90 ≤ NFI < 0,95

Kaynak: Li ve ark (2005); Bagozzi (1981); Browne ve Cudeck (1993); Steiger (2007); Hooper ve ark (2008); Bentler (1990)'dan uyarlanmıştır.

3.4.1. Doğrulayıcı Faktör Analizi Sonuçları

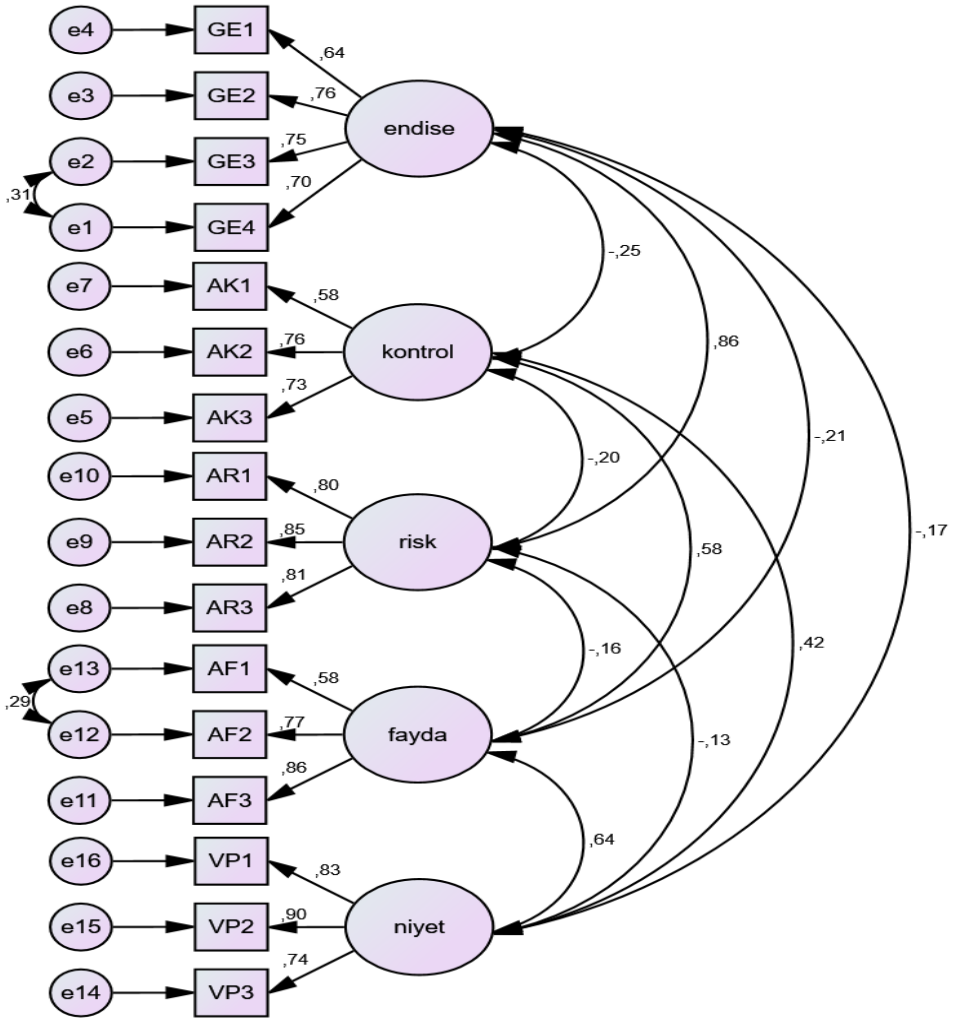
Çizelge 3.3. Modele ait doğrulayıcı faktör analizi sonuçları.

Sorular	STD estimate (faktör yükü)*	STD estimate (faktör yükü)*	Estimate	SE	t Değeri (CR= estimate/SE)	Cronbach Alpha	AVE	Arit. Ort.	Std. Hata
Gizlilik Endişesi						0,823	0,51		
1.	0,632	0,644	1,000					3,01	1,125
2.	0,736	0,763	1,279	0,083	15,321			3,01	1,215
3.	0,810	0,755	1,289	0,085	15,085			2,89	1,237
4.	0,761	0,763	1,201	0,085	14,152			3,12	1,249
Algılanan Kontrol						0,824	0,49		
1.	0,577	0,576	1,000					3,84	1,059
2.	0,759	0,761	1,476	0,122	12,052			3,31	1,185
3.	0,729	0,728	1,385	0,116	11,970			3,51	1,162
Algılanan Risk						0,861	0,68		
1.	0,803	0,804	1,000					3,86	1,661
2.	0,851	0,850	1,149	0,050	22,943			4,20	1,804
3.	0,813	0,813	1,053	0,048	21,877			3,89	1,730
Algılanan Fayda						0,807	0,56		
1.	0,668	0,583	1,000					5,42	1,513
2.	0,839	0,770	1,202	0,075	15,928			5,61	1,377
3.	0,796	0,856	1,374	0,107	12,870			5,43	1,416
Veri Paylaşma Niyeti						0,862	0,68		
1.	0,831	0,832	1,000					5,04	1,624
2.	0,904	0,902	1,174	0,048	24,552			4,92	1,756
3.	0,740	0,741	0,930	0,046	20,418			4,82	1,695

*Faktör yükü tüm faktörler için $p < 0.001$.

Araştırma kapsamında oluşturulan modelde 5 farklı ölçek kullanılmıştır. Ölçeklerin güvenirliklerine Cronbach Alpha değeri ve AVE katsayısı ile bakılmıştır. Elde edilen veriler Çizelge 3.3'te yer almaktadır. Buna göre çalışmada kullanılan ölçeklerin güvenilir değerlere sahip olduğu görülmektedir.

Ölçeklere "Confirmative Factor Analysis (CFA) - Doğrulayıcı Faktör Analizi" uygulanmış ve başlangıç versiyonunda kabul edilebilir uyum değerlerine ulaşılmıştır *(Goodness-of-Fit Statistics: χ2/df=2,759, NFI= .947, CFI=.965, AGFI=.926, GFI=.949, RMSEA=.053)* Modelin iyi uyum değerlerine ulaşabilmesi için hata terimleri arasında kurulması önerilen kovaryans oluşturulup model yeniden çalıştırılmıştır. Bu doğrultuda iyi uyum değerlerine sahip bir model elde edilmiştir *(Goodness-of-Fit Statistics: χ2/df =2,196, NFI= .958, CFI=.977, AGFI=.943, GFI=.961, RMSEA=.043)* AMOS Graphics programı ile yapılan doğrulayıcı faktör analizi modeli şekil 3.1'de yer almaktadır.



Şekil 3.1. Doğrulayıcı faktör analizi modeli

3.4.2. Korelasyon Analizi Sonuçları

Araştırmada değişkenler arası ilişkiler korelasyon analiziyle araştırılmıştır. Sonuçlar Çizelge3.4'te gösterilmektedir.

Çizelge 3.4. Korelasyon analizi.

	Art. Ort.	**Std. Hata**	**1**	**2**	**3**	**4**
1	3,01	0,98				
2	3,55	0,91	-0,19**			
3	3,98	1,53	0,71**	-0,17**		
4	5,49	1,22	-0,12**	0,44**	-0,08*	
5	4,93	1,50	-0,15**	0,37**	-0,13**	0,52**

** Correlation is significant at the 0.01 level (2-tailed).
* Correlation is significant at the 0.05 level (2-tailed).
(1=Gizlilik Endişesi, 2=Algılanan Kontrol, 3=Algılanan Risk, 4=Algılanan Fayda, 5=Veri Paylaşma Niyeti)

Çizelge x'de verilen değişkenler arasındaki ilişkinin tespit edilmesi için yapılan korelasyon analizi sonucunda, veri paylaşma niyeti ile gizlilik endişesi ($r=-0,15$; $p<0,01$) ve algılanan risk ($r=-0,13$; $p<0,01$) arasında negatif bir ilişki, veri paylaşma niyeti ile algılanan kontrol ($r=0,37$; $p<0,01$) ve algılanan fayda ($r=0,52$; $p<0,01$) arasında pozitif bir ilişki bulunmuştur.

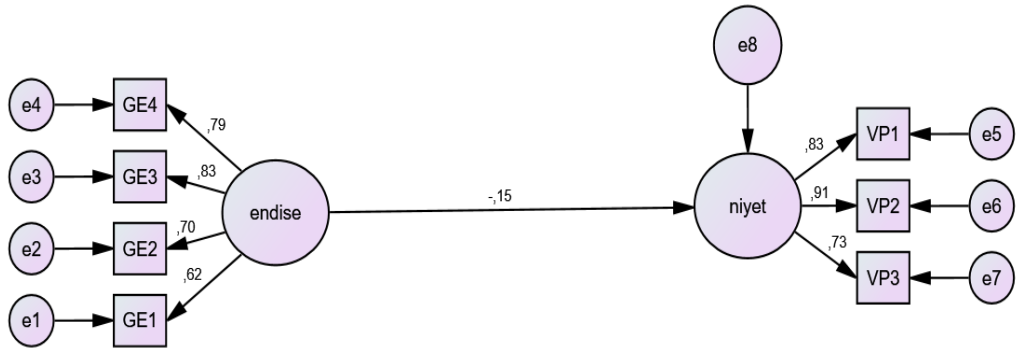
Algılanan fayda ile gizlilik endişesi ($r=-0,12$; $p<0,01$) ve algılanan risk ($r=-0,08$; $p<0,05$) arasında negatif bir ilişki, algılanan fayda ile algılanan kontrol arasında pozitif bir ilişki ($r=0,44$; $p<0,01$) tespit edilmiştir Ayrıca algılanan risk ile gizlilik endişesi arasında pozitif bir ilişki ($r=0,70$; $p<0,01$), algılanan risk ile algılanan kontrol arasında negatif bir ilişki ($r=-0,17$; $p<0,01$) ve algılanan kontrol ile gizlilik endişesi arasında negatif bir ilişki ($r=0,19$; $p<0,01$) bulunmuştur.

3.4.3. Yapısal Eşitlik Modeli

Çalışmada değişkenler arasındaki ilişkiyi belirlemek için AMOS Graphics programıyla yapısal eşitlik modeli (structural equation model) uygulanmıştır.

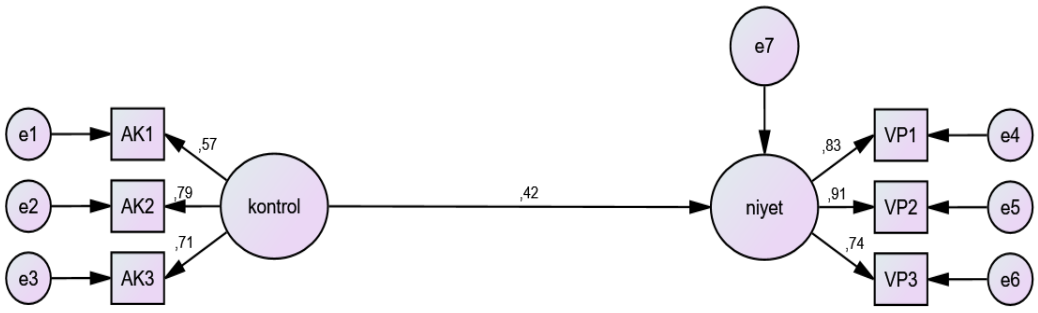
3.4.3.1. Yol (Path) Analizi Sonuçları

Yol (path) analizi sonuçları aşağıdaki gibidir:



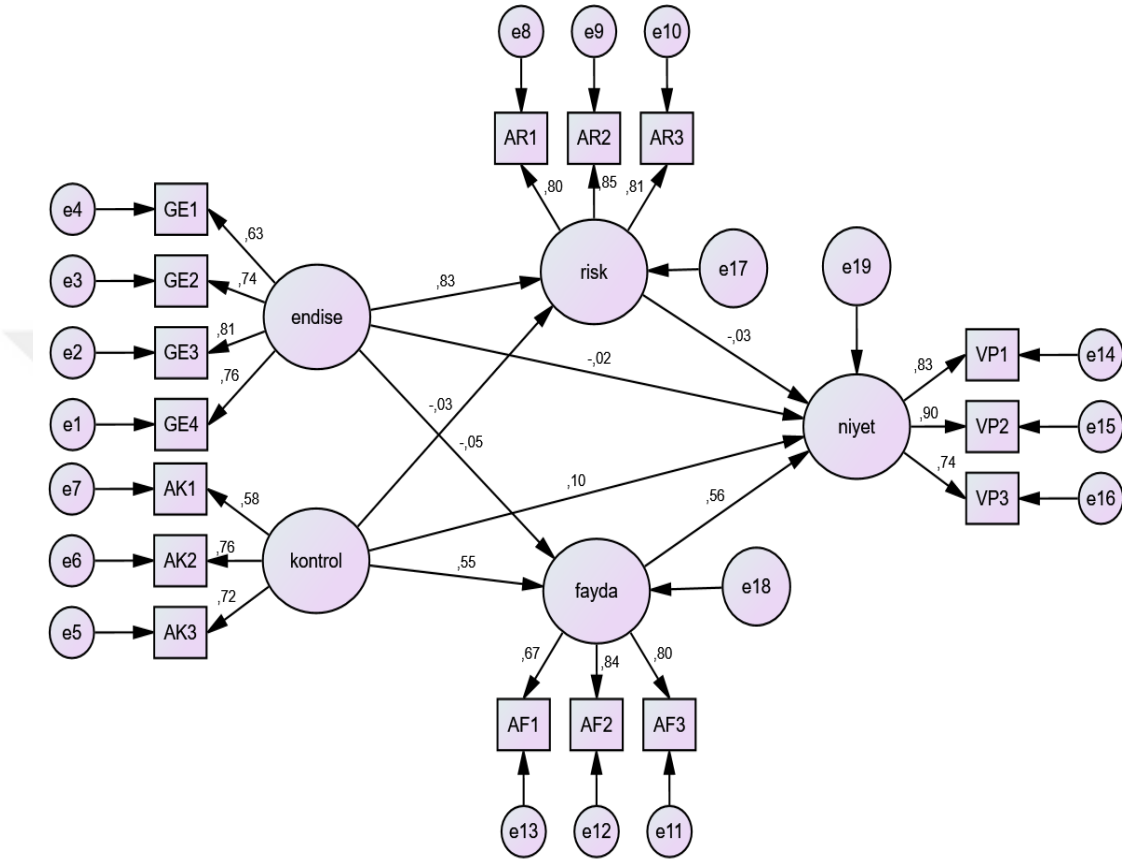
Şekil 3.2. Gizlilik endişesi ve veri paylaşma niyeti ilişkisine yönelik yol analizi ilk aşama.

İlk aşamada gizlilik endişesi ile veri paylaşma niyeti arasındaki ilişki tek başına yol analizi yapılarak belirlenmiştir. Bu analiz sonucunda gizlilik endişesi ile veri paylaşma niyeti arasında yol katsayısı -0,15 olarak bulunmuştur. Bu sonuç aracı değişken sonucunun ilkini karşılamakta olup ilişkinin olabileceğini belirtmektedir.



Şekil 3.3. Algılanan kontrol ve veri paylaşma niyeti ilişkisine yönelik yol analizi ilk aşama.

İlk aşamada algılanan kontrol ile veri paylaşma niyeti arasındaki ilişki tek başına yol analizi yapılarak belirlenmiştir. Bu analiz sonucunda algılanan kontrol ile veri paylaşma niyeti arasında yol katsayısı 0,42 olarak bulunmuştur. Bu sonuç aracı değişken sonucunun ilkini karşılamakta olup ilişkinin olabileceğini belirtmektedir.

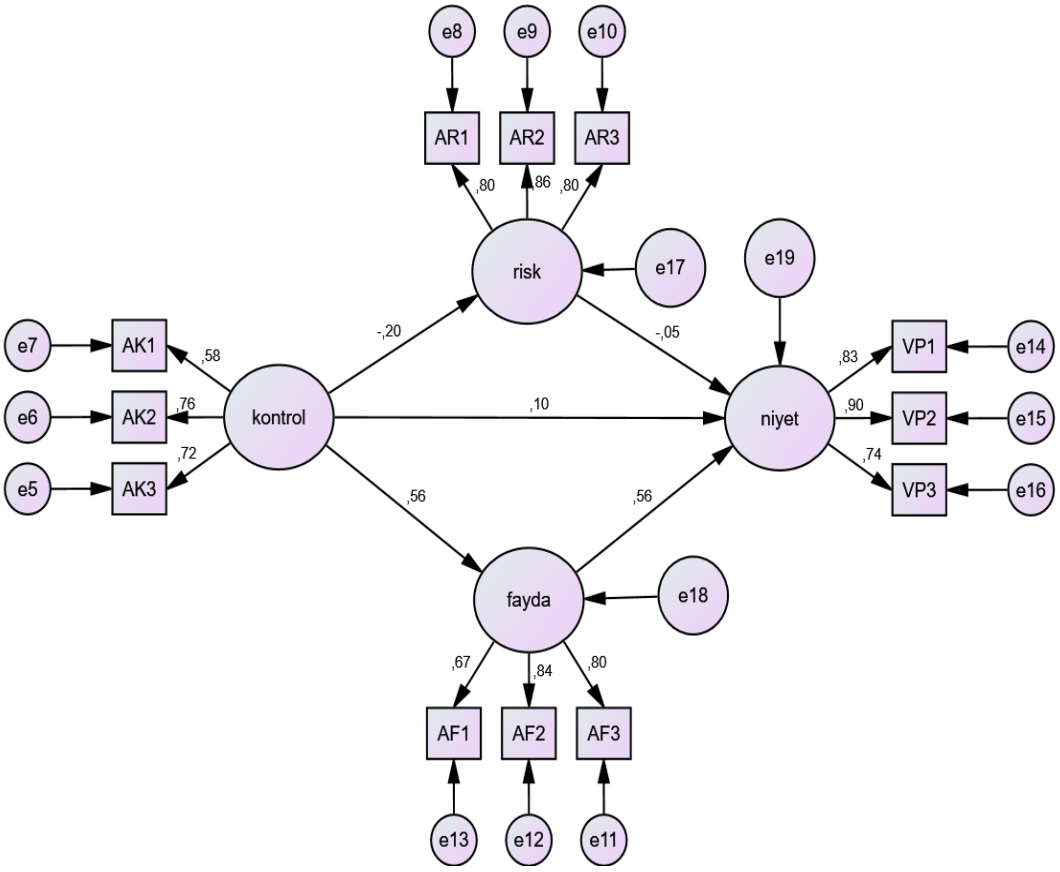


Şekil 3.4. Gizlilik endişesi ve algılanan kontrol ile veri paylaşma niyeti arasındaki ilişkide algılanan fayda ve algılanan riskin aracı rolünü incelemeye ilişkin yol (path) analizi sonuç modeli.

Sonraki aşamada gizlilik endişesi ve algılanan kontrol ile veri paylaşma niyeti arasındaki ilişkide algılanan risk ve algılanan faydanın aracılık rolünü belirlemek için yol analizleri yapılmıştır. Analize ait yol modeli şekil 3.4'te yer almaktadır. Yapılan analizler sonucunda algılanan fayda ile veri paylaşma niyeti (0,56; $p<0,01$) ve algılanan kontrol arasında (0,55; $p<0,01$), algılanan risk ile veri paylaşma niyeti (-0,03; $p<0,01$) ve algılanan kontrol (-0,03; $p<0,01$) arasında anlamlı ilişki tespit edilmiştir. Ayrıca ilk aşamada algılanan kontrol ve veri paylaşma niyeti arasında anlamlı ilişkisi olmasına rağmen modelde bu ilişki bulunamamıştır (0,10; $p>0,05$). Bu durumda algılanan faydanın algılanan kontrol ile veri paylaşma niyeti arasındaki

ilişkide aracılık etkisinden söz edilebilmektedir. Ayrıca çağdaş yaklaşımlarda aracılık etkisi bakılabilmesi için bootstrap yöntemi kullanılmaktadır. Bu yönteme göre bootstrap üst ve alt değerleri arasında 0 (sıfır) bulunmuyorsa aracılık etkisinden söz edilebilirken, 0 (sıfır) bulunuyorsa aracılık etkisinden söz edilememektedir (Hayes 2018). Buna göre modelin bootstrap değerlerine bakıldığında algılanan kontrol ile veri paylaşma niyeti arasındaki ilişkide algılanan risk ve algılanan faydanın aracılık rolü vardır (0,23; 0,402).

Gizlilik endişesi ve algılanan risk (0,83; p<0,01) arasında anlamlı ilişki bulunmuştur. Fakat algılanan risk ile veri paylaşma niyeti arasında (-0,03; p>0,05), gizlilik endişesi ile veri paylaşma niyeti arasında (-0,02; p>0,05) ve gizlilik endişesi ile algılanan fayda arasında (-0,05; p>0,05) anlamlı bir ilişki tespit edilememiştir. Modelin bootstrap değerlerine göre gizlilik endişesi ile veri paylaşma niyeti arasındaki ilişkide algılanan riskin ve algılanan faydanın aracılık rolü yoktur (-0,20; 0,134).



Şekil 3.5. Oluşturulan yeni yol modeli.

Oluşturulan yeni modele göre algılanan kontrol ile algılanan fayda arasında (0,75; p<0,01), algılanan fayda ile veri paylaşma niyeti arasında (0,56; p<0,01) ve algılanan kontrol ile algılanan risk arasında (-0,20; p<0,05) anlamlı bir ilişki tespit edilmiştir. Algılanan risk ile veri paylaşma niyeti arasında (-0,05; p>0,05) ve algılanan kontrol ile veri paylaşma niyeti arasında (0,10; p>0,05) anlamlı bir ilişki bulunamamıştır.

Modelin iyi uyum değerlerine bakıldığında *(Goodness-of-Fit Statistics: χ2/df =2,66, NFI=.962, CFI=.976, AGFI=.98, GFI=.945, RMSEA=.05)* modelin iyi uyum değerlerine sahip olduğu ve kabul edilebilir olduğu söylenebilmektedir.

3.4.4. Hipotez Yorumları

Tablo 3.4. Hipotez yorumları.

Hipotezler	**Kabul/Red**
Hipotez 1. Kişisel sağlık verileri paylaşımında gizlilik endişesi, veri paylaşma niyeti ile negatif yönlü ilişkilidir.	**Kabul**
Hipotez 2. Kişisel sağlık verileri paylaşımında gizlilik endişesi ve veri paylaşma niyeti ilişkisinde algılanan risk aracılık rolüne sahiptir.	**Red**
Hipotez 3. Kişisel sağlık verileri paylaşımında gizlilik endişesi ve veri paylaşma niyeti ilişkisinde algılanan fayda aracılık rolüne sahiptir.	**Red**
Hipotez 4. Kişisel sağlık verileri paylaşımında algılanan kontrol, veri paylaşma niyeti ile pozitif yönlü ilişkilidir.	**Kabul**
Hipotez 5. Kişisel sağlık verileri paylaşımında algılanan kontrol ve veri paylaşma niyeti ilişkisinde algılanan risk aracılık rolüne sahiptir.	**Kabul**
Hipotez 6. Kişisel sağlık verileri paylaşımında algılanan kontrol ve veri paylaşma niyeti ilişkisinde algılanan fayda aracılık rolüne sahiptir.	**Kabul**

4. TARTIŞMA

Literatüre bakıldığında algılanan fayda gizlilik endişelerini azaltmakta (Cocosila ve Archer 2014, Emani 2012) ve kişisel sağlık verilerini paylaşma niyetini olumlu yönde etkilemektedir (Park ve ark 2011). Araştırma sonuçları da literatürdeki bu bulguyu destekler niteliktedir. Buna göre de algılanan fayda, gizlilik endişesi negatif yönlü ilişkili ve veri paylaşma niyeti pozitif yönlü ilişkili bulunmuştur.

Yapılan çalışmalarda bir bireyin gizlilik endişelerinin, kişisel bilgileri paylaşıp paylaşmama niyeti noktasında bir karar sürecine girmesine sebep olduğu sonucuna ulaşılmıştır (Awad ve Krishnan 2016, Belanger ve ark 2002, Culnan ve Armstrong 1998, Culnan ve Bies 2003, Dinev ve Hart 2005, Malhotra ve ark 2014). Bu çalışmada da benzer sonuçlar elde edilmiştir. Buna göre gizlilik endişesi ile veri paylaşma niyeti arasında negatif yönlü bir ilişki vardır. Bireylerin kişisel veri paylaşımında gizlilik endişesi düzeyleri arttıkça veri paylaşımı niyetleri azalmaktadır.

Çalışmada algılanan kontrol ile veri paylaşma niyeti arasında pozitif yönde bir ilişki tespit edilmiştir. Bandura (1977) benzer bir şekilde, algılanan öz-yeterlik üzerine yaptığı çalışmalarda, sağlık verileri paylaşma davranışının önemli bir belirleyicisi olarak algılanan kontrolü ele almış ve kontrol düzeyinin veri paylaşma niyeti üzerinde olumlu etkisi olduğunu vurgulamıştır.

Cruickshank ve ark (2012) tarafından İngiltere'de yaşayan bireylerin kişisel sağlık bilgi sistemlerinikullanımı ile ilgili yapılan bir çalışmaya göre; sağlık kurumlarında tedavi gören 172 farklı hastanın %92.3'ü verilere yetkisiz kişiler tarafından erişim sağlanmasını ve verilerin güvenliğini en büyük sorun olarak ele almaktadır. Dhagarra ve ark (2020) tarafından yapılan bir çalışmada bireylerin kişisel sağlık verileri paylaşımında teknoloji kabul düzeylerinin ölçülmesi amaçlanmış ve çalışmada algılanan fayda, algılanan kullanım kolaylığı, güven ve gizlilik endişesinin sağlık teknolojilerini kullanma ve bilgi paylaşma ile ilişkili olduğu bulunmuştur. Bansal ve ark'a (2010) göre kişisel sağlık verilerinde algılanan gizlilik riski, bilginin kontrolünde olmak, bilgi alışverişinin güvenliği ve bu bilgiyi toplayanın kurallara uygun davranıp davranmayacağı ile ilgilidir (Bansal ve ark 2010). Çalışmada da

algılanan kontrol ile algılanan risk arasında negatif yönlü bir ilişki ve algılanan kontrol ile algılanan fayda arasında pozitif yönlü bir ilişki bulunmuştur.

Araştırmada bireylerin gizlilik endişeleri ile algılanan risk düzeyleri arasında anlamlı bir ilişki tespit edilmiştir. Benzer bir şekilde, Xu ve ark (2008) tarafından sağlık hizmetlerinde bireylerin gizlilik endişelerinin oluşumunu incelemek için yapılan çalışmada, algılanan risk ile gizlilik endişesi arasında anlamlı bir ilişki bulunmuştur. Xu ve ark (2011b) tarafındanyapılan bir diğer çalışmada da sağlık hizmetlerinde bireylerin veri paylaşımında algıladıkları riskler ile gizlilik endişeleri arasında anlamlı bir ilişki bulunmuştur.

Çalışmada kişisel sağlık verileri paylaşma niyeti ile gizlilik endişesi arasındaki ilişkide algılanan risk ve algılanan faydanın aracılık etkisinin olmadığı tespit edilmiştir. Literatüre bakıldığında, gizlilik endişesi ve veri paylaşma niyeti arasında algılanan risk ve faydanın aracılık rolünün olmadığı ama veri paylaşım şeffaflığının aracılık rolü olduğu belirlenmiştir (Awad ve Krishnan 2006).

Çalışmada kişisel sağlık verileri paylaşma niyeti ile algılanan kontrol arasındaki ilişkide algılanan risk ve algılanan faydanınn aracılık rolü olduğu tespit edilmiştir. Lee ve Rao (2007) tarafından yapılan bir çalışmada, veri paylaşma niyeti ile algılanan kontrol arasındaki ilişkide algılanan risk, algılanan fayda ve algılanan kalitenin aracılık rolü olduğu tespit edilmiştir.

5. SONUÇ VE ÖNERİLER

Çalışmada kişisel sağlık verileri paylaşım niyeti ile gizlilik endişesi ve algılanan kontrol ilişkisinde algılanan risk ve algılanan faydanın aracı rolünün araştırılması amaçlanmıştır. Bu doğrultuda çalışmada elde edilen bulgulara ait sonuçlar aşağıda verilmiştir.

5.1. Sosyo-demografik Verilere İlişkin Sonuçlar

- Çalışmaya katılan bireylerden toplanan verilere ilişkin sosyo-demografik bulguların sonuçlarına göre, katılımcıların %56,9 (361)'unun kadın, %38,6 (245)'sının 22 yaş ve altı, %55,7 (354)'snin üniversite mezunu olduğu ve %47,6 (302)'sının İzmir'de yaşamakta olduğu belirlenmiştir.

- Katılımcıların %59,8 (380)'inin herhangi bir hastaneye parmak izi vermediği, %38,6 (245)'sının bir yılda hastaneye 1-2 kez gittiği, %64,9 (412)'unun e-Nabız uygulamasını kullandığı ve %41,1 (261)'inin bir günde internette 4-6 saat vakit geçirdiği sonucuna ulaşılmıştır.

5.2. Araştırmanın Hipotezlerine Ait Sonuçlar

- Çalışmada kişisel sağlık verilerinin paylaşımında gizlilik endişesi ile veri paylaşma niyeti arasında negatif yönlü anlamlı bir ilişki tespit edilmiştir. Buna göre bireylerin kişisel sağlık verilerini paylaşımında gizlilik endişeleri arttıkça veri paylaşma niyetleri de azalmakta ve verilerini paylaşmamaktadırlar. Bu nedenle hipotez 1 *(Kişisel sağlık verileri paylaşımında gizlilik endişesi, veri paylaşma niyeti ile negatif yönlü ilişkilidir.)* kabul edilmiştir.

- Kişisel sağlık verilerinin paylaşımında gizlilik endişesi ile veri paylaşma niyeti arasındaki ilişkide algılanan riskin aracılık rolü bulunamamıştır. Bu nedenle hipotez 2 *(Kişisel sağlık verileri paylaşımında gizlilik endişesi ve veri paylaşma niyeti ilişkisinde algılanan risk aracılık rolüne sahiptir.)* reddedilmiştir.

- Kişisel sağlık verilerinin paylaşımında gizlilik endişesi ile veri paylaşma niyeti arasındaki ilişkide algılanan faydanın aracılık rolü bulunamamıştır. Bu nedenle hipotez 3 *(Kişisel sağlık verileri paylaşımında gizlilik endişesi ve veri paylaşma niyeti ilişkisinde algılanan fayda aracılık rolüne sahiptir.)* reddedilmiştir.

- Çalışmada kişisel sağlık verilerinin paylaşımında algılanan kontrol ile veri paylaşma niyeti arasında pozitif yönlü anlamlı bir ilişki tespit edilmiştir. Buna göre bireylerin kişisel sağlık verilerini paylaşımında algılanan kontrol düzeyleri arttıkça veri paylaşma niyetleri de artmakta ve verilerini paylaşmaktadırlar. Bu nedenle hipotez 4*(Kişisel sağlık verileri paylaşımında algılanan kontrol veri paylaşma niyeti ile pozitif yönlü ilişkilidir.)* kabul edilmiştir.

- Kişisel sağlık verilerinin paylaşımında algılanan kontrol ile veri paylaşma niyeti arasındaki ilişkide algılanan riskin aracılık rolünün olduğu saptanmıştır. Buna göre algılanan risk algılanan kontrol düzeyini azalttığı için veri paylaşma niyetini olumsuz yönde etkilemektedir. Bu nedenle hipotez 5 *(Kişisel sağlık verileri paylaşımında algılanan kontrol ve veri paylaşma niyeti ilişkisinde algılanan risk aracılık rolüne sahiptir.)* kabul edilmiştir.

- Kişisel sağlık verilerinin paylaşımında algılanan kontrol ile veri paylaşma niyeti arasındaki ilişkide algılanan faydanın aracılık rolünün olduğu saptanmıştır. Buna göre algılanan fayda algılanan kontrol düzeyini arttırdığı için veri paylaşma niyetine katkıda bulunmaktadır. Bu nedenle hipotez 5 *(Kişisel sağlık verileri paylaşımında algılanan kontrol ve veri paylaşma niyeti ilişkisinde algılanan risk aracılık rolüne sahiptir.)* kabul edilmiştir.

5.3. Öneriler

- Yapılan araştırma İzmir, Konya ve Adana illerinde gerçekleştirilmiştir. Diğer şehirlerdeki durumları da belirleyebilmek için çalışmalar yürütülebilir.
- Bu çalışmada evren ve örneklem genel halk olarak belirlendiği için daha sonra yapılacak olan çalışmalarda sağlık çalışanlarının mevcut durumu da değerlendirilebilir.
- Çalışmada yapılan analizler sonucunda yeni bir model keşfedilmiştir. Sonraki çalışmalarda bu yeni model kullanılabilir.
- Yapılan araştırmada gizlilik endişesi ve veri paylaşma niyeti değişkenleri arasındaki ilişkide algılanan risk ve faydanın aracılık rolü olmadığı saptandığı için başka değişkenlerin aracılık rolünün olup olmadığı araştırılabilir.
- Bireylerin gizlilik endişesi veri paylaşma niyetini etkilediği için bu endişeleri en aza indirebilmek adına politika yapıcılar, sağlık bilgi teknolojisi üreten firmalar ve sağlık kurum ve kuruluşları halkı bilinçlendirmek, halkın güvende hissetmelerini sağlamak amacıyla eğitimler verebilir.
- Kişisel sağlık verileri önemi yeni anlaşılan bir kavram olduğu için sağlık personellerinin de bu noktada hastanın veri mahremiyetinin korunması açısından eğitilmesi gerekmektedir. Bu doğrultuda hastane yöneticilerine ve idari birimlere büyük görev düşmektedir. Dolayısıyla sağlık kurum ve kuruluşlarında çalışan tüm personelin de veri mahremiyeti seminerleri düzenlenerek bilinçlendirilmesi önerilebilir.

6. KAYNAKLAR

Abouelmehdi K, Beni-Hessane A, Khaloufi H, 2018. Big healthcare data: preserving security and privacy. Journal of Big Data, 5, 1, p. 1-18. doi:10.1186/s40537-017-0110-7.

Acquisti A, Grossklags J, 2005. Privacy and rationality in individual decision making. IEEE Security & Privacy, 3, p. 24-30.

Ada A, Aksoy R, 2020. Giyilebilir teknolojik ürünlerde tüketicilerin algıladıkları risklerin farklılaşması: akıllı saat kullanıcılarına dönük bir araştırma. Herkes için Spor ve Rekreasyon Dergisi, 2, 1, s. 50-61.

Ağıralan E, 2015. Bilgi güvenliği, kişisel verilerin korunması ve mahremiyet etki değerlendirmesi. Yüksek Lisans Tezi, Polis Akademisi Güvenlik Bilimleri Enstitüsü, Ankara.

Ajzen I, 1991. The theory of planned behavior. Organizational Behavior and Human Decision Processes. 50, 2, p. 179-211.

Akçalı Gür B, 2019. Uluslararası hukuk ve ab hukuku boyutuyla kişisel verilerin yurt dışına aktarılması . Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi, 25, 2, s. 850-72.

Akgül A, 2013. Kişisel verilerin korunması açısından idarenin hukuki sorumluluğu ve yargısal denetimi. Doktora Tezi, Kocaeli Üniversitesi Sosyal Bilimler Enstitüsü, Kocaeli.

Akkurt SS, 2020. Kişisel sağlık verilerinin işlenmesine ve covıd-19 pandemisi sürecinde mobil uygulamalarla paylaşılmasına hukukî bir bakış. İstanbul Ticaret Üniversitesi Sosyal Bilimler Dergisi, Covid-19 Hukuk Özel Sayısı, 19, 38, s. 142-160.

Alhakami AS, Slovic P, 1994. A psychological study of the inverse relationship between perceived risk and perceived benefit. In Press, Risk Analysis, 22, p. 1-33.

Alkan N, 2003. Tıp ve sağlık kuruluşlarında bilgi yönetimi. Bilgi Dünyası Dergisi, 4, 2, s. 122-45.

Alonso-Ferres M, Imami L, Slatcher RB, 2020. Untangling the effects of partner responsiveness on health and well-being: The role of perceived control. Journal of Social and Personal Relationships, 37, 4, p. 1150-71.

Alp M, Gürsel İ, 2020. Covıd-19 pandemisinde işçilere ait sağlık verilerinin işlenmesi. Sicil İş Hukuku Dergisi, 44, 11-32.

Altundiş M, 2016. Tıbbi kişisel verilerin tutulması ve korunması yükümlülüğü ve idarenin bu yükümlülüğünü yerine getirmemesinden doğan sorumluluğu. Türkiye Adalet Akademisi Dergisi, 7, 28, s. 313-51.

Angst CM, Agarwal R, 2009. Adoption of electronic health records in the presence of privacy concerns: the elaboration likelihood model and individual persuasion. MIS Quarterly 33, 2, p. 339-70. https://doi.org/10.2307/20650295.

Arslan Ç, 2011. Avrupa birliği hukukunda kişisel verilerin üçüncü ülkelere aktarılması, BAÜHF Kazancı Hakemli Hukuk Dergi, s. 31-61.

Aslan Ş, 2018. Sosyal bilimlerde araştırma yöntemleri, 1.Baskı, Konya, Eğitim Yayınevi, s. 94-5.

Atalay HN, 2021. Mahremiyet kapsamında kişisel sağlık verilerinin korunması ve depolanması. Journal of Academic Perspective on Social Studies, 1, s. 1-20 . Doi: 10.35344/japss.786353.

Avaner E, 2018. Mahremiyet nedir? mahremiyetin sağlık hizmetleri penceresinden görünürlüğü nasıldır?. Türkiye Biyoetik Dergisi, 5, 3, s. 110-16.

Avcı Y, 2019. Kişisel verilerin korunması. Yüksek Lisans Tezi, Selçuk Üniversitesi Sosyal Bilimler Enstitüsü, Konya.

Awad NF, Krishnan MS, 2016. IHcli CCi IV researchnoe The Personalization Privacy Paradox : An Empirical. 30, 1, p. 13–28.

Bagozzi RP, 1981. Evaluating structural equation models with unobservable variables and measurement error: a comment. Journal of Marketing Research, 18, 3, p. 375- 81.

Bandura A, 1977. Self-efficacy: towards a unifying theory of behavioural change, Psychological Review, 84, p. 191-215.

Bani Issa W, Al Akour I, Ibrahim A, Almarzouqi A, Abbas S, Hisham F, Griffiths J, 2020. Privacy, confidentiality, security and patient safety concerns about electronic health records. International Nursing Review, 67, 2, p. 218-30.

Bansal G, Zahedi MF, Gefen D, 2010. The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online. Decision Support Systems, 49, 2, p. 138-50. doi:10.1016/j.dss.2010.01.010.

Baran S, Şener E, 2019. Hastanelerde bilgi güvenliği yönetimi: nitel bir araştırma . Süleyman Demirel Üniversitesi Vizyoner Dergisi, 10, 23, s. 108-25 . DOI: 10.21076/vizyoner.444451.

Başar C, 2019. Türk idare hukuku ve avrupa birliği hukuku ışığında kişisel kişisel verilerin korunması. Doktora Tezi, Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü, İzmir.

Başaran Ü, Aksoy R, 2015. Algılanan fayda ve fedakarlık bileşenlerinin algılanan müşteri değeri üzerindeki etkisi. Ege Akademik Bakış Dergisi. 15, 3, p. 379-99.

Bayındır H, 2019. Özel sağlık kurumları kapsamında kişisel sağlık verilerinin işlenmesi ve korunması. Yüksek Lisans Tezi, İstanbul Üniversitesi Sosyal Bilimler Enstitüsü. İstanbul.

Beck EJ, Gill W, De Lay PR, 2016. Protecting the confidentiality and security of personal health information in low- and middle-income countries in the era of SDGs and Big Data. Global Health Action, 9, 1, p. 1-7.

Becker M, 2018. Understanding users' health information privacy concerns for health wearables. Proceedings of the 51st Hawaii International Conference on System Sciences. URI: http://hdl.handle.net/10125/50301 ISBN: 978-0-9981331-1-9 (CC BY-NC-ND 4.0), p. 3261-70.

Belanger F, Hiller JS, Smith WJ, 2002. Trustworthiness in electronic commerce: the role of privacy, security, and site attributes. 11, p. 245–70.

Beldad A, de Jong M, Steehouder M, 2011. I trust not therefore it must be risky: determinants of the perceived risks of disclosing personal data for e-government transactions. Computers in Human Behavior, 27, 6, p. 2233-42. doi:10.1016/j.chb.2011.07.002

Bennett C, 1967. What price privacy. American Psychologist, 22, 5, p. 371-76.

Bentler PM, 1990. Comparative fit indexes in structural models. Psychological Bulletin, 107, 2, p. 238-46. doi:10.1037/0033-2909.107.2.238.

Bessen J, 1993. Riding the marketing information wave. Harvard Business Review, September-October, 71, 5, p. 150-60.

Beyan O, Choudhury A, Soest JV, Kohlbacher O, Zimmermann L, Stenzhorn H, Karim MDR, Dumontier M, Decker S, Silva Santos LOB, Dekker A, 2020. Distributed analytics on sensitive medical data: the personal health train. Data Intelligence, 2, 2020, p. 96-107.

Bezirgan Gözmener S, 2019. Kişisel sağlık verilerinin kayıt ve korunmasında hemşirelerin cezai sorumluluğu. Yüksek Lisans Tezi, Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü, İzmir.

Borena B, Belanger F, Ejigu D, 2013. Social Networks and Information Privacy: A Model for Low-income Countries. Proceedings of the Nineteenth Americas Conference on Information Systems, August 15-17, Chicago, Illinois.

Boshoff C, Schlecther C, Ward SJ, 2011. Consumers' perceived risks associated with purchasing on a branded website: the mediating effect of brand knowledge. South African Journal of Business Management, 42, 1, p. 45-54.

Bozkurt H, 2019. Kişisel verilerin işlenmesinin hukuki boyutu. Yüksek Lisans Tezi, Kadir Has Üniversitesi Lisansüstü Eğitim Enstitüsü, İstanbul.

Browne MW, Cudeck R, 1993. Alternative ways of assessing model fit. In K. A. Bollen & J. S. Long (Eds.), Testing structural equation models (p. 136-62). Newbury Park, CA: Sage.

Buchanan T, Paine C, Joinson AN, Reips UD, 2007. Development of measures of online privacy concern and protection for use on the internet. Journal Of The Amerıcan Socıety For Informatıon Scıence And Technology, 58, 2, p. 157–65.

Bugental DB, Blue J, Cruzcosa M, 1989. Perceived control over caregiving outcomes: implications for child abuse. Developmental Psychology, 25, 4, p. 532–39.

Cases AS, 2002. Perceived risk and risk-reduction strategies in internet shopping. International Review of Retail, Distribution and Consumer Research, 12, 4, p. 375- 94.

Ceccato N, Price C, 2019. When personal health data is no longer "personal." Healthcare Management Forum, 32, 6, p. 326-8. doi:10.1177/0840470419865851.

Chaudhry A, Crowcoft J, Howard H, Madhavapeddy A, Mortier R, Haddadi H, McAuley D, 2015. Personal data: thinking inside the box. Aarhus Series on Human Centered Computing 1, 4. doi:10.7146/aahcc.v1i1.21312.

Chen R, 2013. Living a private life in public social networks: an exploration of member self-disclosure. Decision Support Systems, 55, p. 661-68.

Chen R, He F, 2003. Examination of brand knowledge, perceived risk and consumers` intention to adopt an online retailer. TQM & Business Excellence, 14, 6, p. 677-93.

Chipperfield JG, Greenslade L, 1999. Perceived control as a buffer in the use of health care services. Journal of Gerontology: Psychologıcal Sciences, 54, 3, p. 146-54.

Chipperfield JG, Perry RP, Stewart TL, 2012. Perceived control. Encyclopedia of Human Behavior, Second edition, Academic Press, p. 42-8.

Choi J, Lee A, Ok C, 2013. The Effects of Consumers' Perceived Risk and Benefit on Attitude and Behavioral Intention: A Study of Street Food. Journal of Travel & Tourism Marketing. 30, 3, p. 222–37.

Clarke A, Steele R, 2015. Smartphone-based public health information systems: anonymity, privacy and intervention. Association for Information Science and Technology, 66, p. 2596–608.

Cocosila M, Archer N, 2014. Perceptions of chronically ill and healthy consumers about electronic personal health records: a comparative empirical investigation. BMJ Open 4, 7, e005304. https://doi.org/10.1136/bmjopen-2014-005304.

Connell JP, 1985. A new multidimensional measure of children's perceptions of control. Child Development, 56, p. 1018-41.

Conner M, Armitage CJ, 1998. Extending the theory of planned behavior: a review and avenues for further research. Journal of Applied Social Psychology, 28, 15, p. 1429–64.

Coşkun R, Altunışık R, Bayraktaroğlu S, Yıldırım E, 2015. Sosyal bilimlerde araştırma yöntemleri. Sakarya Yayıncılık, Sakarya.

Cox DF, 1967. Risk handling in consumer behavior – an intensive study of two cases. Risk Taking and Information Handling on Consumer Behavior, Harvard University Press, Boston, p. 603-39.

Cöddü MB, 2015. İnternetten alışverişte tüketiciler tarafından algılanan risk türlerinin etkileri ve cinsiyet farklılıkları açısından incelenmesi. Yüksek Lisans Tezi. Çukurova Üniversitesi Sosyal Bilimler Enstitüsü, Adana.

Cruickshank J, Packman, C, Paxman J, 2012. Personal Health Records: Putting Patients in Control?. Erişim Adresi: https://2020health.org/publication/personal-health-records-putting-patients-in-control/. Erişim tarihi: 25 Mart 2022.

Culnan MJ, Armstrong PK, 1999. Information privacy concerns, procedural fairness, and impersonal trust: an empirical investigation; INFORMS: Catonsville MD, p. 104–15.

Culnan MJ, Bies RJ, 2003. Consumer privacy: Balancing economic and justice considerations. Journal of Social Issues, 59, 2, p. 323-42. https://doi.org/10.1111/1540-4560.00067.

Çakar Ü, Can, P, 2019. Risk boyutlarının genel algılanan risk üzerine etkisi: e-ticaret sitelerine yönelik bir araştırma. Atatürk İletişim Dergisi, 17, s. 39-68.

Çalık T, 2016. Birleşmiş milletleriİnsan hakları sözleşmeleri kapsamında insan haklarının korunması. Selçuk Üniversitesi Hukuk Fakültesi Dergisi, 24, 1, s. 69-120.

Çelik Y, 2017. Özel hayatın gizliliğinin yansıması olarak kişisel verilerin korunması ve bu bağlamda unutulma hakkı. Türkiye Adalet Akademisi Dergisi, 32, s. 391-410. https://dergipark.org.tr/tr/pub/taad/issue/52657/693992.

Çetin H, 2014. Kişisel veri güvenliği ve kullanıcıların farkındalık düzeylerinin incelenmesi. Akdeniz İ.İ.B.F. Dergisi, 29, s. 86 – 105.

Dankar FK, El Emam K, 2012. The application of differential privacy to health data. ACM International Conference Proceeding Series, 12, p. 158-66.

Das TK, Teng B, 1998. Between Trust and Control: Developing confidence in partner cooperation in alliances. Academy of Management Review, 23, 3, p. 491–512.

Deniz A, Erciş A, 2008. Kişilik özellikleri ile algılanan risk arasındaki ilişkilerin incelenmesi üzerine bir araştırma. İktisadi ve İdari Bilimler Dergisi, 22, 2, s. 301-30.

Devi KK. Prasad SR, 2017. Privacy Preserving for Mobile Health Data. International Research Journal of Engineering and Technology (IRJET). 4, 7, p. 1602-7. e-ISSN: 2395-0056.

Dhaggara D, Goswami M, Kumar G, 2020. Impact of trust and privacy concerns on technology acceptance in healthcare: an ındian perspective. International Journal of Medical Informatics, 141, p. 1-13. doi:10.1016/j.ijmedinf.2020.10416.

Dhillon GS, Moores TT, 2001. Internet privacy: interpreting key issues. Information Resources Management Journal, 14, 4, p. 33-37.

Dimitropoulos L, Patel V, Scheffler SA, Posnack S, 2011. Public attitudes toward health information exchange: perceived benefits and concerns. Am. J. Manag. Care 17, 12, p. 111-16.

Dinev T, Hart P, 2005. Internet privacy concerns and social awareness as determinants of intention to transact. International Journal of Electronic Commerce, 10, 2, p. 7-29. https://doi.org/10.2753/JEC1086-4415100201.

Dinev T, Hart P, 2006. An extended privacy calculus model for e-commerce transactions. Information Systems Research, 17, 1, p. 61-80.

Dinev T, Xu H, Smith JH, Hart P, 2013. Information privacy and correlates: an empirical attempt to bridge and distinguish privacy-related concepts. European Journal of Information Systems, 22, p. 395-16.

Dural M, Öğüz T, 2020. Türk özel hukuku cilt II, 21. Baskı, İstanbul, Filiz Kitabevi, s.215-16.

Durmuş V, 2021. Kişisel sağlık verilerinin korunmasında idarenin hukuki sorumluluğu. Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi(DEUHFED), 14, 1, s. 67-76.

Dülger MV, 2015a. Sağlık hukukunda kişisel verilerin korunması ve hasta mahremiyeti. İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi, 1, 2, s. 43-80.

Dülger MV, 2015b. Bilişim suçları ve internet iletişim hukuku, 6. Basım, Ankara, Seçkin Yayıncılık, s. 675-702.

Dülger MV, 2016. Kişisel verilerin korunması kanunu ve türk ceza kanunu bağlamında kişisel verilerin ceza normlarıyla korunması, İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi, 3, 2, p. 101-68.

Dülger MV, 2019a. Kişisel verilerin korunması hukuku, Hukuk Akademisi Yayıncılık, İstanbul, s. 1.

Dülger MV, 2019b. Kişisel sağlık verileri hakkında yönetmelik'e ilişkin değerlendirme. Hukuki Haber, Erişim Tarihi 19 Şubat 2020, Erişim Adresi https://www.hukukihaber.net/kisisel-saglik-verileri-hakkinda-yonetmelike-iliskin-degerlendirme-makale,6847.html.

Dülger MV, 2019c. Avrupa birliği genel veri koruma tüzüğü bağlamında kişisel verilerin korunması.Yaşar Hukuk Dergisi, 1, 2, s. 71-174.

Eke E, Çetin R, Çetin B, 2018. Mobil sağlık uygulamalarının güvenliğine ilişkin haberler aracılığıyla yaşanan etik sorunların değerlendirilmesi. Bolu Abant İzzet Baysal Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, 18, 3, s. 129-45. DOI: 10.11616/asbed.vi.470699.

Emani S, Yamin CK, Peters E, 2012. Patient perceptions of a personal health record: a test of the diffusion of innovation model. Journal Medical Internet Research, 14, 6, p. 150. https://doi.org/10.2196/jmir.2278.

Ercan F, Köşker H, Albuz N, 2020. Çevrimiçi seyahat rezervasyonuna yönelik algılanan riskin kullanma eğilimi üzerine etkisi. Journal of Yasar University, 15, 59, s. 624-41.

Ergüden Ç, 2019. Kişisel sağlık verilerinin işlenmesi. Erişim tarihi 15 Ocak 2021, Erişim adresi,https://www.academia.edu/40904181/k%c4%b0%c5%9e%c4%b0sel_sa%c4%9elık_ver%c4%b0ler%c4%b0n%c4%b0n_%c4%b0%c5%9elenmes%c4%b0.

Eryılmaz A, Ercan, L, 2010. Öznel iyi oluş ile algılanan kontrol arasındaki ilişkinin incelenmesi. İlköğretim Online, 9, 3, s. 952-59.

Fabiano N, 2019. Ethics and the protection of personal data. Systemics, Cybernetics and Informatics, 17, 2, p. 58-64.

Flender C ,Müller G, 2012. Type indeterminacy in privacy decisions: the privacy paradox revisited. Quantum interaction. Berlin Heidelberg: Springer, p. 148–59.

Forsythe SM, Shi B, 2003. Consumer patronage and risk perceptions in internet shopping. Journal of Business Research, 56, 11, p. 867-75.

Gaylin DS, Moiduddin A, Mohamoud S, Lundeen K, Kelly JA, 2011. Public attitudes about health information technology, and its relationship to health care quality, costs, and privacy. Health Services Research 46, 3, p. 920-38. https://doi.org/ 10.1111/j.1475-6773.2010.01233.x.

George J, Bhila T, 2019. Security, confidentiality and privacy in health of healthcare data. International Journal of Trend in Scientific Research and Development, 3, 4, 373-7. doi:10.31142/ijtsrd23780.

Gerber C, Ward S, Goedhals-Gerber L, 2014. The impact of perceived rısk on on-line purchase behaviour. Risk Governance & Control: Financial Markets & İnstitutions, 4, 4, p. 99-106.

Ghamari N, Mellbin L, 2015. Disclosing personal information to social networking site providers: the role of trust, risk and perceived benefits. Master Thesis, Department of Business, Studies Uppsala University, Sweden.

Goodwin C, 1991. Privacy: recognition of a consumer right. Journal of Public Policy and Marketing, 10, 1, p. 149-166.

Gökay G, Erçil Y, Tokdemir G, Cağıltay N, Aykaç YE, 2015. Kişisel sağlık kaydı sistemleri kullanılabilirlik durum çalışması. Tıp Teknolojileri Ulusal Kongresi Kitabı, s. 15-18, 15 Ekim 2015, Muğla.

Gökçay B, Arda B, 2019. Kişisel sağlık verilerinin korunması kapsamında sağlık araştırmalarında etik bakış. Turk Kardiyol Derneği Araştırmaları, 47, 3, s. 218-27.

Gözüküçük M, 2014. Veri işleme süreçlerinde tartışmalı bir çözüm: veri anonimleştirmesi. Yüksek Lisans Tezi, İstanbul Bilgi Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul.

Gupta P, Dubey A, 2016. E-commerce study of privacy, trust and security from consumer's perspective. International Journal of Computer Science and Mobile Computing, 5, 6, p. 224-32.

Gürsel E, Düğmeci F, 2018. Yapısal anlamda türkiye kişisel verileri koruma kurumuna ilişkin bir değerlendirme. R&S - Research Studies Anatolia Journal, 1, 2, s. 318-29.

Hair JF, Black WC, Babin BJ, Anderson RE, Tatham RL, 2013. Multivariate data analysis: Pearson Education Limited.

Hajli N, Lin X, 2014. Exploring the security of information sharing on social networking sites: the role of perceived control of information. Journal of Business Ethics, 133, 1, p. 111-23.

Hatipoğlu S, 2019. Kişisel verilerin korunması ve idarenin hukuki sorumluluğu. Yüksek Lisans Tezi, Trakya Üniversitesi Sosyal Bilimler Enstitüsü. Trakya.

Hayes AF, 2018. Partial, conditional, and moderated moderated mediation: Quantification, inference, and interpretation. Communication monographs, 85, 1, p. 4-40.

Henkoğlu T, 2017. Kişisel verileriniz ne kadar güvende? Bilgi güvenliği kapsamında bir değerlendirme. Arşiv Dünyası, 18-19, s. 36-47. https://dergipark.org.tr/en/pub/ad/issue/33457/372372.

Hoadley CM, Xu H, Lee JJ, Rosson MB, 2009. Privacy as information access and illusory control: the case of the facebook news feed privacy outcry. Electronic Commerce Research and Applications, 9, 2010, p. 50-60.

Hofmann W, Luhmann M, Fisher RR, Vohs KD, Baumeister RF, 2014. Yes, but are they happy? effects of trait self-control on affective well-being and life satisfaction. Journal Personality, 82, 4, p. 265-77.

Hong IB, 2015. Understanding the consumer's online merchant selection process: the roles of product involvement, perceived risk, and trust expectation. International Journal of Information Management, 35, 3, p. 1-29.

Hong W, Thong JY, 2013. Internet privacy concerns: An integrated conceptualization and four empirical studies. Mis Quarterly, 37, 1, p. 275-98.

Hong Z, Yi L, 2012. Research on the influence of perceived risk in consumer online purchasing decision. Physics Procedia, 24, Part B, p. 1304-10.

Hooper D, Coughlan J, Mullen M, 2008. Evaluating model fit: a synthesis of the structural equation modelling literature. In 7th European Conference on research methodology for business and management studies (pp. 195-200).

Huang WY, Schrank H, Dubinsky AJ, 2004. Effect of brand name on consumers" risk perceptions of online shopping. Journal of Consumer Behaviour, 4, 1, p. 40-50.

Hui KL, Teo HH, Lee SYT, 2007. The value of privacy assurance: An exploratory field experiment. Mis Quarterly, 19-33.

Ibraimi L, Asim M, Petković M, 2009, Secure management of personal health records by applying attribute-based encryption. In Proceedings of the 6th International Workshop on Wearable, Micro, and Nano Technologies for Personalized Health (pp. 71-74). https://doi.org/10.1109/PHEALTH.2009.5754828.

Infurna FJ, Gerstorf D, Zarit SH, 2011. Examining dynamic links between perceived control and health: longitudinal evidence for differential effects in midlife and old age. Developmental Psychology Journal, 47, 1, p. 9-18.

İmançlı C, 2019. Kişisel sağlık verilerinin korunamamasından doğan özel hukuk sorumluluğu. Yüksek lisans Tezi, İstanbul Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul.

JacobyJ, Kaplan LB, 1972. The components of perceived risk. in SV - Proceedings of the Third Annual Conference of the Association for Consumer Research, eds. M.Venkatesan, Chicago, IL : Association for Consumer Research, p. 382-93.

Jarvenpaa SL, Todd PA, 1996. Consumer reactions to electronic shopping on the world wide web. International Journal of Electronic Commerce, 1, 2, p. 59- 88.

Jourard S, 1966. Some psychological aspects of privacy. Law and Contemporary Problems, 31, p. 307-18. Erişim tarihi 19 Ekim 2021, Er,işim adresi: https://scholarship.law.duke.edu/cgi/viewcontent.cgi?referer=https://scholar.google.com/&httpsredir=1&article=3110&context=lcp.

Kandilli E, 2019. Sağlık hukukunda etik açısından kişisel veriler ve mahremiyet hakkı. Yüksek Lisans Tezi, İstanbul Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul.

Karagöz Y, 2021. Spss, amos, meta uygulamalı nitel-nicel-karma bilimsel araştırma yöntemleri ve yayın etiği. Nobel Akademik Yayıncılık, Ankara.

Kart A, Ketizmen M, 2019. Kabahatler kanunu'nun içtima hükümleri açısından kişisel verilerin korunmasına ilişkin suç ve kabahatler ile kurulun idari ceza kararlarına ilişkin bir değerlendirme. Kişisel Verileri Koruma Dergisi, 1, 2, s. 17-29.

Kenny G, Connolly R, 2016. Drivers of health ınformation privacy concern: a comparison study. Proceedings of the 22nd Americas Conference on Information Systems (AMCIS), p. 1-10, San Diego. Erişim tarihi: 02 Eylül 2021, Erişim adresi: https://aisel.aisnet.org/amcis2016/Health/Presentations/3/.

Kılınç D, 2012. Anayasal bir hak olarak kişisel verilerin korunması. Ankara Üniversitesi Hukuk Fakültesi Dergisi, 61, 3, s. 1089-172.

Kim DJ, Ferrin DL, Rao HR, 2008. A trust-based consumer decision-making model in electronic commerce: the role of trust, perceived risk, and their antecedents. Decision Support Systems, 44, 2, p. 544-64. https://doi.org/10.1016/j.dss.2007.07.001.

Kim JW, Jang B, Yoo H, 2018. Privacy-preserving aggregation of personal health data streams. PLOS ONE, 13,11, p. 1-15. doi:10.1371/journal.pone.0207639.

Kişisel Sağlık Verilerinin İşlenmesi Ve Mahremiyetinin Sağlanması Hakkında Yönetmelik. Erişim tarihi, 17 Kasım 2020. Erişim adresi,https://www.lexpera.com.tr/mevzuat/yonetmelikler/kisisel-saglik-verilerinin-islenmesi-ve-mahremiyetinin-saglanmasi-hakkinda-yonetmelik.

Kişisel Verileri Koruma Kurumu, 2018. Kişisel verilerin korunması kanunu hakkında sıkça sorulan sorular. Erişim tarihi 26 Ocak 2021, Erişim adresi,https://www.kvkk.gov.tr/Icerik/4196/Kisisel-Verilerin-Korunmasi-Kanunu-Hakkinda-Sikca-Sorulan-Sorular.

Kişisel Verileri Koruma Kurumu, 2018a. 100 soruda kişisel verileri koruma kanunu. KVKK Yayınları, Ankara.

Kişisel Verileri Koruma Kurumu, 2018b. Erişim tarihi 26 Ocak 2021. Erişim adresi,https://www.kvkk.gov.tr/yayinlar/K%C4%B0%C5%9E%C4%B0SEL%20VER%C4%B0LER%C4%B0N%20KORUNMASI%20KANUNU%20VE%20UYGULAMASI.pdf.

Kişisel Verilerin Korunması Kanununa İlişkin Uygulama Rehberi, 2018. Kişisel Verileri Koruma Kurumu, KVKK Yayınları, Ankara.

Kocagöz E, Dursun Y, 2010. Algılanan davranışsal kontrol, ajzen'in teorisinde nasıl konumlanır? alternatif model analizleri. Karamanoğlu Mehmetbey Üniversitesi Sosyal Ve Ekonomik Araştırmalar Dergisi, 2010, 2, s. 139-52.

Korkmaz İ, 2016. Kişisel Verilerin Korunması Kanunu Hakkında Bir Değerlendirme. Türk Tabipler Birliği(TTB) Dergisi, 124, s. 85-152.

Krasnova H, Spiekermann S, Koroleva K, Hildebrand T, 2010. Online social networks: why we disclose. Journal of Information Technology, 25, 2, p. 109-25.

Kurtz DL, Clow KE, 1997. Services Marketing, New York: John Wiley and Sons, p. 52-69.

Kutlu Ö, Kahraman S, 2017. Türkiye'de kişisel verilerin korunması politikasının analizi. Siyaset, Ekonomi ve Yönetim Araştırmaları Dergisi, 5, 4, s. 45-62.

Laroche M, Bergeron J, Goutaland C, 2003. How intangibility affects perceived risk: the moderating role of knowledge and involvement. Journal of Services Marketing, 17, 2, p. 122-140.

Laufer RS, Wolfe M, 1977. Privacy as a concept and a social issue:a multidimensional developmental theory. Journal of Social Issues, 33, p. 22-41.

Lee J, Rao HR, 2007. Perceived risks, counter-beliefs, and intentions to use anti-/counter-terrorism websites: An exploratory study of government–citizens online interactions in a turbulent environment. Decision Support Systems, 43(4), 1431–1449. doi:10.1016/j.dss.2006.04.008

Lee LM, Gostin LO, 2009. Ethical collection, storage, and use of public health data: a proposal for a national privacy protection. *Jama*, *302*(1), 82-4.

Lee N, Kwon O, 2015. A privacy-aware feature selection method for solving the personalization-privacy paradox in mobile wellness healthcare services. Expert Syst Appl, 42, 5, p. 2764–71.

Li F, Zou X, Liu P, Chen, J. Y. 2011b. New threats to health data privacy. *BMC Bioinformatics, 12(Suppl 12), 2-7.* doi:10.1186/1471-2105-12-s12-s7.

Li H, Sarathy R, Xu H, 2011a. The role of affect and cognition on online consumers' decision to disclose personal information to unfamiliar online vendors. Decision Support Systems, 51, p. 434-45.

Li S, Rao SS, Ragu-Nathan, TS, Ragu-Nathan B, 2005. Development and validation of a measurement instrument for studying supply chain management practices. Journal of operations management, 23, 6, p. 618-41.

Li T, Slee T, 2014. The effects of information privacy concerns on digitizing personal health records. J. Ass. Inf. Sci. Technol. 65, 8, p. 1541-54. https://doi.org/ 10.1002/asi.23068.

Lim N, 2003. Classification of consumers' perceived risk: sources versus consequences. Electronic Commerce Research and Applications, 2, p. 216-28.

Liu LS, Shih PC, Hayes GR. 2011. Barriers to the adoption and use of personal health record systems. In: Proceedings of theiConference. New York, NY: ACM; 2011 Presented at: iConference; Feb 8-11, Seattle, WA, USA p. 363-370. doi:10.1145/1940761.1940811.

Malhotra NK, Kim SS, Agarwal J, 2004. Internet users' ınformation privacy concerns(ıuıpc): the construct, the scale and a causal model. Information System Research, 15, 4, p. 336-55.

Maraş G, Ceyhan Ö, 2021. Hemşirelik öğrencilerinin kişisel sağlık verilerinin kayıt ve korunması konusundaki tutumları. İnönü Üniversitesi Sağlık Hizmetleri Meslek Yüksek Okulu Dergisi, 9, 2, s. 498-509. DOI: 10.33715/inonusaglik.851192.

Marriot HR, Wiiliams WD, Dwivedi YK, 2017. Risk, privacy and security concerns in digital retail. The Marketing Review, 17, 3, p. 1-60.

Mehraeen E, Ayatollahi H, Ahmadi M, 2016. Health Information Security in Hospitals: the Application of Security Safeguards. Acta informatica medica, 24, 1, p.47-50. doi:10.5455/aim.2016.24.47-50.

Nalbantoğlu L, 2018. Kişisel sağlık verilerinin işlenmesi ve mahremiyetinin sağlanması hakkında yönetmelikte yapılan değişiklikler. The Deloitte Times, s. 64-7.

O'Doherty KC, , Christofides E , Yen J, Bentzen HB, Burke H, Hallowell N, Koenig BA, Willison DJ, 2016. If you build it, they will come: unintended future uses of organised health data collections. BMC Medical Ethics, 17, 54, p. 1-16.

Oğuz S, 2018. Kişisel verilerin korunması hukukunun genel ilkeleri. Bilgi Ekonomisi ve Yönetimi Dergisi, 13, 2, s. 121-138.

Ohm P, 2009. Broken promises of privacy: responding to the surprising failure of anonymization. UCLA Law Rewiev, 57, p. 1701-2010.

Olca E, Can Ö. Ulusal ve uluslararası yönetmeliklerde kişisel sağlık verisi mahremiyetinin korunması. 7.Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı, s. 71-76, 17-18 Ekim 2014, İstanbul.

Orel A, Bernik I, 2018. Gdpr and health personal data; tricks and traps of compliance. Stud Health Technol Inform, 255, p. 155-159. PMID: 30306927.

Osatuyi B, 2014. Empirical examination of ınformation privacy concerns ınstrument in the social media context. Transactions on Replication Research, 1,3, p. 1-14.

Öksüzoğlu HT, 2019. 6698 Sayılı kişisel verilerin korunması kanunu ve avrupa birliği hukukunda kişisel verilerin silinmesi ve düzeltilmesi. Bilişim Hukuku Dergisi, 2, s. 185-242.

Özkan E. 2018. Why do consumers behave differently in personal ınformation disclosure and self-disclosure? The role of personality traits and privacy concern. Alphanumeric Journal, 6, 2, p. 257-76. Doi: 10.17093/alphanumeric.460158.

Özkan O, 2020. Kişisel verilerin korunması. Yüksek Lisans Tezi, Ankara Üniversitesi Sosyal Bilimler Enstitüsü, Ankara.

Park J, Robertson R, Wu C, 2004. The Effect of Airline Service Quality on Passengers' Behavioural Intentions: a Korean Case Study. Journal of Air Transport Management. 10, 6, p. 435-9.

Peter JP, Ryan MJ, 1976. An investigation of perceived risk at the brand level. Journal of Marketing Research, 13, 2, p. 184-8.

Phelps J, Nowak G, Ferrell E, 2000. Privacy concerns and consumer willingness to provide personal information. Journal of Public Policy & Marketing. 19, 1, p. 27-41. https://doi.org/ 10.1509/jppm.19.1.27.16941.

Pintiliuc IG, 2018. Protection of personal data. Logos Universality Mentality Education Novelty: Law, 6, 1, p. 37-40.

Princi E, Kramer NC. 2020. Out of control - privacy calculus and the effect of perceived control and moral considerations on the usage of iot healthcare devices. Frontiers in psychology, 11, p. 1-15.

Rittenberg L, Trigarthen T, 2012. Principles of microeconomics. Washington, DC: Flat World Knowledge, p.102-19.

Robinson SA, Lachman ME, 2017. Perceived control and aging: a mini-review and directions for future research. Gerontology, 63, 5, p. 435-42. doi: 10.1159/000468540.

Schiffman LG, Kanuk, LL, 1994. Consumer behavior. Englewood Cliffs, NJ: Prentice-Hall, p.75-9.

Sheehan KB, Hoy MG, 2000. Dimensions of privacy concern among online consumers. Journal of Public Policy and Marketing, 19, 1, p. 62–73.

Sınar H, 2020. Kişisel verileri hukuka aykırı olarak verme, yayma ve ya ele geçirme suçu (TCK md. 136) . Kişisel Verileri Koruma Dergisi, 2, 1, s. 33-62.

Skinner EA, Connell JP, 1986. Control understanding: Suggestions for a developmental framework. M.M. Baltes & P.B. Baltes (Eds.). In: The Pscyhology Of Control And Aging (p. 35-69). Hillsdale, NJ: Lawrence Erlbaum.

Smith HJ, Dinev T, Xu H, 2011. Information privacy research: an interdisciplinary review. MIS Quartely, 35, 4, p. 989-1015.

Smith HJ, Milberg SJ, Burke SJ, 1996. Information privacy: measuring ındividuals' concerns about organizational practices. MIS Quartely, 20, 2, p. 167-96.

Steiger JH, 2007. Understanding the limitations of global fit assessment in structural equation modeling. Personality and Individual differences, 42, 5, p. 893-98.

Stewart KA, Segars AH, 2002. An empirical examination of the concern for information privacy instrument. Information Systems Research, 13, 1, p. 36-49.

Stone RN, Gronhaug K, 1993, Perceived risk: further considerations for the marketing discipline. European Journal of Marketing, 27, 3, p. 372-94.

Sun Y, Fang S, Hwang Y, 2019. Investigating privacy and information disclosure behavior in social electronic commerce. Sustainabilty(MDPI), 11, 3311, p. 1-27.

Sun Y, Wang N, Shen X-L, Zhang JX, 2015. Location information disclosure in location-based social network services: privacy calculus, benefit structure, and gender differences. Computer Human Behaviour, 52, p. 278-92.

Şenyürek G. Etik açıdan kişisel sağlık verileri ve korunması. Kişisel Sağlık Verileri Iı. Ulusal Kongresi Kitabı, s. 151-157, 03-04 Haziran 2017, İstanbul.

Takçı H, Canbay P, 2017. Kişisel verilerin korunmasında öznitelik tabanlı gizlilik etki değerlendirmesi yöntemi . Gazi Üniversitesi Mühendislik Mimarlık Fakültesi Dergisi, 32, 4, s. 1301-1310. DOI: 10.17341/gazimmfd.369733.

Tan M, Teo TSH, 2000. Factors influencing the adoption of Internet banking. Journal of the Association for Information Systems, 1, 5, p. 1-42.

Tanadi T, Samadi B, Gharleghi B, 2015. The Impact of perceived risks and perceived benefits to improve an online intention among generation-y in Malaysia. Asian Social Science, 11, 26, p.226-38.

Tanrıkulu E, Bakır NO, 2021. Tüketicilerin çevrimiçi alışverişteki faydaci ve hedonik alışveriş değerinin algilanan fayda ve risk üzerindeki etkisi: trendyol ve zara tüketicileri üzerine bir araştirma. *Journal of Marmara University Social Sciences Institute / Öneri*, 16, 56, s. 634-67. https://doi.org/10.14783/maruoneri.812174.

Tataroğlu M, 2009. E-devlet'te kullanılan gözetim ve kayıt teknolojilerinin mahremiyet üzerinde etkileri. Abant İzzet Baysal Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, 18, s. 95-120.

Taylor JW, 1974. The role of risk in consumer behaviour, Journal of Marketing, 38, p. 54- 60.

Than Win K, 2005. A review of security of electronic health records. Health Information Management, 34, 1, p. 13.

Thilakanathan D, Calvo RA, Chen S, Nepal S, Glozier, N, 2016. Facilitating secure sharing of personal health data in the cloud. JMIR Medical Informatics, 4, 2, p. 1-18. doi:http://dx.doi.org/10.2196/medinform.4756.

Turan Başara G, 2020. Kişisel veri işleme sözleşmesi. Uyuşmazlık Mahkemesi Dergisi, 16, s. 57-90. https://dergipark.org.tr/en/pub/mdergi/issue/58747/848195.

Türkmen S, 2019. Özel nitelikli kişisel verilerinin işlenmesinde açık rızanın aranmadığı haller. Yüksek Lisans Tezi, İstanbul Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul.

Türkmendağ T, Uygur S, 2020. An investigation of the effect of perceived risk on repurchase intention in online vacation purchases. Turizm Akademik Dergisi, 7, 2, p. 255-66.

Ueltschy LC, Krampf RF, Yannopoulos P, 2004. A cross national study of perceived consumer risk towards online (internet) purchasing, The Multinational Business Review, 12, 2, p. 59-82.

Veri İhlali İstatistiği: Kapsamlı Rehber 2020, 2020. Erişim Adresi https://lundodata.com/veri-ihlali-istatistigi/, Erişim Tarihi: 25 Mart 2022.

Wang T, Duong TD, Chen CC, 2016. Intention to disclose personal information via bobile applications: a privacy calculus perspective. International Journal of Information Management, 36, 4, p. 531-42.

Warner J, 2005. The right to oblivion: data retention from canada to europe in three backward steps. University of Ottawa Law & Technology Journal, 2, 75, p. 75- 104.

Weisz JR, Stipek DJ, 1982. Competence, contingency, and the development of perceived control. Human Development, 25, p. 250-81.

Westin A, 1967. Privacy and freedom. New York: Atheneum.

Win KT, Susilo, W, Mu Y, 2006. Personal health record systems and their security protection. Journal of medical systems, 30, 4, p. 309-15.

Wu HL, Liu CY, Hsu WH, 2008. An Integrative Model of Customers' Perceptions of Health Care Services inTaiwan. The Service Industries Journal. 28, 9, p. 1307-19.

Xu H, Dinev T, Smith HJ, Hart P, 2008. Examining the formation of individual's privacy concerns: Toward an integrative view. ICIS 2008 Proceedings p. 1-16. Erişim tarihi 20 Ağustos 2021, Erişim adresi:http://aisel.aisnet.org/icis2008/6.

Xu H, Dinev T, Smith J, Hart P, 2011b. Information privacy concerns: linking individual perceptions with institutional privacy assurances. Journal of the Association for Information Systems, 12, 12, p. 798-824.

Xu H, Gupta S, Rosson MB, Carroll JM, 2012. Measuring mobile users' concerns for information privacy. Proceedings of 33rd Annual International Conference on Information Systems. s. 1-16, 19 Aralık 2012, Orlando, FL.

Xu H, Luo X, Carroll JM, Rosson MB, 2011a. The personalization privacy paradox: an exploratory study of decision making process for location-aware marketing. Decision Support Systems 51, 42–52.

Xu H, Teo HH, Tan BCY, Agarwal R, 2009. The role of push–pull technology in privacy calculus: the case of location-based services. Journal of Management Information System, 26, 3, p. 135-73.

Yaka D, 2018.Tüketici yenilikçiliği ve algılanan riskin alışverişte self servis teknolojilerini kullanma niyeti üzerindeki etkileri. Yüksek Lisans Tezi, Çukurova Üniversitesi Sosyal Bilimler Enstitüsü, Adana.

Yao MZ, Rice ER, Wallis K, 2007. Predicting user concerns about online privacy. Journal of the American Society For Information Science and Technology, 58, 5, p. 710–22.

Yıldırım BF, 2019. Sağlığın kişiselleşmesi ve kişisel sağlık bilgi sistemleri. Bilgi Yönetimi Dergisi, 2, 2, s. 127-35.

Yılmaz E, 2018. Türk ceza kanunu'nun kişisel verilerin korunmasına ilişkin maddeleri. Erişim tarihi 16 Ocak 2021. Erişim dresi,https://www.kisiselverilerinkorunmasi.org/mevzuat/5237-sayili-turk-ceza-kanunu/.

Yılmaz M, 2009. Enformasyon ve bilgi kavramları bağlamında enformasyon yönetimi ve bilgi yönetimi. Ankara Üniversitesi Dil ve Tarih Coğrafya Fakültesi Dergisi, 49, 1, s. 95-118.

Youn S, 2009. Determinants of online privacy concern and its influence on privacy protection behaviors among young adolescents. *Journal of Consumer affairs*, 43, 3, 389-418.

Yücedağ N, 2017. Medeni hukuk açısından kişisel verilerin korunması kanunu'nun uygulama alanı ve genel hukuka uygunluk sebepleri. İstanbul Üniversitesi Hukuk Fakültesi Mecmuası(İÜHFM), LXXV, 2, s. 765-89.

Yüksel G, 2018. Kişisel sağlık verilerinin hukuki korunması. Sağlık Akademisyenleri Dergisi, 6, 1, s. 1-10.

Zambrano-Cruz R, Cuartas-Montoya GP, Meda-Lara RM, Palomera-Chávez A, Tamayo-Agudelo W, 2018. Perception of risk as a mediator between personality and perception of health: test of a model. Psychology Research and Behavior Management, 11, p. 417-23.

Zeithaml VA, 1988. Consumer Perceptions of Price, Quality, and Value: A Means-End Model and Synthesis Of Evidence. *Journal of Marketing*. 52, 3, p. 2-22.

Zeybek Ünsal Ç, Örnek Büken N, 2018. Biyotıp araştırmaları ile ilgili olarak, "kişisel verilerin korunması kanunu" ve "kişisel sağlık verilerinin işlenmesi ve mahremiyetinin sağlanması hakkında yönetmelik" ne diyor?. Turkiye Klinikleri J Med Ethics Law Hist-Special Topic, 4, 1, s. 82-90.

Zhao H, Li Y, 2012. Research on the ınfluence of perceived risk in consumer on-line purchasing decision. Physics Procedia, 24, p. 1304-10.

Zhao L, Lu Y, Gupta S, 2012. Disclosure intention of location-related information in location-based social network services. International Journal of Electronic Commerce, 16, 4, p. 53-90.

Zlatolas LN, Welzer T, Hölbl M, Heričko M, Kamišalić A, 2019. A model of perception of privacy, trust, and self- disclosure on online social networks. Entropy, 21, 8, p. 1-17.

Žliobaitė I, Custers, B, 2016. Using sensitive personal data may be necessary for avoiding discrimination in data-driven decision models. Artificial Intelligence and Law, 24, 2, p. 183-201.

7. EKLER

EK-A: Anket Formu

Sayın Katılımcı,

Aşağıdaki sorulara vereceğiniz yanıtlar, bilimsel bir çalışmaya katkı sağlayacağından, büyük önem taşımaktadır. Katkınız için şimdiden teşekkür ederiz.

1. Cinsiyetiniz: ( ) Kadın ( )Erkek

2. Yaşınız:
( )18-29
( )30-39
( )40-49
( )50-59
( )60 ve üstü

3. Öğrenim Durumunuz:
( )İlköğretim
( )Lise
( )Üniversite
( )Lisansüstü

4. Annenizin Öğrenim Durumu:
( )İlköğretim
( )Lise
( )Üniversite
( )Lisansüstü

5. Babanızın Öğrenim Durumu:
( )İlköğretim
( )Lise
( )Üniversite
( )Lisansüstü

6. Şuan yaşadığınız şehir?
( )İzmir ( )Adana ( )Konya

7. Aylık Gelir Düzeyiniz:
( ) 2300 TL ve Altı
( ) 2301 TL –3800 TL
( ) 3801 TL - 5000TL
( ) 5001 TL ve Üstü

8. Mesleğiniz nedir?……..….

9. Bir günde internette kaç saat geçiriyorsunuz?
( )Hiç
( )1-2
( )3-4
( )5-6
( )7 ve Üstü

10. E-nabız uygulamasını kullanıyor musunuz?
( )Evet ( )Hayır

11. Kronik Hastalığınız var mı?
( ) Evet ( ) Hayır

12. Yılda Ortalama Kaç Defa Sağlık Kurumuna Gidiyorsunuz?
( )Hiç
( )1-2
( )3-4
( )5-6
( )7 ve Üstü

13. Yaşamınızı çoğunlukla geçirdiğiniz yer:
( )Köy-Kasaba
( )İlçe
( )Şehir
( )Büyükşehir

14. Hayat Eve Sığar Uygulamasını Kullanıyor Musunuz?
( )Evet ( )Hayır

15. HES Kodunuzu paylaşmaktan rahatsızlık duyuyor musunuz?
( )Evet ( )Hayır

16. Hastanelere Hiç Parmak İzi Kaydı Verdiniz Mi?
( )Evet ( )Hayır

17. Randevu alırken aşağıdaki yöntemlerden hangisini/hangilerini kullanıyorsunuz?
( )MHRS ( )182 ( )Hastaneyi Aramak

18. Hastane Bilgi Yönetim Sistemlerininözel yazılım şirketleri tarafından yürütüldüğünü biliyor musunuz?
( )Evet ( )Hayır

19. Hastalık geçmişiniziher hekimin görmesi veri güvenliği açığı mıdır?
( )Evet ( )Hayır

EK-A: Anket Formu (Devam)

		Hiç Katılmıyorum	Katılmıyorum	Orta Düzeyde Katılıyorum	Katılıyorum	Tamamen Katılıyorum
Gizlilik Endişesi						
1	Sağlık kuruluşlarında kişisel bilgilerimi paylaşmam noktasında belirsizlikler mevcuttur.	1	2	3	4	5
2	Sağlık kuruluşlarında kişisel bilgilerimin paylaşım esnasında kaybolma ihtimali yüksektir.	1	2	3	4	5
3	Sağlık kuruluşları ile paylaştığım kişisel bilgilerimin kötüye kullanılma ihtimali vardır.	1	2	3	4	5
4	Sağlık kuruluşlarında paylaşılan bilgiler siber saldırılar gibi, öngörülemeyen birçok sorun içermektedir.	1	2	3	4	5
Algılanan Kontrol						
5	Sağlık kuruluşlarında sağlık personeli ile teşhis ve tedavi işlemleri sırasında paylaşılacak bilgilerin neler olduğunun farkındayım.	1	2	3	4	5
6	Sağlık personeli ile iletişimim sırasında toplanan bilgilerimin sağlık personeli tarafından nasıl kullanılacağını kontrol ettiğime inanıyorum.	1	2	3	4	5
7	Tedavi sürecinde verdiğim bilgileri daha sonra doğrulayabileceğime yani veriyi paylaştıktan sonra düzeltebileceğime inanıyorum.	1	2	3	4	5

		Hiç Katılmıyorum	Katılmıyorum	Nadiren Katılmıyorum	Orta Düzeyde katılıyorum	Kısmen Katılıyorum	Katılıyorum	Tamamen Katılıyorum
Algılanan Riskler								
8	Kişisel bilgilerimin e-nabız gibi mobil uygulamalarla paylaşılması beklenmedik problemleri beraberinde getirebilir.	1	2	3	4	5	6	7
9	Kişisel bilgilerimi e-nabız gibi mobil uygulamalarda paylaşmak üçüncü kişilerin erişimi açısından risk içermektedir.	1	2	3	4	5	6	7
10	Kişisel bilgilerimin veri aktarımı sürecindeki kayıp potansiyeli yüksektir.	1	2	3	4	5	6	7

EK-A: Anket Formu (Devam)

Algılanan Fayda								
11	Sağlık personeli ile veri paylaşmak ve e-sağlık uygulamalarını kullanmak, ihtiyacım olan sağlık bilgilerimi bulmak için arama süremi kısaltır.	1	2	3	4	5	6	7
12	Sağlık personeli ile veri paylaşmak ve e-sağlık uygulamalarını kullanmak ihtiyaç duyduğum sağlık bilgilerime anında ulaşma kolaylığı sağlar.	1	2	3	4	5	6	7
13	Genel olarak, sağlık personeli ile veri paylaşmanın ve e-sağlık uygulamalarını kullanmanın faydalı olduğunu düşünüyorum.	1	2	3	4	5	6	7
Veri Paylaşma Niyeti								
14	Sağlık personeli ile kişisel bilgilerimi paylaşma ihtimalim var.	1	2	3	4	5	6	7
15	Sağlık personeli ile kişisel bilgilerimi paylaşırım.	1	2	3	4	5	6	7
16	Sağlık personeli ile ürün ve hizmet gelişimi için kişisel bilgilerimin paylaşılması benim için genellikle mümkündür.	1	2	3	4	5	6	7

8. TURNİTİN RAPORU

TEZ SON HALİ

Yazar Havvanur Atalay

Gönderim Tarihi: 09-Haz-2022 11:34AM (UTC+0300)
Gönderim Numarası: 1853503436
Dosya adı: TURN_T_N.docx (986.11K)
Kelime sayısı: 15904
Karakter sayısı: 108812

TEZ SON HALİ

ORİJİNALLİK RAPORU

%16	%15	%3	%5
BENZERLİK ENDEKSİ	İNTERNET KAYNAKLARI	YAYINLAR	ÖĞRENCİ ÖDEVLERİ

BİRİNCİL KAYNAKLAR

1	acikbilim.yok.gov.tr İnternet Kaynağı	%3
2	dergipark.org.tr İnternet Kaynağı	%3
3	2793ed39-269b-4a6e-bfbb-1dd53eb9ddcb.filesusr.com İnternet Kaynağı	%2
4	toad.halileksi.net İnternet Kaynağı	%1
5	9lib.net İnternet Kaynağı	<%1
6	Submitted to Nigde University Öğrenci Ödevi	<%1
7	javstudies.com İnternet Kaynağı	<%1
8	Submitted to Selçuk Üniversitesi Öğrenci Ödevi	<%1
9	gorkemtopuz.com İnternet Kaynağı	<%1

10	docplayer.biz.tr İnternet Kaynağı	<%1
11	acikerisimarsiv.selcuk.edu.tr:8080 İnternet Kaynağı	<%1
12	Submitted to Istanbul Bilgi University Öğrenci Ödevi	<%1
13	acikerisim.ybu.edu.tr:8080 İnternet Kaynağı	<%1
14	isletmecilik.org İnternet Kaynağı	<%1
15	www.acarindex.com İnternet Kaynağı	<%1
16	www.rizasaka.av.tr İnternet Kaynağı	<%1
17	Submitted to Istanbul Gelisim University Öğrenci Ödevi	<%1
18	dergi.comu.edu.tr İnternet Kaynağı	<%1
19	publication.codesria.org İnternet Kaynağı	<%1
20	www.hukukihaber.net İnternet Kaynağı	<%1
21	Submitted to Istanbul Aydin University Öğrenci Ödevi	<%1

22	odk.sdu.edu.tr İnternet Kaynağı	<%1
23	www.eab.org.tr İnternet Kaynağı	<%1
24	acikerisim.selcuk.edu.tr:8080 İnternet Kaynağı	<%1
25	dspace.gazi.edu.tr İnternet Kaynağı	<%1
26	Submitted to Bahcesehir University Öğrenci Ödevi	<%1
27	Submitted to Gaziantep Aniversitesi Öğrenci Ödevi	<%1
28	jurix.com.tr İnternet Kaynağı	<%1
29	www.jshsr.org İnternet Kaynağı	<%1
30	siyasetekonomiyonetim.org İnternet Kaynağı	<%1
31	Submitted to Ankara University Öğrenci Ödevi	<%1
32	Submitted to Bülent Ecevit Üniversitesi Öğrenci Ödevi	<%1
33	www.researchgate.net İnternet Kaynağı	<%1

34	Submitted to Beykent Universitesi Öğrenci Ödevi	<%1
35	Submitted to Eskisehir Osmangazi University Öğrenci Ödevi	<%1
36	www.reportshop.co.kr İnternet Kaynağı	<%1
37	tr.wer.wiki İnternet Kaynağı	<%1
38	docs.neu.edu.tr İnternet Kaynağı	<%1
39	dspace.akdeniz.edu.tr İnternet Kaynağı	<%1
40	openaccess.hku.edu.tr İnternet Kaynağı	<%1
41	www.mbkaya.com İnternet Kaynağı	<%1
42	Submitted to The Scientific & Technological Research Council of Turkey (TUBITAK) Öğrenci Ödevi	<%1
43	docs.wixstatic.com İnternet Kaynağı	<%1
44	etd.lib.metu.edu.tr İnternet Kaynağı	<%1
45	etd.repository.ugm.ac.id İnternet Kaynağı	

		<%1
46	iibf.gediz.edu.tr İnternet Kaynağı	<%1
47	www.avukatkatipleri.com İnternet Kaynağı	<%1
48	www.eset.com İnternet Kaynağı	<%1
49	www.saglikaktuel.com İnternet Kaynağı	<%1
50	Submitted to Kastamonu University Öğrenci Ödevi	<%1
51	Submitted to Police Academy Öğrenci Ödevi	<%1
52	openaccess.hacettepe.edu.tr:8080 İnternet Kaynağı	<%1
53	www.erdemirozmen.com İnternet Kaynağı	<%1
54	www.phdernegi.org İnternet Kaynağı	<%1
55	www.sdergi.hacettepe.edu.tr İnternet Kaynağı	<%1
56	www1.mmo.org.tr İnternet Kaynağı	<%1

57	M. Taha TÜFEK, Arda AKTAŞ, Serkan TAŞ. "The Impact of COVID-19 on Physiotherapists' Professional Education Activities: Cross-Sectional Study", Turkiye Klinikleri Journal of Health Sciences, 2022 Yayın	<%1
58	academicrepository.khas.edu.tr İnternet Kaynağı	<%1
59	ayam.anayasa.gov.tr İnternet Kaynağı	<%1
60	nek.istanbul.edu.tr:4444 İnternet Kaynağı	<%1
61	vs1.doczz.cz İnternet Kaynağı	<%1
62	2019.fmgtegitimikongresi.com İnternet Kaynağı	<%1
63	www.oyunyardim.com İnternet Kaynağı	<%1

Alıntıları çıkart Kapat

Eşleşmeleri çıkar Kapat

Bibliyografyayı Çıkart Kapat