



T.C.

SİVAS CUMHURİYET ÜNİVERSİTESİ

SAĞLIK BİLİMLERİ ENSTİTÜSÜ

**SAĞLIK YÖNETİMİ BÖLÜMÜ ÖĞRENCİLERİNİN DİJİTAL
VATANDAŞLIK VE DİJİTAL VERİ GÜVENLİĞİ FARKINDALIĞI
ARASINDAKİ İLİŞKİNİN İNCELENMESİ**

ŞEVVAL ÇİSİL CAJUSTE

0000-0002-9814-9238

YÜKSEK LİSANS TEZİ

SAĞLIK YÖNETİMİ ANABİLİM DALI

SİVAS

EYLÜL 2024

T.C.
SİVAS CUMHURİYET ÜNİVERSİTESİ
SAĞLIK BİLİMLERİ ENSTİTÜSÜ

**SAĞLIK YÖNETİMİ BÖLÜMÜ ÖĞRENCİLERİNİN DİJİTAL
VATANDAŞLIK VE DİJİTAL VERİ GÜVENLİĞİ FARKINDALIĞI
ARASINDAKİ İLİŞKİNİN İNCELENMESİ**

ŞEVVAL ÇİSİL CAJUSTE

YÜKSEK LİSANS TEZİ

SAĞLIK YÖNETİMİ ANABİLİM DALI

TEZ DANIŞMANI
PROF. DR. HATİCE ULUSOY

SİVAS-2024



Bu tez, Sivas Cumhuriyet Üniversitesi Senatosu’nun 2023 tarihli ve 2/9 sayılı kararı ile kabul edilen Sağlık Bilimleri Enstitüsü Lisansüstü Tez Yazım Kılavuzuna göre hazırlanmıştır.

TEŞEKKÜR

Lisans ve yüksek lisans eğitim süreçlerimde beni başarıya taşıyan, engin bilgi birikimi ve yönlendirmeleri ile yolumu aydınlatan saygı değer danışmanım Prof. Dr. Hatice Ulusoy'a içten teşekkürlerimi sunarım. Kendisinin özverili rehberliği, akademik başarılarımın temelini oluşturdu.

Eğitim hayatımın her aşamasında maddi ve manevi destekleriyle her daim yanımda olan annem Lütfiye Demiralp ve babam Ahmet Demiralp'e en derin teşekkürlerimi ifade ederim. Ailemin sağladığı güçlü destek, beni bu günlere getiren önemli bir itici güç oldu.

Kardeşlerim Tuğba Demiralp ve Kübra Demiralp'e de teşekkür ederim. Onların samimi desteği, bu sürecin daha anlamlı olmasını sağladı.

Eşim Djeby Cajuste'a tez sürecimdeki sürekli motivasyonu ve yanımda oluşu için sonsuz teşekkürlerimi iletiyorum. Onun destekleri, bu zorlu yolculuğun daha kolay atlatılmasını sağladı. Bu süreçte emeği geçen herkese teşekkür ediyor, saygılarımı sunuyorum.

ÖZET

SAĞLIK YÖNETİMİ BÖLÜMÜ ÖĞRENCİLERİNİN DİJİTAL VATANDAŞLIK VE DİJİTAL VERİ GÜVENLİĞİ FARKINDALIKLARI ARASINDAKİ İLİŞKİNİN İNCELENMESİ

ŞEVVAL ÇİSİL CAJUSTE YÜKSEK LİSANS TEZİ
SAĞLIK YÖNETİMİ ANABİLİM DALI
DANIŞMAN: PROF.DR. HATİCE ULUSOY
2024, xiv, 80 sayfa

Günümüzde, sağlık sektöründe sürekli yeni teknolojik gelişmeler yaşanmaktadır. Bu ilerlemeler, sağlık çalışanları ve geleceğin sağlık yöneticileri için bu teknolojilere etkin bir şekilde uyum sağlama zorunluluğunu beraberinde getirmektedir. Bu hızlı teknolojik değişimlerle birlikte, dijital vatandaşlık ve dijital veri güvenliği kavramları öne çıkmış, sağlık profesyonellerinin bu alanlarda bilinçli ve yetkin olması gerekliliği daha da belirgin hale gelmiştir. Giderek dijitalleşen sağlık sektöründe dijital vatandaşlık ve dijital veri güvenliği, hasta ve çalışan güvenliğini ve sağlık verilerinin korunmasını sağlamak için de kritik bir rol oynamaktadır.

Dijital vatandaşlık, sağlık profesyonellerinin ve hastaların dijital ortamda etik davranışlar sergileme sorumluluğunu içerir. Bu, hasta gizliliği, bilgi paylaşımı ve dijital platformlarda etik değerlere uygun bir şekilde hareket etmeyi kapsar. Sağlık profesyonellerinin dijital vatandaşlık konusunda bilinçli olması, güvenilir bir sağlık hizmet sunumu için önemlidir. Dijital veri güvenliği ise, hasta ve çalışan bilgilerinin yetkisiz erişimlere karşı korunmasını sağlamak amacıyla alınan önlemleri ifade eder. Hastaların özel sağlık verilerinin güvenli bir şekilde saklanması, siber tehditlere karşı dirençli bir yapı oluşturulması, sağlık sektörünün bütünlüğünü ve güvenilirliğini sürdürmek açısından kritiktir.

Bu çalışma sağlık yönetimi bölümü öğrencilerinin dijital vatandaşlık ve dijital veri güvenliği farkındalıkları arasındaki ilişkinin saptanması amacıyla tanımlayıcı olarak yapılmıştır. Çalışmaya 221 öğrenci katılmıştır. Veriler Kişisel Bilgi Formu, Dijital Vatandaşlık Ölçeği ve Dijital Veri Güvenliği Farkındalığı Ölçeği ile Google Forms aracılığıyla (30.05.23-15.06.23) tarihleri arasında toplanmıştır. Çalışmanın sonuçlarına göre öğrencilerin dijital vatandaşlık ölçeği ortalaması ($\bar{x}=4,06$) dijital veri güvenliği farkındalığı ölçeği ($\bar{x}=3,09$) ortalamasına göre yüksek düzeyde bulunmuştur. Dijital vatandaşlık ölçeği ve dijital veri güvenliği farkındalığı ölçeği toplam puanları

değerlendirildiğinde öğrencilerin dijital vatandaşlık düzeyleri ile dijital veri güvenliği farkındalıkları arasında pozitif yönlü, yüksek düzeyde ve istatistiksel olarak anlamlı ilişki bulunduğu saptanmıştır (%73.8, $p<0.001$). Dijital veri güvenliği farkındalıkları ile dijital vatandaşlık alt boyutları arasında (sağlık %61.3, erişim %60.7, doğru kullanım %69.7, toplumsal sorumluluk %51.5, çevrimiçi işlemler %61.6,) pozitif yönlü orta düzeyde ve istatistiksel olarak anlamlı ilişki saptanmıştır.

Sosyodemografik özelliklere göre incelendiğinde; günlük 8 saatten fazla ($\bar{x}=4,24$) veya 2 saatten az ($\bar{x}=4,24$) internet kullananların, 16.000 lira ve üstü aile geliri olanların ($\bar{x}=4,22$), tablete sahip olanların ($\bar{x}=4,21$), günlük 8 saat ve üzerinde sosyal medya kullananların ($\bar{x}=4,27$); dijital vatandaşlık düzeyi, istatistiksel olarak anlamlı düzeyde yüksek bulunmuştur. Erkek öğrencilerin ($\bar{x}=4,08$), günlük 0-2 saat arasında internet kullananların ($\bar{x}=4,26$), 16.000 lira ve üstü aile geliri olanların ($\bar{x}=4,15$), bilgisayar ($\bar{x}=4,05$) veya tablete ($\bar{x}=4,17$) sahip olanların, günlük 8 saat ve üzerinde sosyal medya kullanımı olanların ($\bar{x}=4,14$); dijital veri güvenliği farkındalığı, istatistiksel olarak anlamlı düzeyde yüksek bulunmuştur. Ayrıca öğrencilerin %98,20'sinin sosyal medya kullandığı ve %33,9'unun günde 6 saat ve üzerinde internet kullandığı saptanmıştır. Bu bulgu, potansiyel bir bağımlılığa işaret edebileceğinden, ileride yapılacak araştırmalarda bu konunun detaylı bir şekilde incelenmesi önerilmiştir.

Sonuç olarak sağlık yönetimi bölümü öğrencilerinin dijital vatandaşlık düzeyleri ile dijital veri güvenliği farkındalıkları arasında pozitif yönlü, yüksek düzeyde ve istatistiksel olarak anlamlı ilişki bulunmaktadır. Öğrencilerin dijital vatandaşlık ortalaması dijital veri güvenliği farkındalığı ortalamasına göre yüksek düzeyde bulunmuştur.

Araştırmada öğrencilerin dijital vatandaşlık ve özellikle dijital veri güvenliği farkındalıklarının çeşitli eğitimlerle artırılması ayrıca, öğrencilere dijital vatandaşlığın sağlık ve toplumsal sorumluluk alt faktörleri konusunda bilinç kazandırılması, internet bağımlılığı konusunda farkındalık yaratılması önerilmiştir.

Anahtar Kelimeler: Dijital Vatandaşlık, Dijital Veri Güvenliği Farkındalığı, Sağlık Yönetimi Bölümü Öğrencileri, Üniversite Öğrencileri

ABSTRACT

SAĞLIK YÖNETİMİ BÖLÜMÜ ÖĞRENCİLERİNİN DİJİTAL VATANDAŞLIK VE DİJİTAL VERİ GÜVENLİĞİ FARKINDALIKLARI ARASINDAKİ İLİŞKİNİN İNCELENMESİ

ŞEVVAL ÇİSİL CAJUSTE

YÜKSEK LİSANS TEZİ

SAĞLIK YÖNETİMİ ANABİLİM DALI

SUPERVİSOR: PROF.DR. HATİCE ULUSOY

2024, xiv , 80 sayfa

Today, there are continuous new technological developments in the health sector. These advances bring along the necessity for healthcare professionals and future healthcare managers to adapt to these technologies effectively. With these rapid technological changes, the concepts of digital citizenship and digital data security have come to the fore, and the necessity for healthcare professionals to be conscious and competent in these areas has become more evident. In the increasingly digitalised healthcare sector, digital citizenship and digital data security play a critical role in ensuring patient and employee safety and the protection of health data.

Digital citizenship includes the responsibility of healthcare professionals and patients to demonstrate ethical behaviour in the digital environment. This includes patient confidentiality, information sharing and acting in accordance with ethical values on digital platforms. It is important for healthcare professionals to be aware of digital citizenship for a reliable healthcare service delivery. Digital data security refers to the measures taken to ensure that patient and employee information is protected against unauthorised access. Storing patients' private health data securely, creating a structure resistant to cyber threats is critical to maintain the integrity and reliability of the health sector.

This descriptive study was conducted to determine the relationship between digital citizenship and digital data security awareness of health management students. 221 students participated in the study. Data were collected through Personal Information Form, Digital Citizenship Scale and Digital Data Security Awareness Scale via Google Forlar between (30.05.23-15.06.23) dates. According to the results of the study, the mean of the digital citizenship scale ($\bar{x}=4,06$) was found to be at a higher level than the mean of the digital data security awareness scale ($\bar{x}=3,09$). When the total scores of the digital citizenship scale and digital data security awareness scale

were evaluated, it was found that there was a positive, high level and statistically significant relationship between the digital citizenship levels of the students and their digital data security awareness (73.8%, $p<0.001$). A positive, moderate and statistically significant relationship was found between digital data security awareness and digital citizenship sub-dimensions (health 61.3%, access 60.7%, correct use 69.7%, social responsibility 51.5%, online transactions 61.6%).

When analysed according to sociodemographic characteristics; the digital citizenship level of those who use the internet for more than 8 hours a day ($\bar{x}=4,24$) or less than 2 hours a day ($\bar{x}=4,24$), have a family income of 16.000 liras or more ($\bar{x}=4,22$), own a tablet ($\bar{x}=4,21$), use social media for 8 hours or more a day ($\bar{x}=4,27$) was found to be statistically significantly higher. The digital data security awareness of male students ($\bar{x}=4,08$), those who use the internet between 0-2 hours daily ($\bar{x}=4,26$), those who have a family income of 16.000 liras and above ($\bar{x}=4,15$), those who have a computer ($\bar{x}=4,05$) or tablet ($\bar{x}=4,17$), those who use social media for 8 hours or more daily ($\bar{x}=4,14$) were found to be statistically significantly higher. In addition, it was found that 98.20% of the students used social media and 33.9% of them used the internet for 6 hours or more per day. Since this finding may indicate a potential addiction, it is suggested that this issue should be examined in detail in future studies.

As a result, there is a positive, high level and statistically significant relationship between digital citizenship levels and digital data security awareness of health management students. The students' digital citizenship average was found to be at a higher level than the average of digital data security awareness. In the study, it was suggested that students' digital citizenship and especially digital data security awareness should be increased with various trainings, and it was also suggested that students should be made aware of the health and social responsibility sub-factors of digital citizenship, and awareness should be raised about internet addiction.

Keywords: Digital Citizenship, Digital Data Security Awareness, Health Management Department Students, University Students

İÇİNDEKİLER

TEŞEKKÜR.....	IV
ÖZET.....	v
ABSTRACT.....	vii
İÇİNDEKİLER.....	ix
TABLolar DİZİNİ.....	xi
ŞEKİLLER DİZİNİ	xii
GRAFİKLER DİZİNİ.....	xiii
KISALTMALAR LİSTESİ.....	xiv
1.GİRİŞ.....	1
1.1 Problemin Tanımı ve Önemi.....	1
1.2. Araştırmanın Amacı.....	4
1.3. Araştırmanın Sınırlıkları.....	4
1.4. Araştırmanın Hipotezleri.....	4
2.GENEL BİLGİLER.....	5
2.1 Vatandaşlık Kavramı.....	5
2.1.1.Dijital Vatandaşlık.....	6
2.1.2.Dijital Vatandaşlığın Boyutları.....	8
2.1.3.Türkiye ve Dünyada Sağlık Alanındaki Dijital Vatandaşlık Projeleri.....	16
2.2. Dijital Veri Güvenliği Farkındalığı.....	22
2.2.1. Dijital Veri Güvenliği.....	22
2.2.2. Dijital Veri Güvenliğini Tehdit Eden Unsurlar.....	23
2.2.3. Sağlıkta Dijital Veri Güvenliği Farkındalığı.....	27

2.2.4. Türkiye’de ve Dünyada Dijital Veri Güvenliğini Sağlamak Amacıyla Yapılan Faaliyetler.....	28
3. GEREÇ VE YÖNTEM.....	33
3.1. Araştırmanın Tipi.....	33
3.2. Araştırmanın Yapıldığı Yer ve Özellikleri.....	33
3.3. Araştırmanın Evreni ve Örneklemi.....	33
3.4. Veri Toplama Araçları.....	33
1. Kişisel Bilgi Formu.....	33
2. Dijital Vatandaşlık Ölçeği.....	34
3. Dijital Veri Güvenliği Farkındalığı Ölçeği.....	34
3.5. Verilerin Toplanması.....	35
3.6. Verilerin Değerlendirilmesi.....	35
3.7. Araştırmanın Etik Yönü.....	35
4. BULGULAR.....	37
5. TARTIŞMA.....	50
6. SONUÇ ve ÖNERİLER.....	57
6.1. Sonuçlar.....	58
6.2. Öneriler.....	59
KAYNAKLAR.....	62

TABLÖLAR DİZİNİ

Tablo 1: Sosyodemografik verilere ilişkin parametrelerin dağılımı.....	36
Tablo 2: Ölçek alt boyutlarına ilişkin bilgiler.....	37
Tablo 3: Sosyodemografik özelliklere göre Dijital Veri Güvenliği Farkındalık Ölçeği'nin değerlendirilmesi.....	37
Tablo 4: Sosyodemografik özelliklere göre Dijital Vatandaşlık Ölçeği'nin değerlendirilmesi.....	39
Tablo 5: Sosyodemografik özelliklere göre Dijital Vatandaşlık Ölçeği Doğru Kullanım alt faktörünün değerlendirilmesi.....	40
Tablo 6: Sosyodemografik özelliklere göre Dijital Vatandaşlık Ölçeği Çevrimiçi İşlemler alt faktörünün değerlendirilmesi.....	41
Tablo 7: Sosyodemografik özelliklere göre Dijital Vatandaşlık Ölçeği Sağlık alt faktörünün değerlendirilmesi.....	43
Tablo 8: Sosyodemografik özelliklere göre Dijital Vatandaşlık Ölçeği Erişim alt faktörünün değerlendirilmesi.....	44
Tablo 9: Sosyodemografik özelliklere göre Dijital Vatandaşlık Ölçeği Toplumsal Sorumluluk alt faktörünün değerlendirilmesi.....	45
Tablo 10: Dijital Veri Güvenliği Farkındalık Ölçeği ile Dijital Vatandaşlık Ölçeği ve alt boyutları arasındaki korelasyonun değerlendirilmesi.....	46

ŞEKİLLER DİZİNİ

Şekil 1: Dijital Vatandaşlığın Boyutları (Kaynak: Ribble, 2023)	8
Şekil 2: Bilgi Güvenliği İlkeleri (Kaynak: Fussel,2005).....	22
Şekil 3: Siber Güvenlik Eğitimi Hedefleri (Kaynakça: SGEP,2017).....	29
Şekil 4: Siber Güvenlik Çerçevesi (Kaynak: Nist, 2023).....	31



GRAFİKLER DİZİNİ

Grafik 1: Hanelerde İnternet Erişim İmkânı ve Bireylerde İnternet Kullanımı, 2012-2022 (Kaynak: TÜİK, 2022).....	10
Grafik 2: İnternette Satın Alma Oranı, 2012-2023 (TÜİK 2022).....	12



KISALTMALAR LİSTESİ

AB:	Avrupa Birliği
BGYS:	Bilgi Güvenliği Yönetim Sistemi
BTK:	Bilgi Teknolojileri ve İletişim Kurumu
CDC:	Hastalık Kontrol ve Önleme Merkezleri
CIS:	İnternet Güvenliği Merkezi
EHR:	Elektronik Sağlık Kayıtları
EMR:	Elektronik Tıbbi Kayıtları
GDPR:	Genel Veri Koruma Düzenlemesi
GDPR:	Genel Veri Koruma Yönetmeliği
HIPAA:	Sağlık Sigortası Taşınabilirlik ve Sorumluluk Yasası
IEC:	Uluslararası Elektronik Komisyonu
ISO:	Uluslararası Standartlar Teşkilatı
KVKK:	Kişisel Verilerin Korunması Kanunu
MHealth:	Mobil sağlık
MHRS:	Merkezi Hekim Randevu Sistemi
NIST:	Ulusal Standartlar ve Teknoloji Enstitüsü
SAS:	Sağlıkta Akreditasyon Standartları
SGEP:	Siber Güvenlik Eğitim ve Farkındalık Programları
SKS:	Sağlıkta Kalite Standartları
SOME:	Siber Olaylara Müdahale Ekipleri
TSE:	Türk standartları enstitüsü
TÜİK:	Türkiye İstatistik Kurumu
USOM:	Ulusal Siber Olaylara Müdahale Merkezi

1.GİRİŞ

1.1. Problemin Tanımı ve Önemi

Teknolojik gelişmelerin hız kazanmasıyla birlikte, bireylerin yaşam standartlarında önemli değişimler yaşanmıştır. Sağlıktan eğitime, endüstriden iletişime kadar pek çok alanda teknolojinin etkisi gözlemlenmiştir. Bu değişimler, literatürde yeni terimler ve tanımlamaların ortaya çıkmasına da neden olmuştur, bu kavramlardan biri de ‘‘dijital vatandaşlık kavramıdır’’ (Yılmaz ve Doğusoy 2020: 2364). Geleneksel vatandaşlık anlayışının geride bırakılması, bireyleri ortak bir noktada birleştiren dijital vatandaşlık kavramının ortaya çıkmasını sağlamıştır (Sarı ve Taşer 2018: 1064).

Çubukçu ve Bayzan’a göre dijital vatandaş, bilgi ve iletişim kaynaklarını kullanma konusunda eleştirel düşünceye sahip, çevrimiçi davranışların etik sonuçlarının bilincinde olan, teknolojiyi başkalarına zarar vermeden etkili bir biçimde kullanabilen, internet ortamında iletişim haklarını doğru bir şekilde kullanmayı bilen, paylaşımlarında ve iş birliğinde doğru tutumu sergileyen ve diğer bireyleri de bu konuda teşvik eden kişidir. Dijital vatandaşlık ise, temel olarak teknoloji kullanımıyla ilgili hak ve sorumlulukları içeren davranış normlarını ifade eder (Çubukçu ve Bayzan 2013: 148). Bu bağlamda, dijital vatandaşlık kavramı, dijital ortamda etik davranış sergileme, güvenlik önlemleri alma ve olumlu ya da olumsuz durumlara hazırlıklı olma gibi konularda pozitif davranış gösteren bireyleri tanımlamak için kullanılmaktadır (Som Vural ve Kurt 2018: 63). Ribble ve Bailey dijital vatandaşlığı teknoloji kullanımına ilişkin davranış normları olarak tanımlamıştır ve dijital vatandaşlığı dijital erişim, dijital ticaret, dijital iletişim, dijital okuryazarlık, dijital etik, dijital hukuk, dijital hak ve sorumluluklar, dijital sağlık ve dijital güvenlik olarak 9 boyut altında toplamıştır (2004:12-15).

İçinde yaşadığımız çağ teknoloji çağı olarak adlandırılmaktadır. Teknoloji hızla değişim göstermektedir ve bu değişime uyum sağlayabilmek için teknolojiyi etkin ve verimli bir şekilde kullanmamız gerekmektedir. Bunu sağlayabilmemiz için öğrencilere ilkokuldan üniversiteye kadar tüm eğitim kademelerinde vatandaşlık eğitiminin yanı sıra dijital vatandaşlık eğitiminin de verilmesi gerekmektedir (İşman ve Güngören: 2014). Bu bağlamda, bilişim ve iletişim teknolojilerinin getirdiği imkanlarla birlikte, bireylerin dijital vatandaşlık bilincine sahip olmaları, dijital

farkındalıkları yüksek bir toplumun oluşturulmasında kilit bir rol oynar. Dijital vatandaşlık, teknolojik gelişmelerin sunduğu olanaklardan en iyi şekilde faydalanırken, aynı zamanda dijital dünyada etik, güvenli ve sorumlu bir şekilde hareket etmeyi amaçlar. Bu sayede, bilgiye ulaşımın kolaylaşması ve küresel iletişim imkanlarının artması, toplumların daha bilinçli ve birbirine daha yakın hale gelmesine katkı sağlar (Çubukçu ve Bayzan 2013: 149).

Genç nesillerin, akıllı telefonlar, tabletler ve dizüstü bilgisayarlar gibi mobil cihazları yoğun bir şekilde kullanmalarıyla birlikte, bu cihazlara özgü bir dizi güvenlik riski ortaya çıkmaktadır. Bu riskler genellikle kullanıcı davranışlarına bağlı güvenlik açıklarından kaynaklanmaktadır. Ayrıca, taşınabilir cihazlar üzerinde veya bu cihazlar aracılığıyla gerçekleştirilen güvenlik ihlallerinin sayısı hızla artmaktadır. Bu bağlamda, dijital yerlilerin (dijital çağda doğup büyüyen gençlerin) mobil cihazlarını nasıl kullandıklarını ve güvenlik farkındalık düzeylerini belirlemek, olumsuz güvenlik etkilerini azaltmak için uygun risk tedbirlerinin uygulanması açısından oldukça önemlidir (Gkioulos ve ark. 2017: 1). Öte yandan günümüzde bilgisayarlar ve iletişim ağlarının yaygın olarak kullanılması, dijital ortamlardaki verilerin güvenliği konusunu gündeme getirmiştir. Bilgi, artık genellikle elektronik ortamlarda üretilmekte ve sunulmaktadır. Bu durum, bazı avantajlar sağlarken, aynı zamanda çeşitli güvenlik sorunlarını da beraberinde getirmiştir. Elektrik kesintileri, dosyalara dışarıdan erişimin engellenmesi, bilgisayarların korunması ve şifrelenmesi, gizlilik ve telif hakları gibi sorunlarla karşılaşma ihtimali nedeniyle dijital verilerin güvenliği günümüzde hayati bir öneme sahiptir (Yılmaz 2015: 2). Literatürde dijital veri güvenliğiyle alakalı çeşitli tanımlamalar mevcuttur (Canbek ve Sağıroğlu 2006: 168).

Dijital veri güvenliğini, elektronik ortamlardaki verilerin bütünlüğünü bozmadan, izinsiz erişimlere karşı koruma sağlamayı ve bu verilerin güvenli bir şekilde saklanması ile taşınmasını sağlamak amacıyla bilgi işleme platformlarının güvenli hale getirilmesi olarak tanımlamaktadır (Kaya ve Öztürk 2017: 86). Dijital veri güvenliğini gizlilik, bütünlük, erişilebilirlik olarak üç maddede özetlemiştir (Fussel 2005).

Gelişen teknoloji çağında, dijital vatandaşlık ve dijital veri güvenliği kavramları, sağlık sektöründe belirleyici bir rol oynamakta ve sektöre önemli ölçüde etki

etmektedir. Çünkü dijitalleşme, sağlık hizmetlerinin sunumunda ve yönetiminde önemli bir rol oynamaktadır. Hasta kayıtları, tıbbi bilgiler ve sağlıkla ilgili diğer hassas verilerin dijital ortamda saklanması ve paylaşılması, hızlı ve etkili bir sağlık hizmeti sunumu için kritik öneme sahiptir. Ancak, bu dijital verilerin güvenliği ve gizliliği, sağlık sektörü için oldukça önemlidir. Dijital vatandaşlık, sağlık profesyonellerinin ve hasta bireylerin dijital dünyada etik davranış sergilemelerini ve dijital hak ve sorumluluklarına uygun olarak hareket etmelerini sağlar. Aynı zamanda, dijital veri güvenliği, sağlık kuruluşlarının siber tehditlere karşı direncini artırarak hastaların kişisel sağlık bilgilerini koruma amacını taşır. Bu kavramlar, sağlık sektörünün dijital dönüşüm sürecinde, bilgi güvenliğini sağlamak, etik standartlara uygunluğu güvence altına almak ve hasta güvenliğini en üst düzeyde tutmak adına kritik bir rol oynar. Bu sebepten, sağlık hizmeti sunan kuruluşların yöneticileri, sektördeki sorumlulukları yerine getirme ve etkili bir şekilde yönetme konusunda bilinçli olmaları gerekmektedir. Dijital vatandaşlık ve dijital veri güvenliği kavramlarının sağlık sektöründe büyük etkisi göz önüne alındığında, sağlık yönetimi öğrencileri, geleceğin sağlık yöneticileri olarak bu alanlarda önemli bir rol üstleneceklerdir.

Bu bağlamda, sağlık yönetimi öğrencilerinin dijital vatandaşlık ve dijital veri güvenliği konularındaki farkındalıklarının incelenmesi, geleceğin sağlık profesyonellerinin bu konularda ne kadar hazır olduğunu anlamamıza yardımcı olacaktır. Bu tez çalışması, dijital dünyada sağlık yönetimi öğrencilerinin bilinçli ve sorumlu dijital vatandaşlar olmalarına ve dijital veri güvenliği konusunda farkındalık sahibi olmalarına katkı sağlamak amacıyla önemli bir adım olarak değerlendirilebilir. İlgili literatür incelendiğinde, dijital vatandaşlık üzerine yapılan çalışmaların genellikle öğretmenler ve öğretmen adayları gibi belirli gruplarla sınırlı olduğu, dolayısıyla sağlık yönetimi bağlamında bu konulara yönelik araştırma eksikliği olduğu görülmüştür. Ayrıca, uluslararası düzeyde dijital sağlık alanında çeşitli çalışmalar mevcut olmakla birlikte, dijital vatandaşlık ve dijital veri güvenliğini bir arada inceleyen çalışmalara rastlanmamaktadır. Mert Hızmalı'nın (2022) üniversite öğrencileri üzerine gerçekleştirdiği araştırma, dijital vatandaşlık ve dijital veri güvenliği konularını birlikte ele almaktadır ancak bu çalışma sağlık yönetimi alanına yönelik değildir. Bu bağlamda, sağlık yönetimi alanında dijital vatandaşlık ve dijital veri güvenliğini bütüncül bir şekilde ele alan araştırmalara ihtiyaç duyulmaktadır.

Bu çalışmada ele alınan konu bağlamında, öğrencilerin dijital vatandaşlık ve dijital veri güvenliği farkındalıkları arasındaki ilişkiyi anlamak üzere belirlenen problem cümlesi şu şekildedir: "sağlık yönetimi öğrencilerinin dijital veri güvenliği farkındalığı ile dijital vatandaşlık düzeyleri arasında bir ilişki mevcut mudur? " Ayrıca, "öğrencilerin dijital veri güvenliği farkındalıkları ile dijital vatandaşlık ortalamaları nelerdir ve bu ortalamalar demografik özelliklere göre farklılık göstermekte midir? "

1.2. Araştırmanın Amacı

Bu çalışmanın amacı Sivas Cumhuriyet Üniversitesi SBF Sağlık Yönetimi Bölümü öğrencilerinin dijital vatandaşlık ve dijital veri güvenliği farkındalığı düzeylerini tespit etmek, bu iki kavram arasındaki ilişkiyi incelemek ve kavramları sosyodemografik faktörlere göre analiz etmektir.

1.3. Araştırmanın Sınırlılıkları

Araştırma; 2022-2023 akademik yılı Sivas Cumhuriyet Üniversitesi SBF Sağlık Yönetimi Bölümü öğrencilerinden elde edilen verilerle sınırlıdır.

1.4. Araştırmanın Hipotezleri

Sağlık yönetimi bölümü öğrencilerinin;

- * **H1:** Dijital vatandaşlık düzeyleri ile dijital veri güvenliği farkındalıkları arasında anlamlı bir ilişki vardır.
- * **H2:** Dijital vatandaşlık ve demografik özellikler arasında anlamlı bir ilişki vardır.
- * **H3:** Dijital veri güvenliği farkındalığı ve demografik özellikler arasında anlamlı bir ilişki vardır.
- * **H4:** Dijital veri güvenliği farkındalığı ile dijital vatandaşlığın alt boyutları arasında anlamlı bir ilişki vardır.
- * **H5:** Demografik faktörler ile dijital vatandaşlığın alt boyutları arasında anlamlı bir ilişki vardır.

2.GENEL BİLGİLER

Bu bölümde dijital vatandaşlık ve dijital veri güvenliği farkındalığı kavramlarının tanımları, önemi, amacı, sağlık hizmetlerindeki durumu, Türkiye'deki ve dünyadaki genel durumu ve tarihsel gelişimine yer verilecektir.

2.1.Vatandaşlık Kavramı

Vatandaşlık kavramı, tarihsel olarak ilk kez Antik Yunan'da ortaya çıkmıştır. Bu kavram, Fransız İhtilali'nin etkisiyle diğer devletlere de yayılmış ve günümüzdeki şeklini almıştır (Nalbant 2014: 80).

Vatandaşlık, soyut bir kavram olup farklı bireyler tarafından çeşitli biçimlerde algılanan bir yapıdır. Dolayısıyla, vatandaşlık kavramını değerlendirmek, bu soyut kavramın çeşitli sınırlar içinde ele alınmasıyla mümkündür. Vatandaşlık, bazı bireyler için vatanseverlik anlamına gelebilirken, diğerleri için ahlaki kurallara uygun bir etik değer olarak tanımlanabilmektedir (Stevenson 2010: 275–291).

Marshall, vatandaşlık kavramı üzerine önemli katkılarda bulunmuş ve özellikle "Vatandaşlık ve Sosyal Sınıf" adlı çalışmasıyla tanınmıştır. Marshall, vatandaşlık kavramını üç ana grupta değerlendirerek tanımlamıştır. Bu gruplar, medeni, sosyal ve siyasi haklardır. Medeni haklar, bireylerin düşünce, inanç ve mülkiyet özgürlüklerini içerir. Siyasi haklar, bireyin devlet içinde yeni düzen oluşturabilme ve siyasi kararlara katılma hakkını içerir. Sosyal haklar ise devlet sınırları içinde yaşayan bireyin ekonomik refah ve sosyal güvenlik haklarından yararlanma hakkını içerir (Marshall 1950; Yarwood, 2016: 4) tarafından aktarılmıştır).

Vatandaşlık, değişken ve çok yönlü bir kavramdır. Tarihsel süreç içinde anlamları ve özellikleri değişmiş olduğundan dolayı dinamik bir kavram olarak nitelendirilebilir. Zaman içinde, farklı topluluklar arasında çeşitli yorumlara ve uygulamalara sahip olması nedeniyle, vatandaşlık kavramı bağlamsal bir boyut taşır. Tartışmaya açık bir kavramdır çünkü zaman ve mekânda, vatandaşlığın ne anlama geldiği ve ne olması gerektiği konusunda görüş ayrılıkları bulunmaktadır. En nihayetinde, vatandaşlık terimi çok yönlüdür ve en az dört farklı boyutu içerir; statü, kimlik, yurttaşlık erdemleri ve faillik. Bu yönler, sırasıyla üyelik meseleleriyle, aidiyet

duygusuyla, eğilimlerle, değerlerle, davranışlarla ve katılım ile siyasi etkinlik meseleleriyle ilgilidir (Schugurensky 2005).

Dijital teknolojilerin ve internetin hızla yaygınlaşması, bireylerin ve grupların ortak ilgi alanlarına sahip olarak topluluklar oluşturmasını mümkün kılmaktadır. Ayrıca, internetin vatandaşlık çalışmaları bağlamında önemli dönüşümlere neden olduğu ve vatandaşlık kavramının anlamının gözden geçirilmesini sağladığı ifade edilmektedir. İnternet, siyasi durumlar hakkında bilgi edinme, siyasi süreçlere etkin katılım, politika kararlarına katılma ve eleştirel düşünce geliştirme gibi vatandaşlık yetkinliklerine yeni açılımlar getirmektedir. Bu bağlamda, internetin vatandaşlık kavramını ve bu kavrama yüklenen anlamları şekillendirme ve tarihsel gelişim sürecinde önemli bir rol oynama potansiyeli olduğu vurgulanmaktadır (Karaduman 2011: 14).

Sonuç olarak, vatandaşlık kavramı geçmişten günümüze çeşitli evrelerden geçmiş, farklı anlamlar kazanmıştır ve hala toplumsal, siyasal ve kültürel bağlamda önemini korumaktadır. Bu kavramın çok yönlü ve dinamik yapısı, bireyler arasında çeşitli yorumlara neden olmuş ve vatandaşlık haklarının tanımlanması konusunda tartışmaları beraberinde getirmiştir.

2.1.1. Dijital Vatandaşlık

Teknolojinin tarihsel evrimi, ateşin keşfi ve tarımın başlaması gibi kritik aşamalardan geçerek olağanüstü bir gelişim göstermiştir (Bacanak, Karamustafaoğlu, Köse, 2003: 191). Bu evrim, son 50 yılda yaşanan teknolojik ilerlemelerle birleşerek, sosyal hayatımızı derinden etkileyerek yaşamımızı birçok yönden kolaylaştıran teknoloji, bilgisayar ve internet gibi unsurların sürekli değişim göstermesine neden olmuştur. Günümüzde akıllı telefonların yaygın kullanımıyla birlikte, birçok insan teknolojiye yoğun bir ilgi göstermekte, çocuklardan yetişkinlere kadar geniş bir kesim interneti kullanarak çeşitli faaliyetlerde bulunmakta ve bu aktiviteler günlük yaşantılarının önemli bir parçası haline gelmektedir (Tan ve Merey 2021: 164).

İnternet ve ilgili teknolojilerin yaygınlaşması, akıllı telefonlar, uygulamalar, sosyal medya platformları, dijital medya içerikleri, online dergiler ve doğru ya da yanlış içerik sunan web siteleri gibi unsurlar aracılığıyla gençten yaşlıya her bireyin yaşamını önemli ölçüde etkilemiştir. Dijital ortamda paylaşılan bilgiler,

sayılamayacak kadar çok ve çeşitli bir boyuta ulaşmıştır; bilgi artık fiziksel sınırların ötesine geçmiş ve bulut tabanlı erişilebilir formata dönüşmüştür. Kısacası, herkes istediği şeyi çevrimiçi olarak paylaşabilir ve sınırsız bir şekilde dijital dünyada gezinebilir hale gelmiştir. İnternetin bireyler ve toplumlar üzerindeki etkisi, vatandaşlık kavramını dijital bir boyuta taşımış ve bu bağlamda dijital vatandaşlık kavramı ortaya çıkmıştır (Aydın 2015: 142). Dijital vatandaşlık kavramı literatürde çeşitli tanımlamalara sahiptir. Ribble ve Bailey'nin (2004:12-15) öncülüğünde ortaya atılan bu kavram, teknolojinin etik ve sorumlu bir şekilde kullanımına dair belirli standartları ifade etmektedir.

Çubukçu ve Bayzan'a, (2013: 148)'a göre dijital vatandaşlık; bilgi ve iletişim kaynaklarını kullanırken eleştirebilme yeteneğine sahip, çevrimiçi davranışların etik sonuçlarını anlayan, teknolojiyi başkalarına zarar vermeden kullanabilen, internet üzerinde iletişim hakkını etkili bir şekilde kullanan, paylaşımlarında doğru tutumu sergileyen ve diğer vatandaşları da bu yönde teşvik eden bireyler olarak belirtilmiştir. Aynı zamanda dijital vatandaşlar, bilgi ve iletişim teknolojilerini kullanırken eleştirel bir bakış geliştirebilen, etik boyutları değerlendirebilen ve bilgi paylaşımında doğru tutumlar sergileyebilen bireylerdir (Mercimek, Yaman, Kelek ve Odabaşı 2015: 69).

Fingal'ın (2022) belirttiği gibi, iyi bir dijital vatandaşın özellikleri çeşitli unsurları içermektedir:

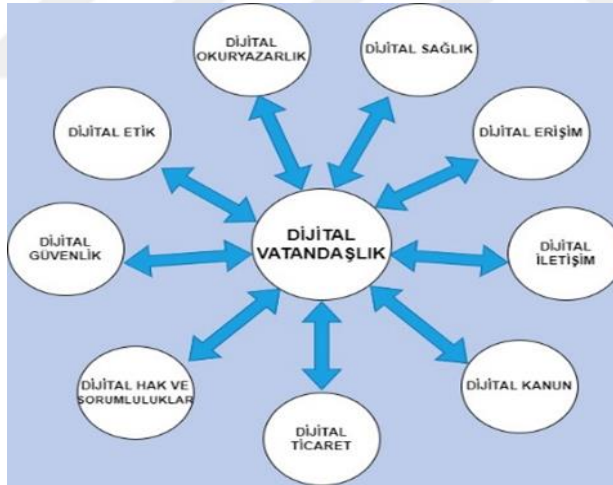
- Çevrimiçi platformlarda, insanlarla saygı ve empati çerçevesinde etkileşimde bulunmayı önemser.
- Çevrimiçi bilgilerin doğruluğunu değerlendirir, farklı perspektifleri anlamaya çalışır.
- Teknolojiyi sivil katılım ve olumlu etkiler yaratmak için aktif bir şekilde kullanır.
- Çevrimiçi ve çevrimdışı aktiviteleri dengeleyerek, zamanı etkili bir şekilde yönetir.
- Çevrimiçi güvenlik ve mahremiyet konularında bilinçli davranır, güvenli dijital alanlar oluşturmayı amaçlar.

Günümüzde, bilişim teknolojisi araçlarının etkili bir şekilde kullanılabilmesi, her bireyin toplumsal hayata ve iş yaşamına entegre olabilmesi için vazgeçilmez bir gereklilik haline gelmiştir. Bireylerin bilişim teknolojilerini kullanma konusundaki bilgi ve beceri eksiklikleri, iş hayatına giriş ve toplumsal adaptasyon süreçlerini zorlaştıran temel engellerden biri olarak ön plana çıkmaktadır. Bu noktada, bilişim

teknolojisi bilgi ve becerilerinin eksikliği, okuma yazma bilmeme gibi durumlarla benzer şekilde bireylerin toplum ve iş dünyasına uyum sağlamalarını önleyen önemli bir faktördür (Demirel 2009: 698). Bu bağlamda kişilerin hızla değişen teknolojik gelişmelere, giderek karmaşıklaşan toplum yaşamına uyum sağlayabilmeleri için, çağdaş bilgi, beceri ve tutumlarla donatılmaları zorunludur. Bu, her bireyin, teknolojik gelişmelerin gerektirdiği yetkinlikleri kazanabilmeleri için bir eğitimden geçmeleriyle mümkündür (Şenel ve Gençoğlu 2003: 52).

2.1.2. Dijital Vatandaşlığın Boyutları

Ribble (2023), dijital vatandaşlığı, 9 farklı alt boyutta ele almıştır. Bu boyutlar, dijital erişim, dijital ticaret, dijital iletişim, dijital okuryazarlık, dijital etik, dijital hukuk, dijital haklar ve sorumluluklar, dijital sağlık ve dijital güvenlik olarak sıralanmaktadır. Ribble, bu boyutların temelinde bireylerin günümüzde sahip olması gereken dijital vatandaşlık özelliklerini geliştirmeyi amaçlamaktadır.



Şekil 1: Dijital Vatandaşlığın Boyutları (Kaynak: Ribble, 2023).

2.1.2.1 Dijital Sağlık

Dijital sağlık, bilgi ve iletişim teknolojisinin kullanılmasıyla hastalıkları önlemeyi ve yaşam kalitesini arttırmayı amaçlayan bir kavramdır. Bu müdahaleler, yaşlanma, çocuk hastalıkları, salgın hastalıklar, pandemiler, yüksek maliyetler, yoksulluk ve ırk ayrımcılığının sağlık hizmetlerine erişim üzerindeki etkileri gibi

küresel endişelerle birlikte değer kazanmaktadır. Dijital sağlık platformları, sağlık sistemleri ve ilgili teknolojiler, bu zorluklarla başa çıkmak ve daha etkili sağlık hizmetleri sunmak amacıyla sürekli olarak gelişmekte ve önem kazanmaktadır (Bernstein 2021).

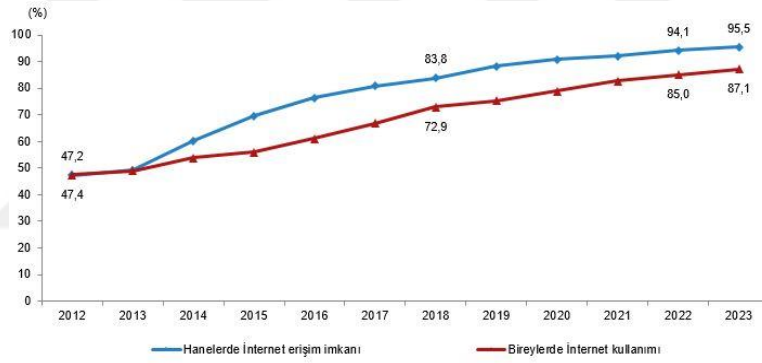
Dijital sağlık uygulamalarının yaygınlaşmasında etkili olan bir dizi faktör bulunmaktadır. Sağlık hizmetlerinin sürdürülebilirliğini artırmak, daha hızlı sonuçlar almak ve daha verimli hizmet sunumu sağlamak gibi beklentiler, dijital sağlık uygulamalarının popülerliğini artırmaktadır. Bu bağlamda, dijital sağlık kavramı bireylerin sağlığına katkıda bulunmanın yanı sıra sağlık hizmetlerinin güncel, verimli ve kaliteli bir şekilde sunulması açısından oldukça önemlidir (Uysal ve Ulusinan 2020: 47) Dijital sağlık teknolojinin bir araya geldiği geniş ve çok disiplinli bir kavramdır. Bu kavram, sağlık alanında dijital dönüşümü sağlamak amacıyla yazılım, donanım ve hizmetleri birleştirir. Dijital sağlık, mobil sağlık (mHealth) uygulamaları, elektronik sağlık kayıtları (EHR'ler), elektronik tıbbi kayıtları (EMR'ler), giyilebilir cihazları, tele sağlık ve tele tıp gibi alanları kapsar. Bu, sağlık hizmetlerini daha etkili ve kişiselleştirilmiş hale getirmeyi amaçlayan bir yaklaşımı içermektedir (Bernstein 2021).

2.1.2.2 Dijital Erişim

Sakallı (2015: 60), dijital vatandaşlığın erişim boyutunu, dünya genelinde her bireyin interneti ve teknolojik cihazları kullanabileceği altyapı ve olanaklara sahip olabilmesini ifade ettiğini belirtmektedir. Dijital erişim, Ribble ve Bailey (2007) tarafından toplumun genel olarak elektronik ortama katılımı olarak tanımlanmaktadır. Bu tanıma göre, tüm bireylerin cinsiyet, etnik köken, yaş, fiziksel ve zihinsel farklılıkları gözetmeksizin çevrimiçi ortamlara kolaylıkla ulaşabilmesi gerekmektedir. Ribble ve Bailey (2004), internete etkin ve verimli erişimin çevrimiçi toplumlara tam katılım için önemli bir bileşen olduğunu savunmaktadırlar. Onlara göre, kolay ve güvenilir internet erişimine sahip bireyler ile sınırlı internet erişimine veya hiç erişimi olmayan bireyler arasında önemli bir fark bulunmaktadır. Ancak, Mossberger, Tolbert ve Hamilton (2012) tarafından belirtildiği gibi, bireyler arasındaki dijital erişim farklılıkları, altyapı sorunları, coğrafi konum ve özel gereksinimler gibi etkenlere dayanabilir. Bu durum, aynı toplum içinde yer alan bireylerin, internet ve dijital

platformlara erişim konusunda eşit şartlara sahip olmamasına neden olabilir. Ribble (2023) bu noktada, dijital vatandaşlığın özellikle bu tür eşitsizlikleri ele alarak daha kapsayıcı ve adil bir dijital geleceğin oluşturulmasına katkı sağlayabileceğini belirtmektedir.

Hanehalkı bilişim teknolojileri kullanım araştırması sonuçlarına göre; 2023 yılında evden internete erişim imkânı olan hanelerin oranı bir önceki yıla göre 1,4 puan artarak %95,5 olmuştur. İnternet kullanım oranı ise 16-74 yaş grubundaki bireylerde 2022 yılında %85,0 iken 2023 yılında %87,1 olmuştur. Cinsiyet ayrımında 2023 yılında internet kullanım oranı; erkeklerde %90,9, kadınlarda %83,3 olarak gözlemlenmiştir (TÜİK 2023).



Grafik 1: Hanelerde İnternet Erişim İmkânı ve Bireylerde İnternet Kullanımı, 2012-2023 (Kaynak: TÜİK, 2023)

2.1.2.3. Dijital Okuryazarlık

Günlük yaşamın ayrılmaz bir parçası olan okuma, bilgi edinmemizi şekillendirir ve bu bilgiler doğrultusunda fikir geliştirmemize olanak tanır. İnternet ve bağlı cihazlar, çeşitli bilgilere hızlı erişim sağlayarak okuma fırsatlarını artırır (Duran ve Özen 2018: 32). Dijital okuryazarlık, bireyin bilgi iletişim teknolojilerini etkin bir şekilde öğrenmesini içerirken aynı zamanda bu teknolojileri kişisel gelişimine katkı sağlamak, hayatın çeşitli bağlamlarında problemler çözmek, toplumsal katılımı ve üretimi desteklemek için teknolojileri güvenli, yasal ve ahlaki bir şekilde kullanma becerilerini ifade eder (Özerbaş ve Kuralbeyava 2008: 16).

Bireylerin sosyal medya platformlarını kullanma, belirli bir grupta etkileşimde bulunma, haber okuma, düşüncelerini paylaşma, müzik dinleme, film izleme gibi farklı amaçlar doğrultusunda interneti kullandığı gözlemlenmektedir.

Dijital okuryazarlığa sahip olmak, yalnızca yazılım kullanma veya dijital cihazları çalıştırma yeteneğiyle sınırlı değildir; aynı zamanda kullanıcıların dijital ortamları etkili bir şekilde kullanabilmeleri için çeşitli karmaşık becerilere sahip olmalarını gerektirir. Bu yetkinlikler, bilişsel, motor, sosyolojik ve duygusal alanlarda çeşitlilik gösterir (Alkali ve Amichai 2004: 420).

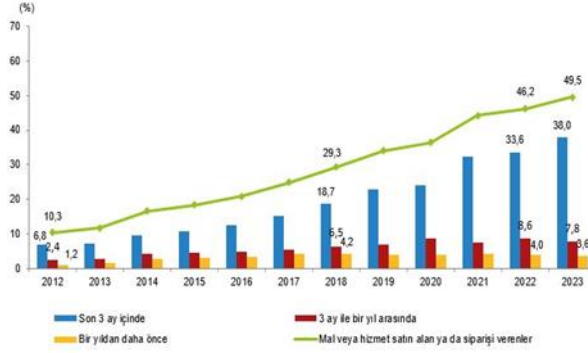
Okuryazarlık, topluma katılımın temel özelliklerinden biridir. Çocuklarda ve eğitim sürecindeki yetişkinlerde, okuma yazma becerilerinin geliştirilmesi, genel bilişsel ve kültürel gelişimin bir parçası olarak toplumsal katılımı sağlar. Bu bağlamda, okuryazarlık, sosyal anlamda normallik kazandıran ve bireyin topluma uyumunu sağlayan önemli bir yetenek olarak öne çıkar (Goodfellow, 2011, s.131-132). Özellikle çocuklara dijital okuryazarlık eğitiminin küçük yaşlardan itibaren verilmeye başlanması oldukça önemlidir çünkü internet okuryazarlığına sahip olmayan çocuklar, pedofili, şiddet içeren paylaşımlar ve taciz gibi risklere maruz kalabilirler. İnternet üzerinde gezinirken aniden ortaya çıkan cinsellik, şiddet içeren reklamlar veya içerikler çocuklar için olumsuz örnekler teşkil eder. Bu nedenle, çocukların dijital okuryazarlık becerilerini geliştirmek ve internet üzerinde karşılaşılabilecekleri tehlikelere karşı bilinçli olmalarını sağlamak önemlidir (Karahisar 2014: 82).

2.1.2.4 Dijital Ticaret

Türkiye'de ve dünya genelinde e-ticaret sektörünün hızla büyümesi, internet kullanıcılarının alışveriş alışkanlıklarındaki değişim ve e-ticaret işletmelerinin teknolojiyi etkin bir şekilde kullanarak iş süreçlerini iyileştirmeleri gibi faktörlere dayanmaktadır (Demirdöğmez ve ark. 2018: 2218). 2023 yılı itibarıyla, Türkiye'deki internet kullanıcıları arasında özel kullanım amacıyla mal veya hizmet satın alma ya da sipariş verme (e-ticaret) oranının %49,5'e yükselmiş olması, bu dönüşümün somut bir göstergesidir (TÜİK 2023).

Özellikle son 3 ay içinde yapılan alışverişler incelendiğinde, giyim, ayakkabı ve aksesuar kategorisinin ön planda olduğu görülmektedir. Cinsiyet bazında karşılaştırmalarda, erkeklerin giyim ürünlerine olan ilgisi ve lokantalardan yapılan

teslimatlarla yakından ilgilenirken, kadınların giyim, kozmetik ve sağlık ürünleri kategorilerine daha fazla yönlendiği gözlemlenmiştir (TÜİK 2023).



Grafik 2: İnternette Satın Alma Oranı, 2012-2023 (TÜİK 2023)

Sonuç olarak, e-ticaretin artan popülerliği, tüketicilere geniş bir ürün yelpazesi sunarken, işletmelerin de daha etkin ve rekabetçi olmalarını sağlamaktadır. Ancak, bu büyümenin sürdürülebilir olması ve tüketicilerin güvenliğini kazanması için güvenlik önlemlerine büyük bir önem verilmelidir. İşletmeler, güvenli ödeme sistemleri ve kişisel veri koruma politikaları gibi önlemleri benimseyerek, tüketicilerin güvenliğini kazanabilir ve e-ticaretin gelecekteki başarısını güvence altına alabilirler.

2.1.2.5. Dijital Hak ve Sorumluluklar

Dijital bir vatandaş olarak, internet ortamında meydana gelen haksızlıklar ve yasadışı içeriklerle mücadele etmek için sorumluluklarımız bulunmaktadır. İnternetin barındırdığı risk gruplarına karşı haklarımızı kullanmak ve aynı zamanda sorumluluklarımızı yerine getirmek, güvenli ve etik bir dijital davranış sergilememizi sağlar (Çubukçu ve Bayzan 2013: 157).

Dijital haklar ve sorumluluklar, bireylere özgürlük tanıdığı gibi, aynı zamanda bireylerin taşıması gereken sorumlulukları da içermektedir. Dijital dünyada sorumlu bir şekilde davranarak hem kendi güvenliğimizi hem de başkalarının güvenliğini koruyabiliriz (Yılmaz 2020: 151).

2.1.2.6. Dijital İletişim

Dijital iletişim, farklı dijital araçlardan yararlanarak dijital ortamlarda bilgi alışverişi yapma ve iletişim kaynaklarını doğru zamanda ve doğru bir şekilde kullanabilme becerisini içerir (Çubukçu ve Bayzan: 2013). Özellikle ergenler arasında popüler olan iletişim biçimleri gün geçtikçe çeşitlenmekte ve teknolojinin gelişmesiyle birlikte iletişim araçları gençler arasında hızla evrim geçirmektedir. E-posta, anlık mesajlaşma, yazılı mesajlaşma, sohbet odaları, bülten panoları, bloglar, sosyal ağlar (örneğin MySpace ve Facebook), video paylaşım siteleri (örneğin YouTube), fotoğraf paylaşımı (örneğin Flickr), çok oyunculu çevrimiçi bilgisayar oyunları (örneğin World of Warcraft), sanal dünyalar (örneğin Second Life ve Teen Second Life) gibi araçlar, gençlerin günlük iletişimlerinde önemli bir rol oynamaktadır. Bu çeşitli iletişim araçları, gençlerin birbirleriyle etkileşimde bulunma şekillerini çeşitlendirmekte ve dijital medya konusundaki becerilerini geliştirmelerine olanak tanımaktadır (Subrahmanyam ve Greenfield, 2008: 121)

Yapılan TÜİK araştırmasına göre, bireylerin %82,0'si en çok tercih ettikleri uygulamanın WhatsApp olduğunu belirtmiştir. WhatsApp'ı sırasıyla %67,2 ile YouTube ve %57,6 ile Instagram takip etmektedir. Cinsiyete göre incelendiğinde, erkeklerin %85,9'u en çok WhatsApp, %70,8'i YouTube ve %61,5'i Facebook'u tercih etmektedir. Kadınlarda ise bu oranlar sırasıyla %78,1 (WhatsApp), %63,7 (YouTube) ve %55,9 (Instagram) şeklinde görülmektedir. Bu veriler, bireylerin sosyal medya ve mesajlaşma uygulamalarını geniş bir yelpazede kullanarak dijital iletişimde çeşitlilik gösterdiklerini göstermektedir (TÜİK 2023).

Dijital iletişimdeki avantajlara rağmen, bazı risklerle karşılaşmak da mümkündür. Özellikle sosyal medyada oluşturulan sahte profiller, çocuklar için potansiyel bir tehlike oluşturabilir. Dijital iletişim ortamlarında, bireyler kişisel veya ticari bilgilerini tanımadıkları kişilere vererek dolandırıcılık gibi risklere maruz kalabilirler. Bu nedenle, dijital iletişimde dikkatli olmak ve güvenlik önlemlerini almak önemlidir (Yılmaz 2019: 10).

2.1.2.7. Dijital Güvenlik

Dijital güvenlik, günümüz toplumlarında önemli birer konu haline gelmiştir. Ribble ve Bailey (2007), dijital güvenliği, "tüm dijital kullanıcılarının kişisel

güvenliğini ve ağlarının güvenliğini koruması için önlemler topluluğu" olarak tanımlamışlardır. Bu tanım, dijital vatandaşlar için bilgi güvenliği ve çevrimiçi ağların güvenliğine odaklanan bir süreç olarak nitelendirilebilir.

Güvenlik, sadece bir ürün değil, aynı zamanda bir süreçtir. Bir süreç olarak, birçok bileşen içerir ve bu bileşenlerin birbirleriyle uyum içinde olması gerekmektedir. Güvenlik sürecindeki bileşenler arasında sağlamlık, güvenilirlik ve etkinlik açısından farklılıklar olabilir. Bu bileşenlerin uyumlu olması, güvenlik sürecinin daha etkili çalışmasına katkı sağlar. Güvenlik süreci, bir zincir gibi birbirine bağlı halkalardan oluşur ve her bir halkanın güçlü olması genel güvenliği artırır. Bu süreçteki zayıf halkalar genellikle bileşenler arasındaki arayüzlerdir ve bu arayüzlerin güvenliği kritik bir rol oynar (Schneier 2000: 84).

Dijital vatandaşlar için güvenli bir çevrimiçi deneyim, kişisel bilgi güvenliğine verilen önemle başlar. Çevrimiçi platformlarda dolaşırken güvenilir sayfalara yönelme ve kişisel bilgilerin korunması büyük bir öneme sahiptir. Ayrıca, filtreleme programları, güvenli internet paketleri ve anti-virüs programlarını içeren internet koruma paketleri gibi güvenlik önlemlerini kullanmak da önemlidir. Bu önlemler, çevrimiçi ortamda karşılaşılabilecek içerik, temas ve ticari risklere karşı korunmada etkili olabilir (Çubukçu ve Bayzan, 2013: 158).

Sonuç olarak, dijital iletişimde güvenlik, güçlü bir süreç ve bu süreci oluşturan güvenli bileşenlerin uyumlu bir şekilde çalışmasıyla sağlanabilir. Dijital vatandaşlar, kişisel bilgi güvenliklerine ve çevrimiçi güvenliğe önem vererek, dijital iletişimde daha güvenli bir ortam oluşturabilirler. Güvenlik, bireylerin dijital dünyada bilinçli ve güvenli bir şekilde hareket etmelerini sağlayarak, dijital iletişimin olumlu bir şekilde ilerlemesine katkı sağlar.

2.1.2.8. Dijital Etik

Ethos kelimesinden türetilen "etik" terimi, başlangıçta gelenekler ve adetlerle ilişkilendirilmiştir. Ethos, Yunanca kökenli bir kelime olup, başlangıçta bir grup veya topluluğa ait olanların karakterini veya mizacını ifade etmiştir. Gelenekler, sadece alışılmış davranış biçimlerini değil, aynı zamanda grup veya toplum tarafından onaylanan normları temsil etmiştir. Bu normlara aykırı davranmak, ciddi hoşnutsuzluğa neden olmuştur. Etik ve moral terimleri, günümüzde karmaşık ve

gelişmiş bir yaşam tarzını ifade ederken, aslında ethos ve törelerin ahlaki yaşamın nasıl başladığına işaret ettiği düşünülmektedir. Bu terimler, doğru ve yanlış, iyi ve kötü gibi tutumları temsil etmektedir, ancak günümüzde daha karmaşık bir bağlamda kullanılmaktadır (Näsman ve Nyholm, 2021).

2.1.2.9. Dijital Kanun

Dijital vatandaşlar, sadece gerçek hayatta değil, özellikle internet ortamında da dikkat etmeleri gereken belirli kurallara riayet etmelidirler. İnternet üzerinde suç teşkil eden davranışların gerçek dünyada da suç olduğu bilinciyle hareket etmek önemlidir. Aynı zamanda, dijital vatandaşlar, internet üzerinde suç işleyenleri ilgili mercilere şikâyet etmelidirler. Bu bağlamda, internetin risk boyutlarıyla ilişkilendirilen içerikleri üretmek ve paylaşmak da suç teşkil edebilir (Çubukçu ve Bayzan 2013: 157).

1990'lı yılların başlarında, internetin yaygınlaşarak dünya genelindeki bilgisayar kullanıcıları arasında bağlantı kurma imkânı sağlaması, suç işleme eğilimindeki birey ve gruplar için yeni suç alanlarının ortaya çıkmasına sebep olmuştur (Durmaz 2005: 76).

Bilişim suçları alanındaki yasal düzenlemelerden hareketle ülkemizde bilişim suçları sekiz ana başlık altında gruplandırılmaktadır (Kale 2014: 51):

- a) Bilgisayar sistemlerine yetkisiz erişim,
- b) Bilişim sistemlerini engelleme, bozma, verileri yok etme,
- c) Yazılımların izinsiz kullanılması,
- d) Yasadışı yayınlar,
- e) Müstehcenlik- çocuk pornografisi,
- f) Nitelikli dolandırıcılık,
- g) Hakaret, sövme ve şantaj,
- h) Elektronik imza kanununa karşı çıkma.

Sonuç olarak, dijital vatandaşlar olarak internet üzerindeki davranışlarımızın gerçek dünya ile aynı hukuki sorumluluğu taşıdığını bilmeli ve bu bilinçle hareket etmeliyiz. Aynı zamanda, bilişim suçlarıyla mücadelede iş birliği ve toplumsal bilinç, dijital güvenliği sağlamak adına kritik öneme sahip olduğunun bilincinde olmalıyız.

2.1.3. Türkiye ve Dünyada Sağlık Alanındaki Dijital Vatandaşlık Projeleri

2.1.3.1. E Nabız

Türkiye'de Sağlık Bakanlığı'nın hayata geçirdiği e-Nabız programı ve Sağlık Dosyam/E-Sağlık Dosyam gibi gelişmeler, kişisel sağlık kayıtlarının daha etkili bir şekilde yönetilmesi amacıyla atılan önemli adımlar olarak değerlendirilebilir (Arslan ve Demir 2017: 24).

E-Nabız, sağlık kuruluşları tarafından toplanan sağlık verilerine, vatandaşlar ve sağlık profesyonelleri için internet ve mobil cihazlar üzerinden erişilebilen bir uygulamadır. Bu uygulama, muayene, tetkik ve tedavilerin nerede gerçekleştirildiğine bakılmaksızın, tüm sağlık bilgilerini yönetebilme imkânı sunan, tıbbi özgeçmişe tek bir yerden ulaşabilme olanağı sağlayan bir kişisel sağlık kaydı sistemidir (E-nabız).

E-Nabız sistemi tüm verileri şifreleyerek kriptolu bir şekilde saklamaktadır. Bu sayede kullanıcıların sağlık verilerin gizliliği ve güvenliği sağlanmış olur. Ayrıca kullanıcılar verilerini izin verdikleri yakınları ve hekimleriyle paylaşabilir ve dilediklerinde veri erişim yetkilerini geri alabilirler. Bu kontrol mekanizmaları, sistem üzerindeki bilgi güvenliği ve gizlilik standartlarını güçlendirmektedir (İleri ve Uludağ 2017: 321).

2.1.3.2 MHRS

Merkezi Hekim Randevu Sistemi (MHRS), Türkiye Cumhuriyeti Sağlık Bakanlığı tarafından başlatılan Sağlıkta Dönüşüm Projesi kapsamında hayata geçirilen önemli bir uygulamadır. Bu proje, sağlık hizmetlerine daha etkin ve verimli bir erişim sağlamayı hedeflemektedir. MHRS, bu programın önemli bir ayağını oluşturarak vatandaşlara sağlık randevularını düzenleme imkânı sunmaktadır (MHRS 2021).

MHRS (Merkezi Hekim Randevu Sistemi), Sağlık Bakanlığı'na bağlı 2. ve 3. basamak hastaneler ile ağız ve diş sağlığı merkezleri için kullanılan bir hizmettir. Bu sistem aracılığıyla, Alo 182 hattından MHRS'yi arayarak canlı operatörlerle iletişim kurabilir veya web üzerinden kendilerine uygun hastane ve hekimden randevu alabilirler (Yıldızbaşı ve ark. 2016: 296).

2.1.3.3 AFAD Acil Mobil Uygulama Projesi

T.C. İçişleri Bakanlığı, afet ve acil durumların etkilerini minimize etmek, vatandaşları afet öncesinde bilinçlendirmek ve hızlı müdahale sağlamak amacıyla AFAD Acil Uygulamasını geliştirmiştir. Bu uygulama, doğal afetlerden etkilenen kişilerin konum ve durum bilgilerini sesli ve mesajlı iletişim aracılığıyla veri hattı üzerinden 112 Acil Çağrı Merkezlerine iletmek, merkezlerde durumu değerlendirip sahadaki ekiplerle paylaşmak ve uygulama üzerinden bireylerle iletişime geçmek üzere tasarlanmıştır.

Kullanıcılar, acil durumlarda yakınlarının iletişim bilgilerini uygulamaya ekleyerek, bu bilgilerin 112 Acil Çağrı Merkezi personeli tarafından anında görülebilmesini sağlayabilir. Ayrıca, afetzedelerin güncel bilgileri, gerektiğinde yakınlarına iletmek üzere paylaşılabilir.

Olası bir afet anında, vatandaşların toplanacağı güvenli bölgeler olarak belirlenen toplanma alanları, uygulamanın ana ekranında bulunan harita üzerinde gösterilmektedir. Bu noktalar, vatandaşların afetin ilk saatlerinde tehlikeli yapılardan uzak kalmalarını ve geçici olarak güvenli bir alana yönlendirilmelerini sağlamak amacıyla belirlenmiştir. Vatandaşlar, uygulama üzerinden bu alanlara nasıl ulaşacaklarını gösteren yol tariflerini alabilirler (AFAD 2021).

2.1.3.4 Giyilebilir Sağlık Teknolojisi

Giyilebilir teknolojiler, zamanında geri bildirim sağlayarak sağlık bilincini artırma potansiyeline sahiptir. Bu teknolojiler, bireylerin yaşam tarzlarını kullanıcı odaklı bir sağlık anlayışıyla düzenlemelerine yardımcı olmaktadır. Daha da önemlisi, giyilebilir bilişim teknolojileri, hastaya sağlığıyla ilgili daha fazla kontrol verir ve hastalık oluşmadan önce önleme fırsatı sunar. (Ananthanarayan, Siek 2012: 236)

Giyilebilir sağlık cihazlarına örnek olarak giyilebilir spor izleyicileri, akıllı saatler, giyilebilir EKG monitörleri, giyilebilir kan basıncı monitörleri ve biyosensörler verilebilir (Türkiye Sağlık Vakfı 2023).

2.1.3.5 İTS (İlaç Takip Sistemi)

İlaç Takip Sistemi, beşerî tıbbi ürünlerin karekod teknolojisi kullanılarak izlenmesini sağlayan bir merkezi kayıt ve takip sistemidir. Bu sistem, ürünlerin üretiminden itibaren tüm hareketlerini üretim, ithalat, ihracat, alış, satış, devir, tüketim, zayi olma ve geri ödeme gibi gerçek zamanlı olarak izler ve kaydeder. Karekod sayesinde her ürünün tedarik zincirindeki konumları ve durumları net bir şekilde takip edilebilir.

Ürünlerin tedarik ve dağıtım süreçlerinde hangi konumda olduklarını belirlemek bu sayede mümkündür. Türkiye'nin Sağlık Bakanlığı tarafından geliştirilen bu sistem, uluslararası alanda ilgi görmekte ve birçok ülke tarafından uygulama için destek talebi gelmektedir (İTS 2019). Sistemin amacı, vatandaşların güvenli bir şekilde ilaca erişimini sağlamaktır.

2.1.3.6. ESK (Elektronik Sağlık Kaydı)

Elektronik Sağlık Kaydı (ESK), bireylerin fiziksel ve ruhsal sağlıklarına dair geçmiş, mevcut ve gelecekteki bilgilerin elektronik sistemler aracılığıyla kayıt altına alınması, saklanması, iletilmesi, erişilmesi ve işlenmesi anlamına gelir. ESK sistemleri, hasta bilgilerini bilgisayar ortamında toplar ve bu bilgilerin gerekli durumlarda kullanılmasını sağlar. Bu sistemler, sağlık kayıtlarının faydalı, etkili, etik ve yasal kurallara uygun şekilde iletilmesini ve verilerin bütünlüğünün korunmasını amaçlar.

ESK sistemleri, sağlık bilgisinin toplanması, saklanması, işlenmesi, iletilmesi, güvenliği ve sunulması gibi işlevleri içerir. Genellikle hastaların kimlik bilgileri, hastalık sınıflamaları ve demografik faktörlere dayalı kayıtların indekslenmesini kapsar. Bu yapı, araştırma ve denetimlerde kayıtların kolayca geri çağırılmasını sağlar. Ayrıca, bazı sistemler bağlı sistemler aracılığıyla acil servislerde, polikliniklerde ve hasta giriş ekranlarında hastalık kayıt özetlerine erişim imkânı sunar. ESK sistemlerinin mahremiyet, güvenlik, izlenebilirlik ve veri bütünlüğü gibi önemli özellikleri sağlaması gerekmektedir (Sağlık Bakanlığı 2014).

2.1.3.7. Tele Sağlık Hizmetleri

Gemi personelinin sağlık koşullarını iyileştirmek için dünya genelinde sürekli standartlar güncellenmektedir. Türkiye'de, gemilerde sağlık sorunlarına uzaktan tıbbi yardım sağlamak amacıyla 7/24 hizmet veren Tele Sağlık Merkezi bulunur. Bu merkez, uluslararası düzeyde tıbbi danışmanlık sunar ve acil durumlarda tıbbi tahliye organizasyonlarını yürütür. Ayrıca, Türk Arama Kurtarma Yönetmeliği kapsamında arama kurtarma faaliyetlerinde sağlık organizasyonu sağlar (Sağlık Bakanlığı 2015).

2.1.3.8. Teleradyoloji Sistemi

Teleradyoloji, radyolojik görüntülere web ve mobil ortamda 7/24 erişim sağlayan, bu görüntülerin raporlanmasını ve radyologlar arasında telekonsültasyon yapılmasını mümkün kılan bir sistemdir. Türkiye'de T.C. Sağlık Bakanlığı tarafından geliştirilen Teleradyoloji Sistemi, tıbbi görüntülerin ve raporların kalite açısından değerlendirilmesini ve e-Nabız uygulaması üzerinden vatandaşlarla paylaşılmasını da içerir. Bu sistem, radyolojik tetkiklerin uzaktan incelenmesini ve raporlanmasını kolaylaştırarak sağlık hizmetlerinin erişimini ve kalitesini artırır (Sağlık Bakanlığı 2015).

2.1.3.9. Neyim Var Uygulaması

Neyim Var uygulaması, kullanıcıların girdiği şikayetlere dayanarak olası teşhis tahminleri yapar ve doğru branşa yönlendirme sağlar. Kullanıcılar, şikayetlerini belirtilen soruları yanıtlayarak muhtemel teşhisler alabilir ve Merkezi Hekim Randevu Sistemi'ne (MHRS) bağlanarak ilgili branştan randevu oluşturabilirler. Neyim Var? uygulaması, Türkiye'nin sağlık sektöründeki çalışmaları geliştirmek ve sağlık hizmetlerinde yenilikçi fikirleri teşvik etmek amacıyla düzenlenen Doktorclub Awards'da "Yılın Sağlık Bilgi Sistemleri- Yenilikçi Ürünü/Uygulaması" ödülünü kazandı. Bu ödülle, sağlık sektöründe farklılık ve farkındalık yaratmak için önemli bir adım atıldı (Sağlık Bakanlığı 2024).

2.1.3.10 Yaşlı Bireylere Güvenlik Destek Uygulamaları

Türkiye'de yaşlılar, engelliler ve hasta kişiler için evde kullanıma yönelik sağlık alarm sistemleri mevcuttur. Bunlardan biri, Esenler Belediyesi'nin "Hayat Butonu" uygulamasıdır. 2013 yılında tanıtılan ve 2016'da kolye şekline dönüştürülen bu buton, yaşlıların sürekli taşıyabilmesi için tasarlanmıştır. Kablosuz bağlantı teknolojisine sahip acil durum hayat kolyesi, ev telefonuna 50 metreye kadar olan mesafede çalışmaktadır. Butona basarak ESTİM'e ihtiyaçlarını bildiren yaşlılar, bu sayede hızlıca yardım alabilirler. Proje, 440 09 23 numaralı özel hat üzerinden de acil durumlarda destek sunar (Esenler Belediyesi 2016).

2.1.3.11. Uzaktan Hasta Değerlendirme

Uzaktan hasta izleme (Remote patient monitoring), hastaların sağlık hizmetlerine kliniklere gitmeden erişmelerini sağlayan bir teknolojidir. Bu sistemler, sağlıklı bireylerin yanı sıra yaşlı ve sağlıklı insanların sağlık durumlarını takip etmek için de kullanılır. Giyilebilir sağlık cihazları ve mobil uygulamalarla çalışan bu sistemler, sağlık hizmeti maliyetlerini azaltırken, kişiye özel sağlık haritaları oluşturarak erken teşhis ve tedaviye yardımcı olur. Kişisel veriler KVKK kapsamında güvenli bir şekilde saklanır ve analiz edilir (T.C. Çevre, Şehircilik ve İklim Değişikliği Bakanlığı 2024).

2.1.3.12. EPİC

Epic yazılımı, sağlık hizmetlerinde çeşitliliği ve eşitliği destekleyerek hasta bakımını iyileştirmeyi amaçlar. Yazılım, ırk, cinsiyet, yönelim gibi kişisel farklılıkları gözetmeden tüm bireylerin sağlık eşitsizliklerini belirlemeye ve çözmeye yardımcı olur. Geniş ölçekli sağlık sistemlerinden küçük Federally Qualified Health Centers'a kadar pek çok kuruluş tarafından kullanılır. Epic, toplumsal katkıyı önemser ve çalışanları aracılığıyla gönüllü faaliyetler, bağışlar yapar. 2022 yılında, sağlık, konut ve eğitim alanlarında birçok kuruma bağış yapılmıştır. Epic'in hedefleri arasında kapsayıcı bir çalışma ortamı sağlamak, eşitlik projelerini desteklemek ve çeşitli geçmişlere sahip nitelikli personelin işe alımını teşvik etmek yer alır (Epic 2024).

2.1.3.14. Cerner Health

Cerner Health, sađlık verilerini merkezi bir platformda toplama ve yonetme surecini sadelestiren bir cozumdur. Ilaclar, alerjiler, doktor ziyaretleri ve kisisel sađlık olcumlari gibi bilgileri duzenleyip saklayarak, kullanicilarin sađlık verilerini aile uyerleriyle paylasmalarına olanak tanir Ebeveynlerin ve aile uyelerinin sađlık bilgilerini yonetmelerine olanak sađlayan bu ozellik, cocukların, genclerin ve yasli aile bireylerinin sađlığını etkili bir sekilde koordine eder. Cerner Health, doktorlar ve hastanelerle elektronik iletisimi destekler ve e-ziyaretler aracılığıyla fiziksel ziyaret gereksinimini ortadan kaldirir. Ayrıca, kisisel sađlık olcumlerrinin takibiyle, sađlık eđilimlerini proaktif bir sekilde yonetmenize ve sađlık hedeflerinize gore ilerlemenizi izlemenize yardımcı olur. İnternet erişimi olan her yerde sađlık bilgilerinize ulaşmanızı sađlayan bu sistem, guvenli bir kullanıcı kimligi ile kisisel sađlık bilgilerinizi korur ve her an erişilebilir kılar (Cerner Health 2024).

2.1.3.14. IBM Watson Health

Son yıllarda sađlık teknolojilerinin benimsenmesi ve dijital yeniden yapılandırma hızla ilerlemiştir. IBM, sađlık sektöründeki dönüşümü destekleyerek akıllı mimariler, modernize edilmiş çekirdek sistemler, açık standartların benimsenmesi ve ölçeklenmiş veri deđerleri sunmaktadır. Şirket, veri ve yapay zeka ihtiyaçlarına yönelik guvenli platform deneyimleri tasarlamaktadır. Ayrıca, gelişmiş sađlık teknolojisi çözümleri ve dijital dönüşüm hizmetleri sađlayarak, bu çözümleri geniş ölçekli olarak uygulama imkânı sunmaktadır. IBM, sađlık sektöründeki dönüşüm sürecinde guvenilir bir ortak olarak önemli bir rol oynamaktadır. (IBM 2024)

2.1.3.15. Veradigm

Veradigm, 1986 yılında kurulan ve daha önce Allscripts olarak bilinen bir entegre veri sistemleri ve hizmetler şirkettir. Veri odaklı klinik bilgiler ve uygulanabilir araçları bir araya getirerek, yaşam bilimleri, sađlık planları, sađlık hizmeti sađlayıcıları ve hastalar gibi sađlık hizmeti paydaşlarının hizmet kalitesini, verimliliğini ve deđerini artırmalarına yardımcı olur. Veradigm, klinik ve finansal çözümler, açık standartlara bađlılık ve geniş bir sađlık hizmeti sađlayıcı ağı sunar. Şirket, sađlık, teknoloji ve yenilik liderlerini çekerek, sađlık kalitesini artırmayı ve maliyetleri düşürmeyi

amaçlayan ileri düzey çözümler geliştirmektedir. Veradigm Ağı, sağlık hizmetlerini dönüştüren ve değer yaratan çözümler sunan dinamik bir şirket topluluğudur (Veradigm 2024).

2.2. Dijital Veri Güvenliği Farkındalığı

2.2.1. Dijital Veri Güvenliği

Günümüzde yaygın olarak kullanılan iletişim araçları, dijital veri güvenliği konusunu önemli kılmıştır. Elektronik ortamda bilgilerin yaygın kullanımının sunduğu avantajlarla birlikte, bu durumun dezavantajları da giderek daha belirgin hale gelmektedir (Yılmaz 2015: 2).

McCumber'ın (2005) tanımına göre bilgi güvenliği, bilgi ve bilgi sistemlerini kötü niyetli erişim, kullanım, ifşa edilme, bozulma veya değiştirme gibi tehditlere karşı korumak amacıyla alınan önlemleri içerir. Aynı zamanda bu önlemler, bilginin gizliliği, bütünlüğü ve kullanılabilirliği açısından da koruma sağlamayı hedefler. McCumber'ın tanımı, teknolojik gelişmelere ve günümüzdeki güvenlik zorluklarına uyumlu bir şekilde bilgi güvenliğini ele almaktadır (Henkoğlu ve Yılmaz 2013: 453). Bir başka tanımda ise bilgi güvenliği, elektronik ortamlarda verilerin korunması için yapılan çabalardır. Bu çabalar, bilgilerin bütünlüğünün sağlanması ve izinsiz erişimlere karşı koruma içerir. Bu hedeflere ulaşmak için uygun bir güvenlik politikasının belirlenmesi ve uygulanması oldukça önemlidir (Canbek ve Sağıroğlu 2006: 168). Fussel (2005)'e göre bilgi güvenliği gizlilik, bütünlük ve erişilebilirlik olarak üç kısımdan oluşmaktadır.



Şekil 2: Bilgi Güvenliği İlkeleri (Kaynak: Fussel, 2005)

Gizlilik: Yetkisi olmayan kişilerin bilgiye erişememesi esasına dayanır. Bu sayede hassas bilgiler korunur.

Bütünlük: Bilginin doğruluğunun ve bütünlüğünün korunmasıdır. Bilginin içeriği değiştirilmemiş ve bozulmamış olmalıdır.

Erişilebilirlik: Bilgiye erişim yetkisi olanların, bilgiye istedikleri anda ulaşabilmesi ve kullanabilmesidir (Doğantimur 2009: 7).

Bilgi güvenliği, gizliliği, bütünlüğü ve erişilebilirliği içeren üç temel unsuru bir arada sağlamayı amaçlar. Bilgi gizliliği, bilgiye yetkisiz erişimi önlerken bilginin erişilebilir olması, istenildiği zaman kullanılabilir olmasını gerektirir. Aynı zamanda erişilebilen bilginin bütünlüğü korunmalıdır; çünkü bilgi doğru ve eksiksiz olmalıdır. Bu üç unsurdan herhangi biri göz ardı edildiğinde, bilgi güvenliği riske girebilir ve olumsuz sonuçlara yol açabilir (Doğantimur 2009: 7).

2.2.2. Dijital Veri Güvenliğini Tehdit Eden Unsurlar

2.2.2.1. İnsan Kaynaklı Tehditler

Tekerek 2008' e göre insan kaynaklı tehditler bir kullanıcının sistemi bilinçsiz ve bilgisizce, yeterli eğitime sahip olmadan kullanmasıyla ortaya çıkma olasılığı bulunan aksaklıklar yer almaktadır (Tekerek 2008: 134)

Wagner ve Brooke'un (2007) çalışmasına göre, insan kaynaklı faktörlerin, veri güvenliğinde olumsuz durumların meydana gelmesinde önemli bir rol oynadığı görüşü dile getirilmektedir. İnsan kaynaklı tehditler, siber güvenliği etkileyen önemli unsurlardan biridir ve genellikle bilinçli veya bilinçsiz olarak gerçekleştirilen girişimlere dayanmaktadır. Bu tehditler, kurum içindeki güvenlik yönetimindeki eksiklikler, yetersiz güvenlik farkındalığı ve denetim mekanizmalarındaki eksiklikler gibi faktörlere bağlı olarak ortaya çıkmaktadır (Korucu 2021: 22).

2.2.2.2. Yazılım Tehditleri

Yazılımlar, kötü niyetli müdahalelere maruz kalarak tahrip edilebilir, değiştirilebilir, silinebilir veya kaza ile değişikliğe uğrayabilir. Bu tür yazılım değişiklikleri genellikle kolayca fark edilemez. Örneğin, bir program, daha önce gerçekleştirdiği her işlemi yapmaya devam edecek ve aynı zamanda saldırganın istediği ekstra işlemleri gerçekleştirecek şekilde değiştirilebilir (Shephard, 2002).

Yazılım tehditleri, bilgisayar sistemlerindeki yazılımları hedef alan çeşitli riskleri içermektedir. Bu tehditler, kullanıcı bilgisayarlarına zarar verebilen veya veri kaybına yol açabilen çeşitli saldırıları içerir. Örneğin, kötü amaçlı yazılımların bulaşması, yazılımların bilinçsizce değiştirilmesi veya silinmesi gibi durumlar yazılım tehditlerine dahildir (Korucu 2021: 23).

2.2.2.3. Güvenlik Zafiyetleri

Toplumun her kesimi, sanal hayatları ile gerçek hayatları arasındaki sınırların belirsizleşmesinden kaynaklanan güvenlik açıklarından etkilenmektedir. Bu tür sitelere sağladığımız kişisel bilgilerin kötüye kullanılması, banka hesaplarının boşaltılması, bilgisayar sistemlerine virüs bulaştırılması ve hatta bireylerin küçük düşürülmesi gibi çeşitli tehditlerle karşılaşılabilir.

Korucu'nun ifadesine göre, güvenlik zafiyetleri, yazılım, donanım veya tasarım hatalarından kaynaklanan açıklıklardır ve bu hatalar bilgisayar sistemlerinin güvenliğini tehlikeye atar. Bu zafiyetler, kötü niyetli virüs veya trojan gibi zararlı yazılımlar tarafından söz konusu hataların istismar edilmesiyle ortaya çıkar, bu da veri açıklıklarına neden olabilir. (Korucu 2021: 23)

2.2.2.4. Veri Açıklıkları

İnceleme sonuçlarına göre, bilginin ve teknolojinin birbirine entegre olduğu, teknolojinin hızla gelişen elektronik ortamları desteklediği bir dönemde, kötü niyetli kişilerin veya casus yazılımların sistemi açık bulma, bu açıkları kullanarak izinsiz erişim sağlama ve kişisel veya kurumsal zarar verme amacıyla birçok yöntemi denediği belirlenmiştir.

Bilgisayar sistemlerindeki verilerin istenmeyen bir şekilde dışarı sızması veri açıklıklarından kaynaklanmaktadır. Bu tür olaylar güvenlik açıklıklarının bilgisayar korsanları tarafından istismar edilmesi, siber saldırılar veya finansal çıkar amacıyla gerçekleştirilen hack olaylarını kapsar (Korucu 2021: 23).

2.2.2.5. Siber Casusluk ve Sürekli Tehditler

Aslay 2017' göre Bilişim ve internetin hızla yaygınlaşması, kullanıcılara kolaylık ve özgürlük sağlarken, aynı zamanda ortaya çıkan güvenlik açıkları nedeniyle sistemlerin kötüye kullanılmasına sebebiyet vermektedir. Bu güvenlik açıkları,

yalnızca bireyleri değil, kişisel önlemlerin alınmaması nedeniyle zaman zaman sistemleri de tehlikeye atabilmektedir. (Aslay, 2017:24).

Siber casusluk, genellikle devletler veya büyük ölçekli organizasyonlar tarafından, geniş kaynaklar ve uzun vadeli stratejilerle planlanan veri hırsızlığı faaliyetlerini ifade eder. Bu tür saldırılar genellikle devlet destekli aktörler veya büyük çaplı siber suç örgütleri tarafından gerçekleştirilir. Ayrıca, "Advanced Persistent Threat (APT)" olarak bilinen tehditler, özellikle uzun vadeli saldırıları içerir (Korucu 2021: 24).

2.2.2.6. Mobil Tehditler

Teknolojinin hızlı gelişimi ve çeşitlenen mobil cihazlar, kullanıcılara sağladığı çeşitli hizmetler ve kolaylıklarla günlük yaşantımızın vazgeçilmez bir parçası haline gelmiştir. İletişim amacıyla kullanılan telefonlar, karmaşık fonksiyonlara sahip araçlar haline evrim geçirmiş ve mobil teknolojilerin sürekli yenilenmesi ve artan talep, gelecekteki dönemlerin mobil cihazlara odaklanacağını göstermektedir (Arslan, Gündüz, Sağıroğlu 2015: 1).

Mobil tehditler, cep telefonları, tabletler ve benzeri mobil platformları hedef alan zararlı yazılımları kapsar ve bu tür tehditler son yıllarda giderek daha fazla gündeme gelmektedir. Mobil zararlı yazılımlar genellikle kullanıcı verilerini hedef alır ve bu cihazlarda depolanan hassas bilgileri tehlikeye atar. Özellikle Android tabanlı platformların yaygınlaşması ve resmi uygulama mağazalarının dışından uygulama yüklenmesine izin verilmesi, mobil tehditlerin çeşitlenmesine ve artmasına olanak sağlamıştır (Korucu 2021: 24).

2.2.2.7. E-Posta Tehditleri ve Spam E-Postalar:

E-posta hem akademik hem de ticari iş süreçlerinde yaygın olarak kullanılmakta olup, resmi yazışmalardan duyurulara kadar birçok kurumsal durumda iletişim aracı olarak kullanılmaktadır. Ancak, bu yaygın kullanım güvenlik endişelerini de beraberinde getirmiştir. Gönderilen veya alınan e-postaların güvenliği, kurum içi uygulamalarda sıklıkla sorgulanan bir konu haline gelmiştir (Levi 2003: 1).

E-posta tehditleri ve spam e-postalar, bireylerin ve işletmelerin e-posta adreslerinin izinsiz bir şekilde paylaşılması ve kontrolsüz erişim sağlanan internet

siteleri aracılığıyla gönderilen istenmeyen e-posta iletilerini içermektedir (Korucu 2021: 24).

2.2.2.8. Sosyal Medya Tehditleri

Sosyal medya platformlarının gelişimi ve yaygınlaşması, günümüzün dijital çağında ergenler arasında vazgeçilmez bir etkileşim ve iletişim alanı haline gelmiştir. Facebook, Instagram, MySpace, Twitter, WhatsApp gibi platformlar, gençlerin diğer insanlarla bağlantı kurma, bilgi paylaşma ve ortak ilgi alanlarını sürdürme amacıyla önemli miktarda zaman harcadıkları birer mecra haline gelmiştir. Bu eğilim, son yıllarda sosyal ağ kullanıcılarının sayısında belirgin bir artış olduğunu göstermektedir (Elmalı 2020: 440). Ergenler gibi yetişkinler de sosyal medya platformlarını sıklıkla kullanmaktadır. Ancak, bu platformların sıklıkla kullanılması, siber tehditlerin de artmasına neden olmaktadır. Sosyal mühendislik saldırıları ve oltalama teknikleri, bu sosyal medya platformlarında en sık uygulanan saldırı yöntemleri arasında yer almaktadır. Bu durum, Kişisel Verileri Koruma Kanunu (KVKK) ve uluslararası düzeyde Genel Veri Koruma Yönetmeliği (GDPR) ile bağlantılı olarak sık sık gündeme gelmektedir (Korucu 2021: 24).

2.2.2.9. Bulut Teknolojileri Tehditleri

Bulut bilişim, paralel hesaplama, dağıtık hesaplama ve sanallaştırma teknolojilerinin gelişimini simgeler, talep üzerine internet altyapısına dayanarak esnek, uygun maliyetli ve yapılandırılabilir hesaplama kaynakları sunan bir teknolojidir (Aksakallı 2019: 8). Son yıllarda önemli bir ivme kazanan ve gelecekte de oldukça önemli bir konumda olacağı düşünülen bulut bilişim teknolojileri, siber güvenlik tehditlerinde önemli bir artışa neden olmaktadır. Bulut sistemleri, her türden veriyi barındırması nedeniyle yeni güvenlik düzenlemelerine ihtiyaç duyulduğunu işaret etmektedir. Öne çıkan bir bulut bilişim siber tehdidi örneği, ünlülerin Apple'a ait iCloud platformundan çalınan ve internete sızdırılan fotoğraflarıdır. Apple firması, bu saldırıda sorumluluk kabul etmeyerek, veri kaybının kullanıcıların hatalı kullanımından kaynaklandığını belirterek kullanıcıları suçlamıştır (Korucu 2021: 25).

2.2.3. Saęlıkta Dijital Veri Gvenlięi Farkındalıęı

Dijital veri gvenlięi konusundaki farkındalık dzeyi, bireylerin kendi dijital bilgilerinin gvenlięini saęlama, kiřiisel bilgilerin sınırlarını belirleme, kiřiisel hak ihlallerini nleme ve kiřiisel veri gvenlięi aısından kritik bir neme sahiptir. Bu baęlamda, yksek farkındalıęa sahip olan bireylerin dijital verilere olan gven dzeyinin de arttıęı gzlemlenmiřiştir. Bireylerin bu konuda sahip olduęu bilgi birikimi dijital veri gvenlięini saęlamak adına nemli bir etken olarak ne ıkmaktadır (Karaaslan, nr, oban 2023: 167).

Saęlık kuruluřları iin, hastaya ait bilgilerin gizlilięi ve mahremiyet ilkelerinin korunması, temel ve kritik alanlardan biridir. Saęlıkta Akreditasyon Standartları (SAS) ve Saęlıkta Kalite Standartları (SKS) deęerlendirildięinde, bilgi ve belge gvenlięi gibi konuların, rekabet avantajı elde etme aısından byk bir neme sahip olduęu gze arpmaktadır (Varol, Orhan, Tuncer, Akyz 2016: 155). Dijital saldırıların temel sebeplerinden biri de hastalara ait zel ve nemli bilgilerin, nc kiřiiler tarafından kullanılmasının beraberinde maddi ve manevi eřitli getirilere yol amasıdır. Hastaların kimlik bilgileri, saęlık gemiři, medikal grntleri, gemiři ve mevcut rahatsızlıklar, tehdit eden rahatsızlıkları, tedavi ierikleri, diyet programları, cinsel saęlık sorunları, genetik bilgiler, psikolojik profiller ve fiziksel eksikliklere dair birok veri ve bilgi, kt niyetli kiřiiler tarafından istismar edilebilecek niteliktedir (Mercuri 2004: 27).

2000'li yılların bařında, dnya genelinde saęlık kuruluřları, hastaların bilgilerini elektronik veri tabanlarına gizleme amacıyla nemli abalar gstermiři olsa da bu veri tabanlarına ynelik saldırılar byk bir artıř gstermiři ve milyonlarca hastanın kiřiisel bilgileri yasadıřı yollarla nc kiřiilere sızarak ciddi bir gvenlik sorunu ortaya ıkmıřtır (Solutions 2008: 3).

Hasta bilgilerini paylařırken gven duygusu n plandadır. Saęlık kuruluřlarında, bu zel verilerin etkili bir řekilde korunması, hastaların gvenlięi ve gizlilięi iin kritik bir neme sahiptir. Bununla birlikte, alıřanların saęlıkla ilgili verilere ynelik olası risklere karřı daima dikkatli olmaları nemlidir. Zira veri gvenlięi alıřmaları srecinde, daha ok iř gcnn neden olduęu sorunlar ne ıkmaktadır (Damrongsak ve Brown 2008: 420).

Sonu olarak, dijital veri gvenlięi farkındalıęı bireylerin dijital bilgilerini koruma ve saęlık sektrnde hastaların gizlilięini saęlama konularında kritik bir rol oynamaktadır. Farkındalık dzeyinin yksek olması, bireylerin dijital verilere olan gvenini artırabilir ve saęlık kuruluřları iin bilgi gvenlięi standartlarına uymak rekabet avantajı saęlayabilir. Ancak, dijital saldırılar ve veri gvenlięi ihlalleri, zellikle saęlık sektrnde ciddi tehditler oluřturmaktadır. Saęlık kuruluřlarının etkili bir bilgi gvenlięi politikası benimsemesi ve alıřanları bu konuda eęitmesi kritik bir gerekliliktir. alıřanların bilinli davranması ve daima tedbirli olmaları, bu alandaki riskleri minimize etmede nemli bir rol oynar. Dijital veri gvenlięi, gvenilir ve srdrlebilir bir dijital ortam oluřturmak iin srekli olarak geliřtirilmeli ve glendirilmelidir.

2.2.4. Trkiye’de ve Dnyada Dijital Veri Gvenlięini Saęlamak Amacıyla Yapılan Faaliyetler

2.2.4.1.Kiřisel Verilerin Korunması Kanunu (KVKK):

Gnmzde, birok kiřisel veri otomatik yollarla iřlenmektedir. nceden manuel olarak iřlenen veriler de hızla elektronik ortama tařınmaktadır. Bu nedenle, “tamamen veya kısmen otomatik yollarla iřlenen veriler” ve “veri kayıt sistemlerinin bir parası olarak otomatik olmayan yollarla iřlenen veriler,” 6698 sayılı Kiřisel Verilerin Korunması Kanunu kapsamında korunmaktadır (KVKK 2010).

2.2.4.2.Bilgi Gvenlięi Ynetim Sistemi (BGYS) Standardı (ISO/IEC 27001):

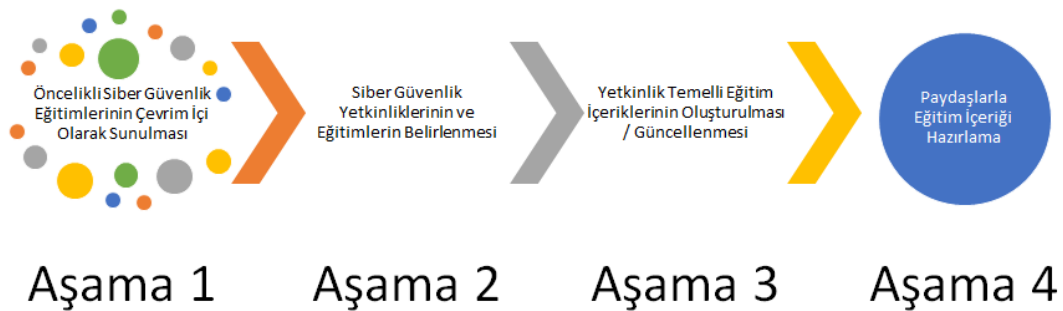
Gn getike artan iletiřim ortamları ve kullanımı, bilgi gvenlięinin saęlanması gereklilięini daha da n plana ıkarmıřtır. Ancak, yalnızca teknik nlemlerle (gvenlik duvarları, saldırı tespit sistemleri, antivirs yazılımları, řifreleme, vb.) kurumsal bilgi gvenlięini saęlamanın yetersiz olduęu anlařılmaktadır. Bu baęlamda, insanları, sreleri ve bilgi sistemlerini kapsayan, st ynetim tarafından desteklenen bir ynetim sistemi kurma ihtiyaı ortaya ıkmıřtır (Yılmaz 2014). ISO/IEC 27001 Bilgi Gvenlięi Ynetim Sistemi, bilgi varlıklarını korumak ve gvenlik kontrollerini saęlamak iin tasarlanmış uluslararası bir standarttır. Bu standart risk deęerlendirmesi, politika oluřturma, uygulama ve srekli iyileřtirme gibi alanlarda rehberlik saęlar. Trk Standartları Enstits de bu alanda alıřmalar yaparak bilgi gvenlięi ynetim sistemlerinin belgelendirilmesine katkıda bulunmaktadır (T.S.E 2023).

2.2.4.3. Siber Güvenlik Strateji ve Eylem Planı:

Türkiye'de siber güvenlik alanında önemli bir kilometre taşı olan "Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı", 20 Haziran 2013 tarihli ve 28683 sayılı Resmî Gazete'de yayımlanarak yasallaştırıldı. Bu iki yıllık süre boyunca siber güvenlik politikasının kullanımı, kritik altyapıların güvenliğinin sağlanması, küresel siber güvenliğin çeşitliliği ve siber tehditlerin ayrılması ve önlenmesi gibi çeşitli işlemler hayata geçirilmiştir. Ayrıca, 2013 yılında Bilgi Teknolojileri ve İletişim Kurumu bünyesinde faaliyet gösteren Ulusal Siber Olaylara Müdahale Merkezi (USOM) kurularak, kayıtlı kritik altyapı sektörleri başta olmak üzere kurum ve kuruluşlarda Siber Olaylara Müdahale Ekipleri (SOME) hizmet vermeye başlamıştır. Bu sayede ulusal siber güvenlik desteği oluşturularak, kurumsal ve organizasyonel yapılar güçlendirilmiştir (T.C Ulaştırma ve altyapı bakanlığı 2020-2023).

2.2.4.4. Siber Güvenlik Eğitim ve Farkındalık Programları:

Siber Güvenlik Eğitim Portalı, Kalkınma Bakanlığı iş birliğiyle TÜBİTAK-BİLGEM Siber Güvenlik Enstitüsü tarafından yönetilen Siber Güvenlik Eğitim ve Araştırma Merkezi Projesi, Siber Güvenlik Eğitim Altyapısı iş paketi kapsamında faaliyete geçirilmiştir. Siber Güvenlik Eğitim Portalının hedefleri arasında toplumun siber güvenlik konularındaki farkındalığını artırmak, yükseköğretim öğrencilerine siber güvenlik teknolojileri konusunda teknik bilgi kazandırmak ve siber güvenlik uzmanlarının yetkinliklerini geliştirmek için gerekli eğitimleri çevrim içi olarak sunmak yer almaktadır (SGEP 2017).



Şekil 3: Siber Güvenlik Eğitimi Hedefleri (Kaynakça: SGEP, 2017)

2.2.4.5. Elektronik İmza ve Elektronik Belge Hizmet Sağlayıcıları:

Elektronik belgeler, temel olarak sayısal olarak kodlanmış verileri ifade eder. Bu kapsamda, internet üzerinde gerçekleştirilen hukuki işlemler, e-posta aracılığıyla iletilen irade beyanları ve çeşitli veri taşıyıcılarına kaydedilmiş irade açıklamalarını içeren elektronik verileri anlamamıza olanak tanır (Erturgut 2003: 66). Elektronik belge yönetim sistemleri, e-devlet projelerinin temel inşaat taşlarından biridir ve kurumsal süreçlerin düzenlenmesi ve kayıt altına alınması için hayati bir araç olarak hizmet vermektedir (Kandur 2011: 4).

Elektronik imza, kanun kapsamında, başka bir elektronik veriye eklenen veya elektronik veriyle mantıksal bağlantısı bulunan ve kimlik doğrulama amacıyla kullanılan elektronik veri olarak tanımlanmıştır. Kanunun belirlediği şartlara uygun olarak kullanılan güvenli elektronik imzanın, elle atılan imza ile aynı hukuki sonucu doğurması, elle atılan imza ile aynı ispat gücünü haiz olması, usulüne göre güvenli elektronik imza ile oluşturulan elektronik verilerin senet hükmünde olması ve bu verilerin aksi ispat edilinceye kadar kesin delil sayılması gibi hukuki açıdan önemli yenilikleri getirdiği belirtilmektedir (BTK 2017). Elektronik imzanın önemi, hukuki işlemlerde güvenliğin, kimlik tespitinin ve inkar edilememe özelliklerinin aranmasından kaynaklanmaktadır. Elektronik imza, bu temel unsurları sağlama konusunda dijital platformlara güvenilir bir çözüm sunar (Erturgut 2003: 68).

2.2.4.6. Kamu Siber Olaylara Müdahale Ekipleri (USOM):

Ülkemizin siber güvenliğine yönelik önemli adımları düzenleyen belgeler arasında, 20/10/2012 tarih ve 28447 sayılı Resmi Gazete’de yayınlanan "Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Bakanlar Kurulu Kararı" ile 5809 sayılı Elektronik Haberleşme Kanunu gereğince 20/06/2013 tarih ve 28683 sayılı Resmi Gazete’de yayımlanan 2013/4890 sayılı Bakanlar Kurulu Kararı bulunmaktadır. Bu kararlar, "2013-2014 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı"nı başlatmıştır (USOM 2023).

Bu strateji ve eylem planı kapsamında, Bilgi Teknolojileri ve İletişim Kurumu bünyesinde 27/05/2013 tarihinde Ulusal Siber Olaylara Müdahale Merkezi (USOM, TR-CERT) kurulmuştur. Aynı dönemde kamu kurum ve kuruluşları bünyesinde de Siber Olaylara Müdahale Ekipleri (Kurumsal SOME, Sektörel SOME)

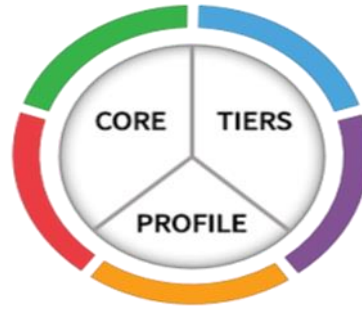
oluşturulmuştur. USOM ve SOME'ler, siber olayların belirlenmesi, etkilerinin azaltılması veya ortadan kaldırılması için önlemlerin geliştirilmesi amacıyla hayati öneme sahiptir. Bu yapılar, siber olay yönetiminin ulusal düzeyde koordinasyon ve iş birliği içerisinde gerçekleştirilmesine katkı sağlamaktadır (USOM 2023).

2.2.4.7. NIST Cybersecurity Framework:

Ulusal Standartlar ve Teknoloji Enstitüsü (NIST), kritik altyapı sektörlerindeki kuruluşlara siber güvenlikle ilgili riskleri azaltmaları için rehberlik sağlamak amacıyla bir çerçeve yayınlamıştır (Almuhammadi ve Alsaleh 2017).

Siber güvenlik çerçevesi, temel olarak çekirdek, uygulama kademeleri ve profiller olmak üzere üç ana bileşenden oluşmaktadır. Çerçeve çekirdeği, siber güvenlik faaliyetleri ve sonuçlarını anlaşılabilir bir dil kullanarak kuruluşlara rehberlik eder.

Çerçeve uygulama kademeleri, bir kuruluşun siber güvenlik risk yönetimini etkili bir şekilde gerçekleştirir. Çerçeve profilleri ise bir kuruluşun kurumsal gereksinimlerini, hedeflerini, risk analizini ve kaynaklarını çerçeve çekirdeğinin istenen sonuçlarına göre özelleştirmesini sağlar. Bu profiller, siber güvenliğin iyileştirilmesine yönelik fırsatları belirlemek için kullanılır (Nist 2023).



Şekil 4: Siber Güvenlik Çerçevesi (Kaynak: Nist, 2023)

2.2.4.8. CIS Critical Security Controls:

Center for Internet Security, Inc. (CIS), dünyayı daha güvenli hale getirmeyi amaçlayan, iş birliği ve yenilikçilik üzerine odaklanan bir kuruluştur. CIS sorumlu, topluluk odaklı, kâr amacı gütmeyen bir organizasyondur. Bu standartları sürekli

olarak gncelleyerek ve proaktif bir koruma saęlamak amacıyla rn ve hizmetler sunarak kresel bir BT profesyonelleri topluluęuna liderlik etmektedir. CIS bulutta gvenli, isteęe baęlı ve leklenebilir bilgi iřlem ortamları sunmaktadır (CIS 2023).

2.2.4.9. GDPR (General Data Protection Regulation):

AB Genel Veri Koruma Dzenlemesi (GDPR), dnya genelinde en etkili gizlilik ve gvenlik yasası olarak kabul edilmektedir. Bu dzenleme, 1995 tarihli veri koruma direktifinin temel prensiplerini gncelleyip modernize ederek, 2016 yılında kabul edilmiř ve 25 Mayıs 2018 tarihinde yrrlęe girmiřtir.

GDPR, dijital aęda bireylerin temel haklarını, veri iřleyenlerin ykmllklerini ve uygunluęun saęlanmasıya ynelik yntemleri tanımlar. Ayrıca, bu kurallara uymayanlara ciddi yaptırımlar ngrr (AB 2023).

2.2.4.10. HIPAA (Health Insurance Portability and Accountability Act):

HIPAA Amerika'da saęlık sektrnde faaliyet gsteren kuruluřları dzenleyen bir yasadır. Kiřisel saęlık bilgilerinin gvenlięini saęlamak ve gizlilięini korumak amacıyla oluřturulmuřtur.

Halk saęlıęı hukuku nceliklerini belirleme, arařtırma kanunları zerinde alıřma, halk saęlıęı yasal hazırlıęı analiz etme, yetki alanları arasında karřılařtırmalı analizler yapma, rehberlik etme, makaleler yazma, raporlar ve ara kitleri hazırlama gibi amalarla halk saęlıęı departmanları ve dięer ortaklarla birlikte alıřır. Ayrıca, halk saęlıęı hukuku mfredatının geliřtirilmesi ve yaygınlařtırılmasına da odaklanır (CDC 2023).

3.GEREÇ VE YÖNTEM

3.1 Araştırmanın Tipi

Tanımlayıcı kesitsel tipteki bu çalışma, Sivas Cumhuriyet Üniversitesi Sağlık Bilimleri Fakültesi (SBF) Sağlık Yönetimi Bölümü öğrencilerinin dijital vatandaşlık ve dijital veri güvenliği farkındalıkları arasındaki ilişkinin incelenmesi amacıyla yapılmıştır.

3.2 Araştırmanın Yapıldığı Yer ve Özellikleri

Araştırma Sivas Cumhuriyet Üniversitesi SBF Sağlık yönetimi Bölümünde gerçekleştirilmiştir. Araştırma için veriler Google Forms üzerinden online olarak toplanmıştır.

3.3. Araştırmanın Evreni ve Örneklemi

Araştırmanın evrenini (30.05.23-15.06.23) tarihleri arasında Sivas Cumhuriyet Üniversitesi SBF Sağlık Yönetimi bölümünde öğrenim gören (N=536) öğrenciler oluşturmaktadır. Araştırmanın örneklemini ise, bu tarihler arasında öğrenim gören ve araştırmaya katılmayı gönüllü olarak kabul eden (N=221) öğrenci oluşturmuştur. Çalışmada evrenin tümüne ulaşılabilceği düşünüldüğünden ayrıca örneklem seçimine gidilmemiştir.

3.4. Veri Toplama Araçları

Verilerin toplanmasında üç bölümlük veri toplama aracı kullanılmıştır. (EK 1) Bunlar; araştırmacılar tarafından hazırlanan ‘‘Kişisel Bilgi Formu’’, ‘‘Dijital Vatandaşlık Ölçeği ve ‘‘ Dijital Veri Güvenliği Farkındalığı Ölçeğidir ‘‘.

1.Kişisel Bilgi Formu

Bu formda araştırmada yer alan öğrencilerin cinsiyet, sınıf düzeyi, öğrenim gördüğü program, günlük internet kullanım süresi, aile gelir durumu, genel not ortalaması, teknolojik cihaz sahipliği, sosyal medya kullanım durumu ve sosyal medya kullanım süresini belirlemeye yönelik toplam 9 adet soru bulunmaktadır.

2.Dijital Vatandaşlık Ölçeği (DVÖ)

Dijital Vatandaşlık Ölçeği Seçil Som Vural tarafından üniversite öğrencilerinin bakış açısıyla dijital vatandaşlık göstergelerini ortaya çıkarmak amacıyla geliştirilmiştir. Ölçek toplam 23 sorudan ve (doğru kullanım, çevrimiçi işlemler, sağlık, erişim ve toplumsal sorumluluk) 5 alt boyuttan oluşmaktadır. Öğrencilerin dijital vatandaşlık düzeylerinin belirlendiği beşli Likert tipi ölçek “Kesinlikle katılıyorum=5”, “Katılıyorum=4”, “Kararsızım=3”, “Katılmıyorum=2” ve “Kesinlikle katılmıyorum=1” olarak yapılandırılmıştır.

Ölçeğin alt boyutları ve soru sayıları şu şekildedir:

Doğru kullanım alt boyutunda toplam 11 soru bulunmaktadır. Bu sorular güvenliğinden emin olmadığım dijital araçlarla parola gerektiren işleri yapmam ve dijital ortamlardaki paylaşımların bireyler üzerindeki etkisinin farkındayım gibi maddeleri içermektedir. Çevrimiçi işlemler alt boyutunda toplam 4 soru bulunmaktadır. Bu sorular çevrimiçi alışveriş yapmadan önce ürün veya hizmet ile ilgili bir araştırma (fiyat, kalite vb.) yaparım ve dijital araçları/ortamları kullanarak resmi işlemlerimi (bankacılık işlemleri, nüfus, askerlik, ikametgâh vb.) yürütürüm gibi maddeleri içermektedir. Sağlık alt boyutunda toplam 3 soru bulunmaktadır. Bu sorular dijital araçları kullanırken çalışma ortamımı ergonomik açıdan uygun şekilde (masa, sandalye, ortam ışığı vb.) düzenlerim ve dijital araçları, bu araçlardan kaynaklanabilecek sağlık sorunlarına (göz/iskelet sistemi rahatsızlıkları vb.) dikkat ederek kullanırım gibi maddeleri içermektedir. Erişim alt boyutunda toplam 3 soru bulunmaktadır. Bu sorular dijital ortamlara (sosyal ağlar, haber siteleri, bloglar vb.) çeşitli dijital araçlarla istediğim an bağlanırım ve haberleşme amaçlı farklı dijital iletişim ortamları (e-posta, sosyal paylaşım Erişim siteleri, bloglar, whatsapp vb.) kullanırım gibi maddeleri içermektedir. Toplumsal sorumluluk alt boyutunda toplam 2 soru bulunmaktadır. Bu sorular dijital ortamlarda yapılan yardım çağrılarına destek veririm ve dijital ortamlarda toplumsal sorumluluk projelerine katılımda bulunurum gibi maddeleri içermektedir.

3.Dijital Veri Güvenliği Farkındalığı Ölçeği (DVGFÖ).

Ölçek Eray Yılmaz tarafından öğretmenlerin dijital veri güvenliği farkındalıklarını ortaya koymak amacıyla hazırlanmıştır. Tamamı olumlu ifadeler içeren 32 madde tek

boyuttan oluřan ölçek, dijital veri güvenlięi konusundaki farkındalıęı ölçmeyi amaçlamaktadır. Ölçekteki ifadeler beřli Likert tipinde “Kesinlikle Katılıyorum=5”, “Katılıyorum=4”, “Kararsızım=3”, “Katılmıyorum=2”, “Kesinlikle Katılmıyorum=1” biçimindedir. “Kesinlikle Katılmıyorum” seçeneęinden başlamak üzere 1’den 5’e artan şekilde puanlanmıştır. Ölçekteki tüm maddeler olumlu ifadeler içermektedir. Ölçekten alınabilecek puan 32 ile 160 arasında deęişmektedir. Ölçekten elde edilen toplam puan arttıkça dijital veri güvenlięi farkındalıęı da artmaktadır.

3.5. Verilerin Toplanması

Veriler arařtırmaya gönüllü olarak katılım gösteren öğrencilerden Google Forms aracılığıyla online anket formu ile (30.05.23-15.06.23) tarihleri arasında toplanmıştır. Online formun linki öğrenci gruplarında paylaşılmıř gerekli açıklamalar yapılarak öğrenciler arařtırmaya katılmaları için davet edilmiştir.

3.6. Verilerin Deęerlendirilmesi

Çalıřmadan elde edilen verilerin analizi için IBM SPSS 25 (IBM SPSS, Türkiye) yazılımı kullanılmıştır. Verilerin normal daęılıma uygunluęu Shapiro-Wilk testi ile deęerlendirilmiştir. Tanımlayıcı istatistikler (ortalama, standart sapma, frekans) ile birlikte, nicel verilerin karşılaştırılması için normal daęılım göstermeyen parametreler arasında gruplar arası karşılařtırmalar için Kruskal-Wallis testi ve farklılık tespiti için Dunn’s testi kullanıldı. İki grup arasında normal daęılım göstermeyen parametrelerin karşılaştırılması için Mann-Whitney U testi kullanılmıştır. Normal daęılıma uygun olmayan parametreler arasındaki iliřkiler Spearman’s Rho korelasyon analizi ile incelenmiştir. Anlamlılık düzeyi ($p<0.05$) olarak belirlenmiştir.

3.7. Arařtırmanın Etik Yönü

Çalıřmaya başlamadan önce Sivas Cumhuriyet Üniversitesi 19.04.2023 tarihli ve 2023-04/06 karar numaralı Klinik Arařtırmalar Etik Kurul onayı (EK:3) ve Dijital Vatandaşlık Ölçeęi ile Dijital Veri Güvenlięi Farkındalıęı Ölçeęi’nin (EK:2) bu çalıřmada kullanılabilmesi için yazarlardan gerekli izinler alınmıştır . Arařtırmaya başlamadan önce öğrencilere çalıřmaya katılımın gönüllülük esasına göre olduęu

vurgulanmış, çalışma katılım sağlasa bile istediği zaman anketleri yanıtlamaktan vaz geçebileceği, kişisel bilgilerin gizli tutulacağı, isim yazmanın gerekmediği, elde edilecek verilerin yalnızca bilimsel amaçlı olarak kullanılacağı gibi gerekli açıklamalar yapılmıştır.



4. BULGULAR

Tablo 1: Öğrencilerin sosyo-demografik özelliklerinin dağılımı (N=221)

		N	%
Cinsiyet	Erkek	70	31,7
	Kadın	151	68,3
Sınıf	1	55	24,9
	2	47	21,3
	3	67	30,3
	4	52	23,5
Program	Normal öğretim	184	83,3
	İkinci öğretim	37	16,7
Günlük internet kullanım süresi	0-2	11	5,00
	2-4	62	28,1
	4-6	73	33,0
	6-8	37	16,7
	8+	38	17,2
Ailenin aylık geliri	<8500	71	32,1
	8500-12500	62	28,1
	12500-16000	40	18,1
	16000+	48	21,7
Genel not ortalaması	0-2	19	8,6
	2-3	104	47,1
	3-3,5	73	33,0
	3,5-4	25	11,3
Kendine ait bilgisayar var mı?	Yok	116	52,5
	Var	105	47,5
Kendine ait tableti var mı?	Yok	191	86,4
	Var	30	13,6
Kendine ait akıllı telefonu var mı?	Yok	21	9,5
	Var	200	90,50
Sosyal medya kullanımı	Hayır	4	1,80
	Evet	217	98,2
Günlük sosyal medya kullanım süresi	0-2	45	20,4
	2-4	60	27,1
	4-6	66	29,9
	6-8	31	14,0
	8+	19	8,6

n:frekans(sayı) %:yüzde

Çalışmaya katılan öğrencilerin % 68,3'ünü kadınların, %30,3'ünü 3. Sınıf öğrencilerinin, %83,3'ünü normal öğretim öğrencilerinin oluşturduğu, yarıya yakınının (%47,1) not ortalamasının 2.00-3.00 arasında olduğu saptanmıştır. Öğrencilerin %32,1'inin ailelerinin aylık gelir düzeyi 8500 TL'den (araştırma yapıldığı tarihte asgari ücret 8500 TL'ydi) daha azdır. Öğrencilerin %47,50'sinin bilgisayarı, %13,60'ının tableti, %90,50'sinin akıllı telefona sahiptir. Öğrencilerin %33,00'ü 4-6 saat arasında günlük internet kullanmaktadır. Öğrencilerin tamamına yakını (%98,20) sosyal medya kullanmaktadır (Tablo 1).

Tablo 2: Ölçeklerin toplam puanlarının ve alt boyutlarına ilişkin bilgilerin dağılımı

	Min.	Maks.	Ortalama	Standart sapma
DVGFÖ	1	5	3,9743	0,56308
DVÖ	1,17	5	4,0694	0,58824
Doğru Kullanım	1	5	4,1455	0,62613
Çevrimiçi İşlemler	1	5	4,1659	0,6679
Sağlık	1	5	3,8727	0,80773
Erişim	1	5	4,1288	0,70519
Toplumsal Sorumluluk	1	5	3,6636	0,90435

Öğrencilerin DVGFÖ, DVÖ toplam puan ve alt boyut puanlarına ilişkin bilgiler Tablo 2'de verilmiştir. Buna göre, DVÖ'nün toplam puan ortalaması ($\bar{x}$:4,0694) olarak saptanmıştır. DVÖ alt boyutlarından en yüksek ortalamaya sahip boyut çevrimiçi işlemler boyutu en düşük ortalamaya sahip olan boyut ise toplumsal sorumluluk boyutudur. DVGFÖ'nün toplam puan ortalaması ise ($\bar{x}$:3,9743) olarak saptanmıştır.

Tablo 3: Sosyodemografik özelliklere göre DVGFÖ'nin değerlendirilmesi

		Min.	Maks.	Ortanca	Ortalama	Standard Sapma	p
Cinsiyet¹	Erkek	1	5	4,09	4,08	0,69	0,026*
	Kadın	2,44	5	3,97	3,93	0,49	
Sınıf²	1	1	5	4	4,06	0,7	0,326
	2	2,81	4,97	3,88	3,88	0,51	
	3	2,94	5	4	3,99	0,42	
	4	2,44	5	3,92	3,94	0,61	
Program¹	NÖ	1	5	3,97	3,96	0,57	0,544
	İÖ	2,44	5	3,97	4,03	0,53	
Günlük İnternet Kullanımı Süresi²	0-2	3,63	5	4,31	4,26	0,5	0,021*
	2-4	2,97	5	3,88	3,88	0,47	
	4-6	2,81	4,97	3,97	3,99	0,46	
	6-8	2,72	5	3,91	3,9	0,61	
Gelir²	8+	1	5	4,25	4,09	0,78	0,005*
	<8500	2,44	5	3,83	3,83	0,53	
	8500-12500	2,94	5	3,97	3,99	0,5	
	12500-16000	2,81	5	4	4,01	0,47	
	16000+	1	5	4,08	4,15	0,7	
GNO²	0-2	2,81	4,59	4,06	3,95	0,44	0,363
	2-3	2,44	5	3,94	3,92	0,53	
	3-3,5	2,72	5	4	4,06	0,56	
	3,5-4	1	5	4	3,98	0,76	
Bilgisayar¹	Yok	2,44	5	3,97	3,9	0,5	0,046*
	Var	1	5	4	4,05	0,62	
Tablet¹	Yok	1	5	3,97	3,94	0,56	0,031*
	Var	3,09	5	4,28	4,17	0,54	
Telefon¹	Yok	3,22	5	4	4,12	0,55	0,334*
	Var	1	5	3,96	3,95	0,56	
Sosyal Medya Kullanımı¹	Hayır	2,72	4,53	3,36	3,49	0,79	0,125
	Evet	1	5	3,97	3,98	0,56	
Günlük sosyal medya kullanım süresi²	0-2	2,72	5	4	4,04	0,53	0,019*
	2-4	2,94	4,97	3,84	3,85	0,46	
	4-6	2,81	5	3,97	3,98	0,5	
	6-8	2,44	5	3,91	4,01	0,64	
	8+	1	5	4,31	4,14	0,89	

¹ Mann Whitney U Test ² Kruskal Wallis-H Testi *p<0.05

Erkek öğrencilerin ($\bar{x}=4,08$), günlük 0-2 saat arasında internet kullanan öğrencilerin ($\bar{x}=4,26$), aile geliri 16000 TL ve üstü olan öğrencilerin ($\bar{x}=4,15$), bilgisayar ($\bar{x}=4,05$) veya tablete ($\bar{x}=4,17$) sahip olan öğrencilerin, günlük 8 saat ve üzerinde sosyal medya kullanımı olan öğrencilerin ($\bar{x}=4,14$) dijital veri güvenliği farkındalığı, istatistiksel olarak anlamlı düzeyde yüksek bulunmuştur. Öğrencilerin hangi sınıfta olduğu, hangi programda olduğu, genel not ortalaması, telefona sahip olma durumu ve sosyal medya kullanıp kullanmaması, dijital veri güvenliği farkındalığı açısından istatistiksel olarak anlamlı bir farklılık oluşturmamaktadır (Tablo 3).

Tablo 4: Sosyodemografik özelliklere göre DVÖ'nin değerlendirilmesi

		Min.	Mak.	Ortanca	Ortal ama	Standard Sapma	p
Cinsiyet¹	Erkek	1,17	5	4,15	4,14	0,7	0,133
	Kadın	1,57	5	4	4,04	0,53	
Sınıf²	1	1,17	5	4,04	4,11	0,73	0,342
	2	3	5	4,17	4,08	0,47	
	3	2,91	5	4,02	4,14	0,47	
	4	1,57	5	4	3,93	0,64	
Program¹	NÖ	1,17	5	4,04	4,05	0,61	0,312
	İÖ	3	5	4	4,19	0,48	
Günlük İnternet Kullanımı Süresi²	0-2	3	5	4,17	4,24	0,61	0,017*
	2-4	1,57	5	4	3,91	0,57	
	4-6	3	5	4,07	4,12	0,49	
	6-8	2,65	5	4	4	0,59	
	8+	1,17	5	4,3	4,24	0,72	
Gelir²	<8500	2,65	5	4	3,96	0,5	0,008*
	8500-12500	2,91	5	4	4,07	0,52	
	12500-16000	3	5	4,11	4,08	0,49	
	16000+	1,17	5	4,35	4,22	0,8	
GNO²	0-2	3	4,87	4,04	4,01	0,55	0,315
	2-3	1,57	5	4	4,05	0,58	
	3-3,5	2,65	5	4	4,08	0,5	
	3,5-4	1,17	5	4,3	4,18	0,84	
Bilgisayar¹	Yok	2,65	5	4,04	4,05	0,53	0,588
	Var	1,17	5	4,04	4,09	0,65	
Tablet¹	Yok	1,17	5	4	4,05	0,56	0,048*
	Var	1,57	5	4,17	4,21	0,75	
Telefon¹	Yok	3,17	5	4,17	4,18	0,43	0,309*
	Var	1,17	5	4	4,05	0,60	

Sosyal Medya Kullanımı¹	Hayır	2,65	4,22	3,48	3,46	0,69	0,079
	Evet	1,17	5	4,04	4,08	0,58	
Günlük sosyal medya kullanım süresi²	0-2	2,65	5	4	4	0,58	0,016*
	2-4	1,57	5	4	3,91	0,59	
	4-6	3	5	4,09	4,15	0,47	
	6-8	3	5	4,13	4,19	0,44	
	8+	1,17	5	4,65	4,27	0,96	

¹ Mann Whitney U Test ² Kruskal Wallis-H Testi * $p < 0.05$

Günlük 8 saatten fazla ($\bar{x}=4,24$) veya 2 saatten az ($\bar{x}=4,24$) internet kullanan öğrencilerin, aile geliri 16000 TL ve üstü olan öğrencilerin ($\bar{x}=4,22$), tablete sahip olan öğrencilerin ($\bar{x}=4,21$), günlük 8 saat ve üzerinde sosyal medya kullanımı olan öğrencilerin ($\bar{x}=4,27$) dijital vatandaşlık düzeyi, istatistiksel olarak anlamlı düzeyde yüksek bulunmuştur. Öğrencinin cinsiyeti, hangi sınıfta olduğu, hangi programda olduğu, genel not ortalaması, bilgisayara veya telefona sahip olup olmaması ve sosyal medya kullanıp kullanmaması, dijital vatandaşlık düzeyi açısından istatistiksel olarak anlamlı bir farklılık oluşturmamaktadır (Tablo 5).

Tablo 5: Sosyodemografik özelliklere göre DVÖ'nin Doğru Kullanım alt faktörünün değerlendirilmesi

		Min.	Mak.	Ortanca	Ortalama	Standard Sapma	p
Cinsiyet¹	Erkek	1	5	4,23	4,19	0,72	0,338
	Kadın	1,18	5	4	4,13	0,58	
Sınıf²	1	1	5	4,18	4,18	0,79	0,17
	2	3	5	4,27	4,22	0,5	
	3	3	5	4	4,19	0,5	
	4	1,18	5	4	3,98	0,66	
Program¹	NÖ	1	5	4,09	4,13	0,65	0,563
	İÖ	3,09	5	4	4,21	0,5	
Günlük İnternet Kullanımı Süresi²	0-2	3	5	4,27	4,35	0,64	0,017*
	2-4	1,18	5	4	3,99	0,61	
	4-6	3	5	4,09	4,2	0,52	
	6-8	2,64	5	4	4,06	0,61	
	8+	1	5	4,55	4,32	0,78	
Gelir²	<8500	2,64	5	4	4,06	0,55	0,049*
	8500-12500	3	5	4	4,16	0,53	

	12500-16000	3	5	4,18	4,13	0,53	
	16000+	1	5	4,36	4,27	0,87	
GNO ²	0-2	3	5	4,18	4,14	0,64	0,359
	2-3	1,18	5	4	4,12	0,62	
	3-3,5	3	5	4	4,14	0,52	
	3,5-4	1	5	4,55	4,25	0,89	
Bilgisayar ¹	Yok	3	5	4	4,14	0,56	0,697
	Var	1	5	4,09	4,15	0,7	
Tablet ¹	Yok	1	5	4	4,13	0,59	0,111
	Var	1,18	5	4,45	4,25	0,83	
Telefon ¹	Yok	1	5	4	4,07	0,67	0,04*
	Var	3	5	4,18	4,28	0,52	
Sosyal Medya Kullanımı ¹	Hayır	3,09	4,64	3,27	3,57	0,72	0,074
	Evet	1	5	4,09	4,16	0,62	
Günlük sosyal medya kullanım süresi ²	0-2	3	5	4	4,09	0,61	0,014*
	2-4	1,18	5	4	3,97	0,65	
	4-6	3	5	4,09	4,26	0,5	
	6-8	3	5	4,18	4,21	0,47	
	8+	1	5	4,64	4,34	0,99	

¹ Mann Whitney U Test ² Kruskal Wallis-H Testi * $p < 0.05$

Günlük 8 saatten fazla ($\bar{x}=4,32$) internet kullanan öğrencilerin, aile geliri 16000 TL ve üstü olan öğrencilerin ($\bar{x}=4,27$), günlük 8 saat ve üzerinde sosyal medya kullanımı olan öğrencilerin ($\bar{x}=4,34$) dijital vatandaşlık düzeyi doğru kullanım alt faktör puanı, istatistiksel olarak anlamlı düzeyde yüksek bulunmuştur. Öğrencinin cinsiyeti, hangi sınıfta olduğu, hangi programda olduğu, genel not ortalaması, bilgisayar, tablet veya telefona sahip olup olmaması ve sosyal medya kullanıp kullanmaması, dijital vatandaşlık düzeyi doğru kullanım alt faktöründe istatistiksel olarak anlamlı bir farklılık oluşturmamaktadır (Tablo 6).

Tablo 6: Sosyodemografik özelliklere göre Dijital Vatandaşlık Ölçeği Çevrimiçi İşlemler alt faktörünün değerlendirilmesi

		Min.	Mak.	Ortanca	Ortalama	Standard Sapma	p
Cinsiyet ¹	Erkek	2	5	4,25	4,23	0,71	0,2
	Kadın	1	5	4	4,14	0,65	
Sınıf ²	1	2	5	4,5	4,29	0,68	0,226
	2	2,75	5	4	4,15	0,6	

	3	2,75	5	4,25	4,19	0,58	
	4	1	5	4	4,02	0,8	
Program¹	NÖ	1	5	4	4,14	0,7	0,362
	İÖ	3	5	4,25	4,28	0,46	
Günlük İnternet Kullanımı Süresi²	0-2	3	5	4	4,2	0,74	0,139
	2-4	1	5	4	4,07	0,66	
	4-6	2,75	5	4	4,19	0,6	
	6-8	1,5	5	4	4,07	0,75	
	8+	2	5	4,5	4,36	0,7	
Gelir²	<8500	1,5	5	4	4,01	0,64	0,008*
	8500-12500	2,75	5	4	4,19	0,57	
	12500-16000	3	5	4,25	4,21	0,56	
	16000+	1	5	4,5	4,33	0,85	
GNO²	0-2	3	5	4	4,09	0,58	0,04*
	2-3	1	5	4	4,11	0,68	
	3-3,5	1,5	5	4,25	4,16	0,64	
	3,5-4	2	5	4,75	4,44	0,74	
Bilgisayar¹	Yok	1,5	5	4	4,16	0,59	0,532
	Var	1	5	4,25	4,17	0,75	
Tablet¹	Yok	1,5	5	4	4,15	0,64	0,045*
	Var	1	5	4,5	4,3	0,84	
Telefon¹	Yok	3,5	5	4,37	4,36	0,43	0,198
	Var	1	5	4	4,14	0,68	
Sosyal Medya Kullanımı¹	Hayır	1,5	5	4	3,63	1,55	0,61
	Evet	1	5	4,25	4,18	0,64	
Günlük sosyal medya kullanım süresi²	0-2	1,5	5	4	4,06	0,71	0,193
	2-4	1	5	4	4,08	0,73	
	4-6	2,75	5	4,25	4,2	0,54	
	6-8	3	5	4,25	4,35	0,53	
	8+	2	5	4,75	4,28	0,9	

¹ Mann Whitney U Test ² Kruskal Wallis-H Testi * $p < 0.05$

Aile geliri 16000 TL ve üstü olan öğrencilerin ($\bar{x}=4,33$), genel not ortalaması 3,5-4 arası olan öğrencilerin ($\bar{x}=4,44$), tablete sahip olan öğrencilerin ($\bar{x}=4,30$) dijital vatandaşlık düzeyi çevrimiçi işlemler alt faktör puanı, istatistiksel olarak anlamlı düzeyde yüksek bulunmuştur. Öğrencinin cinsiyeti, hangi sınıfta olduğu, hangi programda olduğu, günlük internet kullanımı süresi, bilgisayar veya telefona sahip olup olmaması, sosyal medya kullanıp kullanmaması ve günlük sosyal medya kullanım süresi, dijital vatandaşlık düzeyi çevrimiçi işlemler alt faktöründe istatistiksel olarak anlamlı bir farklılık oluşturmamaktadır (Tablo 7).

Tablo 7: Sosyodemografik özelliklere göre DVÖ'nün Sağlık alt faktörünün değerlendirilmesi

		Min.	Mak.	Ortanca	Ortalama	Standard Sapma	p
Cinsiyet¹	Erkek	1	5	4	3,94	0,94	0,237
	Kadın	1,67	5	4	3,84	0,74	
Sınıf²	1	1	5	4	3,82	0,98	0,354
	2	1,67	5	4	3,8	0,78	
	3	2,67	5	4	4,05	0,6	
	4	1,67	5	4	3,77	0,85	
Program¹	NÖ	1	5	4	3,82	0,83	0,057
	İÖ	3	5	4	4,14	0,6	
Günlük İnternet Kullanımı Süresi²	0-2	3	5	4	4,15	0,64	0,072
	2-4	1,67	5	4	3,67	0,77	
	4-6	2	5	4	3,87	0,82	
	6-8	1,67	5	4	3,92	0,76	
	8+	1	5	4	4,09	0,89	
Gelir²	<8500	1,67	5	4	3,71	0,78	0,046*
	8500-12500	2	5	4	3,85	0,81	
	12500-16000	2	5	4	3,95	0,72	
	16000+	1	5	4	4,08	0,88	
GNO²	0-2	2	5	3,67	3,68	0,74	0,615
	2-3	2	5	4	3,91	0,77	
	3-3,5	1,67	5	4	3,86	0,84	
	3,5-4	1	5	4	3,89	0,94	
Bilgisayar¹	Yok	1,67	5	4	3,83	0,81	0,431
	Var	1	5	4	3,92	0,8	
Tablet¹	Yok	1	5	4	3,87	0,8	0,941
	Var	2,33	5	4	3,9	0,87	
Telefon¹	Yok	1	5	4	3,81	0,85	0,253
	Var	2	5	4	3,98	0,72	
Sosyal Medya Kullanımı¹	Hayır	1,67	3,33	2,83	2,67	0,82	0,01*
	Evet	1	5	4	3,9	0,79	
Günlük sosyal medya kullanım süresi²	0-2	1,67	5	4	3,81	0,84	0,018*
	2-4	1,67	5	3,83	3,63	0,84	
	4-6	2,33	5	4	3,93	0,71	
	6-8	3	5	4	4,17	0,59	
	8+	1	5	4,33	4,11	1,05	

¹ Mann Whitney U Test ² Kruskal Wallis-H Testi *p<0.05

Aile geliri 16000 TL ve üstü olan öğrencilerin ($\bar{x}$ =4,08), sosyal medya kullanan öğrencilerin ($\bar{x}$ =3,90), günlük 4 saat ve üzeri sosyal medya kullanımı olan öğrencilerin

(sırayla; 4-6 saat için $\bar{x}=3,93$, 6-8 saat için $\bar{x}=4,17$, 8 saat ve üzeri için $\bar{x}=4,11$) dijital vatandaşlık düzeyi sağlık alt faktör puanı, istatistiksel olarak anlamlı düzeyde yüksek bulunmuştur. Öğrencinin cinsiyeti, hangi sınıfta olduğu, hangi programda olduğu, günlük internet kullanımı süresi, genel not ortalaması, bilgisayar, tablet veya telefona sahip olup olmaması, dijital vatandaşlık düzeyi sağlık alt faktöründe istatistiksel olarak anlamlı bir farklılık oluşturmamaktadır (Tablo 8).

Tablo 8: Sosyodemografik özelliklere göre DVÖ'nin Erişim alt faktörünün değerlendirilmesi

		Min.	Mak.	Ortanca	Ortalama	Standard Sapma	p
Cinsiyet¹	Erkek	1	5	4,17	4,22	0,78	0,087
	Kadın	1,33	5	4	4,08	0,66	
Sınıf²	1	1	5	4,33	4,19	0,84	0,337
	2	1,33	5	4	4,19	0,7	
	3	2,33	5	4	4,11	0,59	
	4	2	5	4	4,03	0,69	
Program¹	NÖ	1	5	4	4,12	0,74	0,675
	İÖ	3	5	4	4,15	0,53	
Günlük İnternet Kullanımı Süresi²	0-2	3	5	4,33	4,18	0,69	0,096
	2-4	2	5	4	3,96	0,7	
	4-6	2,33	5	4	4,22	0,56	
	6-8	3	5	4	4,14	0,63	
	8+	1	5	4,5	4,2	0,97	
Gelir²	<8500	1,33	5	4	4,02	0,68	0,033*
	8500-12500	2,67	5	4	4,1	0,64	
	12500-16000	2,33	5	4	4,15	0,64	
	16000+	1	5	4,67	4,3	0,84	
GNO²	0-2	2,33	5	4	4,07	0,73	0,355
	2-3	1,33	5	4	4,08	0,7	
	3-3,5	2,33	5	4	4,17	0,62	
	3,5-4	1	5	4,67	4,27	0,93	
Bilgisayar¹	Yok	1,33	5	4	4,1	0,68	0,442
	Var	1	5	4	4,16	0,74	
Tablet¹	Yok	1	5	4	4,09	0,7	0,019*
	Var	2,67	5	4,67	4,38	0,67	
Telefon¹	Yok	1	5	4	4,04	0,74	0,011*
	Var	2,33	5	4,17	4,29	0,61	
Sosyal Medya	Hayır	3,67	4	4	3,92	0,17	0,283

Kullanımı¹	Evet	1	5	4	4,13	0,71	
	0-2	1,33	5	4	3,99	0,78	
Günlük sosyal medya kullanım süresi²	2-4	2,33	5	4	4,04	0,69	
	4-6	2,33	5	4	4,2	0,56	0,103
	6-8	3	5	4	4,26	0,57	
	8+	1	5	4,67	4,28	1,1	

Aile geliri 16000 TL ve üstü olan öğrencilerin ($\bar{x}=4,30$) ve tablete sahip olan öğrencilerin ($\bar{x}=4,38$) dijital vatandaşlık düzeyi erişim alt faktör puanı, istatistiksel olarak anlamlı düzeyde yüksek bulunmuştur. Öğrencinin cinsiyeti, hangi sınıfta olduğu, hangi programda olduğu, günlük internet kullanımı süresi, genel not ortalaması, bilgisayar veya telefona sahip olup olmaması, sosyal medya kullanıp kullanmaması ve günlük sosyal medya kullanım süresi, dijital vatandaşlık düzeyi erişim alt faktöründe istatistiksel olarak anlamlı bir farklılık oluşturmamaktadır (Tablo 9).

Tablo 9: Sosyodemografik özelliklere göre DVÖ'nin Toplumsal Sorumluluk alt faktörünün değerlendirilmesi

		Min.	Mak.	Ortanca	Ortalama	Standard Sapma	p
Cinsiyet¹	Erkek	1	5	4	3,86	0,97	0,022*
	Kadın	1	5	3,75	3,57	0,86	
Sınıf²	1	1	5	3,5	3,64	1,03	0,045*
	2	1,5	5	3,5	3,45	0,92	
	3	2	5	4	3,9	0,76	
	4	2	5	3,75	3,59	0,88	
Program¹	NÖ	1	5	3,5	3,6	0,93	0,028*
	İÖ	2,5	5	4	3,97	0,73	
Günlük İnternet Kullanımı Süresi²	0-2	2	5	4	3,91	1,11	0,078
	2-4	1	5	3,5	3,46	0,87	
	4-6	2	5	4	3,78	0,8	
	6-8	1,5	5	3,5	3,53	0,9	
	8+	1	5	4	3,83	1,04	
	<8500	1	5	3,5	3,54	0,88	
Gelir²	8500-12500	2	5	4	3,66	0,92	0,228
	12500-16000	1,5	5	3,75	3,65	0,79	
	16000+	1	5	4	3,86	1	
GNO²	0-2	1	5	3,5	3,55	1,1	0,873
	2-3	1,5	5	4	3,65	0,9	
	3-3,5	2	5	4	3,73	0,86	
	3,5-4	1	5	3,5	3,6	0,95	
Bilgisayar¹	Yok	1,5	5	4	3,61	0,91	0,362
	Var	1	5	4	3,72	0,9	
Tablet¹	Yok	1	5	4	3,62	0,89	0,044*
	Var	2	5	4	3,98	0,92	
Telefon¹	Yok	1	5	4	3,59	0,92	0,114
	Var	1	5	4	3,79	0,87	
Sosyal Medya Kullanımı¹	Hayır	2	5	2,5	3	1,41	0,189
	Evet	1	5	4	3,68	0,89	
Günlük sosyal medya kullanım süresi²	0-2	2	5	4	3,64	0,99	0,124
	2-4	1	5	3,5	3,47	0,88	
	4-6	2	5	4	3,74	0,77	
	6-8	1,5	5	4	3,69	0,91	
	8+	1	5	4,5	4,03	1,11	

¹ Mann Whitney U Test ² Kruskal Wallis-H Testi *p<0.05

Erkek öğrencilerin ($\bar{x}=3,86$), 3. sınıfta okuyan öğrencilerin ($\bar{x}=3,90$) ve ikinci öğretimde okuyan öğrencilerin ($\bar{x}=3,97$) dijital vatandaşlık düzeyi toplumsal sorumluluk alt faktörü ortalama puanı, istatistiksel olarak anlamlı düzeyde yüksek bulunmuştur. Öğrencinin günlük internet kullanımı süresi, ailesinin gelir düzeyi, genel not ortalaması, bilgisayar, tablet veya telefona sahip olup olmaması, sosyal medya kullanıp kullanmaması ve günlük sosyal medya kullanım süresi, dijital vatandaşlık düzeyi toplumsal sorumluluk alt faktöründe istatistiksel olarak anlamlı bir farklılık oluşturmamaktadır (Tablo 10).

Tablo 10: DVGFÖ'nin ile DVÖ ve alt boyutları arasındaki korelasyonun değerlendirilmesi

Ölçek Boyut	İstatistik	DVGF	DV	Doğru Kullanım	Çevrimiçi İşlemler	Sağlık	Erişim
DVGF	r	1					
	p	.					
DV	r	0,738	1				
	p	<0,001	.				
Doğru Kullanım	r	0,697	0,932	1			
	p	<0,001	<0,001	.			
Çevrimiçi İşlemler	r	0,616	0,84	0,775	1		
	p	<0,001	<0,001	<0,001	.		
Sağlık	r	0,613	0,783	0,651	0,532	1	
	p	<0,001	<0,001	<0,001	<0,001	.	
Erişim	r	0,607	0,83	0,711	0,715	0,57	1
	p	<0,001	<0,001	<0,001	<0,001	<0,001	.
Toplumsal Sorumluluk	r	0,515	0,549	0,366	0,342	0,592	0,438
	p	<0,001	<0,001	<0,001	<0,001	<0,001	<0,001

r: Spearman Rho Korelasyon Analizi

**p<0.05*

Dijital veri güvenliği farkındalığı ile dijital vatandaşlık düzeyi arasında pozitif yönlü, yüksek düzeyde ve istatistiksel olarak anlamlı ilişki bulunmaktadır (%73,8, $p<0.001$) (Tablo 10).

Dijital veri güvenliği farkındalığı ile dijital vatandaşlık düzeyinin alt faktörlerinden doğru kullanım (%69,7), çevrimiçi işlemler (%61,6), sağlık (%61,3), erişim (%60,7) ve toplumsal sorumluluk (%51,5) arasında pozitif yönlü, orta düzeyde ve istatistiksel olarak anlamlı ilişki bulunmaktadır.

Dijital vatandaşlık düzeyi ile doğru kullanım alt faktörü arasında çok yüksek düzeyde (%93,2), çevrimiçi işlemler (%84,0), sağlık (%78,3) ve erişim (%83,0) alt faktörü arasında yüksek düzeyde, toplumsal sorumluluk (%54,9) alt faktörü arasında ise orta düzeyde anlamlı ilişki bulunmaktadır.

Doğru kullanım ile çevrimiçi işlemler (%77,5) ve erişim (%71,1) arasında yüksek düzeyde, sağlık (%65,1) ile orta düzeyde, toplumsal sorumluluk (%36,6) ile zayıf düzeyde anlamlı ilişki bulunmaktadır.

Çevrimiçi işlemler ile sağlık (%53,2) arasında orta düzeyde, erişim (%71,5) arasında yüksek düzeyde, toplumsal sorumluluk (%34,2) arasında zayıf düzeyde anlamlı ilişki bulunmaktadır.

Sağlık alt faktörü ile erişim (%57,0) ve toplumsal sorumluluk (%59,2) arasında orta düzeyde anlamlı ilişki bulunmaktadır. Sağlık alt faktörü ile toplumsal sorumluluk alt faktörü arasında pozitif yönlü, orta düzeyde ve istatistiksel olarak anlamlı ilişki bulunmaktadır (%59,2, $p<0.001$).

Erişim alt faktörü ile toplumsal sorumluluk arasında zayıf düzeyde anlamlı ilişki bulunmaktadır (%43,8, $p<0.001$).

5. TARTIŞMA

Bu bölümde, araştırmaya katılan ve Sivas Cumhuriyet Üniversitesi SBF Sağlık Yönetimi Bölümde öğrenim gören (N=271) öğrenciye ait bulgular ve öğrencilerin dijital vatandaşlık ve dijital veri güvenliği farkındalığı düzeyleri ile bu iki kavram arasındaki ilişkiler literatür ışığında tartışılacaktır. Çalışmaya katılan öğrencilerin (%68,3)'ünü kadınların, (%30,3)'ünü 3. Sınıf öğrencilerinin, (%83,3)'ünü normal öğretim öğrencilerinin oluşturduğu ve yarıya yakınının (%47,1) not ortalamasının 2.00-3.00 arasında olduğu saptanmıştır. Öğrencilerin (%32,1)'inin ailelerinin aylık gelir düzeyi 8500 TL'den daha azdır. (Araştırma yapıldığı tarihte asgari ücret 8500 TL'ydi) Öğrencilerin (%47,50)'sinin bilgisayarı, (%13,60)'ının tableti, (%90,50)'sinin akıllı telefona vardır. Öğrencilerin %33,9'u günde 6 saat ve üzerinde internet kullanırken, tamamına yakını (%98,20) sosyal medya kullanmaktadır. (Tablo 1).

Çalışmadan elde edilen bulgulara göre, dijital veri güvenliği farkındalığı ile dijital vatandaşlık düzeyi arasında pozitif yönlü, yüksek düzeyde ve istatistiksel olarak anlamlı bir ilişki mevcuttur. (%73.8, $p<0.001$) Benzer bir bulgu, Hızmalı'nın (2022) üniversite öğrencileri üzerinde yaptığı çalışmada da ortaya çıkmıştır. ($r=0,759$, $p<0,05$) Ancak, dijital vatandaşlık ve veri güvenliğini birlikte ele alan başka ulusal ya da uluslararası çalışmanın bulunmaması, bu alandaki literatürün sınırlı olduğunu ortaya koymaktadır. Bu durum, çalışmamızın önemini ve özgünlüğünü artırmaktadır, çünkü dijital vatandaşlık ve veri güvenliği arasındaki ilişkinin derinlemesine incelenmesi, dijital dünya ile etkileşimde olan bireylerin daha bilinçli ve güvenli bir şekilde hareket etmelerini sağlayacak önemli bilgiler sunmaktadır. Bu nedenle, gelecekte yapılacak araştırmaların bu iki kavramı birlikte ele alarak, dijital veri güvenliği farkındalığını ve dijital vatandaşlık düzeyini artırmaya yönelik stratejiler geliştirmesi gerekmektedir.

Çalışma bulgularına göre, katılımcıların genelinde dijital vatandaşlık ortalamasının ($\bar{x}$:4,06) olduğu tespit edilmiştir. Bu sonuçlar, öğretmen adayı öğrencilerin dijital vatandaşlık düzeyini inceleyen Cender ve Doğu'nun çalışması ile Sakallı ve Çiftçi'nin ($\bar{x}$:118,93) çalışmasıyla benzerlik göstermektedir.

Sağlık yönetimi bölümü öğrencilerinin ölçek alt boyutlarına yönelik ortalamalarını değerlendirdiğimizde, çevrimiçi işlemler ($\bar{x}$:4,1659) alt boyutunun en yüksek ortalamaya sahip olduğu belirlenmiştir. Bu ortalamayı sırasıyla doğru kullanım, ($\bar{x}$:4,1455) erişim ($\bar{x}$:4,1288) sağlık ($\bar{x}$:3,8727) ve toplumsal sorumluluk ($\bar{x}$:3,6636) alt boyutları takip etmektedir. Çevrimiçi işlemler alt boyutunun en yüksek orana sahip olmasının temel sebepleri, tüketicilerin hızlı erişim, geniş ürün seçenekleri, çeşitli kampanyalar ve güvenli ödeme seçenekleri gibi avantajlardan dolayı çevrimiçi alışverişi tercih etmeleri olarak düşünülmektedir. Ayrıca, zaman ve nakit tasarrufu sağlayan dijital platformlar sayesinde insanlar, bankacılık, e-devlet gibi resmi işlemlerini de internet üzerinden hızlı, kolay ve güvenli bir şekilde gerçekleştirmektedirler. Bu bağlamda 2023 yılında gerçekleştirilen TÜİK hane halkı bilişim teknolojileri kullanım araştırmasına göre bireylerin %73,9'u E-devlet platformunu kullanmaktadır. Ayrıca bireylerin internet üzerinden mal veya hizmet satın alma ya da sipariş verme oranı %49,5 olarak tespit edilmiştir. Seçil Som Vural'ın çalışmasının sonucunda ise üniversite öğrencilerinin yanıtlarının erişim faktöründe en yüksek değerde ($\bar{x}$ =4,356) olduğu ve bunu sırasıyla doğru kullanım ($\bar{x}$ =4,315), çevrimiçi işlemler ($\bar{x}$ =3,985), sağlık ($\bar{x}$ =3,633) ve toplumsal sorumluluk ($\bar{x}$ =3,443) faktörlerinin izlediği belirlenmiştir. Seçil Som Vural'ın dijital vatandaşlık konusundaki çalışmasıyla kendi araştırma sonuçlarımız arasındaki temel farklılıkları değerlendirdiğimizde, bu farklılıkların altında birkaç önemli faktör bulunabilir. İlk olarak, öğrencilerin dijital vatandaşlık alt boyutlarına olan yaklaşımları arasındaki bu ayrım, teknolojik gelişmelerin hızına bağlı olarak dijital vatandaşlık davranışlarını etkilemiş olabilir. Ayrıca, Seçil Som Vural'ın çalışmasında vurgulanan dijital vatandaşlık boyutlarının sıralamasındaki farklılıklar, öğrenci profilleri, öğrenim görülen bölüm veya dijital beceri düzeyleri gibi faktörlere dayanabilir.

Çalışma kapsamında sağlık yönetimi öğrencilerinin dijital vatandaşlık düzeylerine dair yapılan analizde, cinsiyet faktörü açısından anlamlı bir farklılık tespit edilmemiştir. (p :0,133) Bu sonuçlar, erkek ve kadın öğrenciler arasında dijital vatandaşlık becerileri konusunda önemli bir ayrım olmadığını göstermektedir. Dolayısıyla, dijital vatandaşlık eğitimi veya benzeri programların bu öğrenci grubu için cinsiyet temelinde özel bir odaklanma gerektirmediği sonucuna varılabilir. Benzer şekilde, sosyal bilgiler öğretmen adayı öğrencilerinin dijital vatandaşlık algılarını

inceleyen akmak ve Aslan'ın alışmasında cinsiyet deęiřkeni ile dijital vatandaşlık arasında anlamlı bir fark saptanmamıştır.

Arařtırma sonuçlarına göre, öğrencilerin sınıf düzeyleri ile dijital vatandaşlık ortalamaları arasında istatistiksel olarak anlamlı bir fark tespit edilmemiřtir. (p: 0,342) Bu durum, farklı sınıf düzeylerindeki öğrencilerin dijital vatandaşlık konusundaki performanslarının benzer olduęunu göstermektedir. Ancak, sınıf düzeyinin yükselmesiyle birlikte, öğrencilerin dijital vatandaşlık becerilerinin de artması gerektięi düşünölmektedir. Bu bulgu, eğitimcilerin dijital vatandaşlık konusunda özel eğitim programları geliştirme ve uygulama ihtiyacını vurgulamaktadır. Ayrıca, olak ve Öztürk'ün (2022) sosyal bilgiler öğretmen adayları öğrencilerinin dijital vatandaşlık düzeylerini deęerlendiren bir alışmasında, sınıf düzeyi ile dijital vatandaşlık düzeyi arasında anlamlı farklılıklar ortaya konmuřtur. Lyons (2012)' da öğrencilerle yaptıęı alışmada sınıf düzeyi arttıka kişisel güvenlik ve dijital vatandaşlık davranışlarının arttığını belirlemiřtir. Bu farklılıęın, öğrenim görölen kurumdaki eğitim programları, eğitimci yaklaşımları veya altyapı farklılıkları gibi etkenlerden kaynaklanabileceęi düşünölmektedir. Bu bağlamda, gelecekteki alışmalarda bu faktörlerin daha detaylı bir şekilde incelenmesi, benzer alışmalar arasındaki farklılıkları anlamamıza katkı sağlayabilir.

Günlük internet kullanım süresi ile dijital vatandaşlık düzeyi arasında istatistiksel olarak anlamlı bir farklılık belirlenmiřtir. (p: 0,017) Özellikle, 8 saat ve üzeri internet kullanan öğrencilerin dijital vatandaşlık düzeyi ortalamaları ($\bar{x}$: 4,24), 2-4 ($\bar{x}$: 3,91), 4-6 ($\bar{x}$: 4,12), 6-8 ($\bar{x}$: 4,00) saat internet kullanan öğrencilere kıyasla daha yüksek bulunmuřtur. Öğrencilerin günlük internet kullanım süresi ile dijital vatandaşlık düzeyi arasındaki bu anlamlı farklılık, dijital dünyada daha fazla etkileşimde bulunan öğrencilerin dijital vatandaşlık konusundaki bilin ve beceri düzeylerinin daha yüksek olduęunu işaret edebilir. Bu bulgu, dijital vatandaşlık eğitimine odaklanırken günlük internet kullanım süresinin göz önünde bulundurulmasının önemini vurgulamaktadır. İlgili literatür incelendięinde sonuçlar öğretmen adaylarıyla gerekleştirilen Cender ve Doęu ve Sakallı ve ifti'nin alışmalarıyla uyumlu bir sonuç göstermektedir.

Ailenin gelir düzeyi ile dijital vatandaşlık düzeyi arasında anlamlı bir ilişki olduğu belirlenmiştir (p: 0,008). Özellikle, ailenin gelir düzeyinin 16.000 ve üzeri olan katılımcılar, dijital vatandaşlık düzeyleri açısından en yüksek grupta yer almaktadır. Bu bulgu, daha yüksek gelir düzeyine sahip ailelerin bireylerinin dijital vatandaşlık konusundaki bilinç ve beceri düzeylerinin diğer gruplara göre daha üst düzeyde olduğunu göstermektedir. Bu durum, gelir düzeyinin dijital vatandaşlık eğitimi ve farkındalığı üzerinde etkili olabileceğini düşündürmektedir. Aslan ve Çakmak'ın (2018) sosyal bilgiler öğretmen adaylarının dijital vatandaşlık davranışlarının bazı değişkenler açısından incelediği çalışmasında da benzer sonuçlara rastlanmıştır.

Ayrıca, genel not ortalamasının dijital vatandaşlık düzeyi açısından istatistiksel olarak anlamlı bir fark oluşturmadığı tespit edilmiştir (p: 0,315). Bu bulgu, öğrencilerin akademik başarılarının dijital vatandaşlık becerileri üzerinde doğrudan bir etkisi olmadığını göstermektedir.

Çalışmamızda, tablet ($\bar{x}$: 4,21) sahibi olan katılımcıların dijital vatandaşlık düzeyi, tablet sahibi olmayanlara ($\bar{x}$: 4,05) göre istatistiksel olarak anlamlı düzeyde yüksek bulunmuştur. Bu durum, tablet kullanımının dijital vatandaşlık becerilerini artırabileceğini düşündürmektedir. Sonuç olarak, dijital cihaz sahipliğinin dijital vatandaşlık düzeyine etkisinin cihaz türüne göre farklılık gösterdiği ve özellikle tablet kullanımının dijital vatandaşlık becerilerini artırma konusunda önemli bir rol oynayabileceği gözlemlenmektedir. Yılmaz ve Doğusoy'un öğretmen adaylarıyla gerçekleştirdiği çalışmasında ise dijital vatandaşlık düzeyinin bilgisayar sahibi olma açısından anlamlı bir şekilde farklılaştığı görülmektedir. Bulguların farklı olmasının nedeni, teknoloji ve dijital cihaz kullanımının sürekli değişim göstermesi olarak düşünülmektedir.

Çalışmanın sonuçlarına göre, sosyal medya kullanımı ile dijital vatandaşlık düzeyi arasında istatistiksel olarak anlamlı bir farklılık saptanmamıştır (p: 0,016). Bu durum, sosyal medya kullanımının dijital vatandaşlık becerileri üzerinde doğrudan bir etki yaratmadığını gösterebilir.

Günlük sosyal medya kullanım süresi ile dijital vatandaşlık düzeyi arasındaki istatistiksel anlamlılık incelendiğinde, özellikle günde 8 saat ve üzeri sosyal medya kullanan bireylerin dijital vatandaşlık düzeylerinin diğer gruplara göre istatistiksel

olarak daha yüksek bulunduđu ortaya çıkmıştır ($\bar{x}$: 4,27) Bu durum, uzun süreli sosyal medya kullanımının dijital vatandaşlık becerilerini olumlu bir şekilde etkileyebileceğine işaret edebilir. Bu bağlamda, sosyal medya platformlarının günlük yaşantımızda giderek daha fazla yer kaplaması ve bireylerin çevrimiçi etkileşimlerinin artması, dijital vatandaşlık becerilerinin gelişiminde önemli bir faktör olabilir.

Çalışmamızda günlük internet kullanım süresi ile dijital vatandaşlık düzeyinin "doğru kullanım" ve "çevrimiçi işlemler" alt faktörleri arasında istatistiksel olarak anlamlı farklılıklar olduğu belirlenmiştir. Özellikle, günde 8 saat ve üzeri internet kullanan katılımcıların bu alt faktörlerde en yüksek puanları aldığı gözlemlenmiştir: "doğru kullanım ($\bar{x}$: 4,32), çevrimiçi işlemler ($\bar{x}$:4,36)". Bu durum, uzun süreli internet kullanımının, doğru kullanım ve çevrimiçi işlemler konusundaki dijital vatandaşlık becerilerini olumlu yönde etkileyebileceğini düşündürmektedir. Günde 8 saat ve üzeri internet kullanan bireylerin, dijital ortamda etkili bir şekilde işlem yapma ve doğru kullanma konularındaki deneyimlerinin daha gelişmiş olduğu söylenebilir. Ancak, "sağlık" alt boyutuna odaklandığımızda, günlük 0-2 saat ($\bar{x}$: 4,15). Bu durum, daha düşük internet kullanım sürelerinin, dijital sağlık konularında daha yüksek bir bilinç düzeyine işaret edebilir.

Araştırmamızdaki dijital vatandaşlık düzeyi ile doğru kullanım alt faktörü arasında çok yüksek düzeyde (%93.2), çevrimiçi işlemler (%84.0), sağlık (%78.3) ve erişim (%83.0) alt faktörü arasında yüksek düzeyde, toplumsal sorumluluk (%54.9) alt faktörü arasında ise orta düzeyde anlamlı ilişki bulunduğu saptanmıştır. Bu bulgular, bireylerin dijital vatandaşlık düzeyleri ile çevrimiçi işlemler, sağlık, erişim, doğru kullanım ve toplumsal sorumluluk gibi dijital vatandaşlık alt faktörleri arasında güçlü bir bağlantı olduğunu ortaya koymaktadır. Özellikle doğru kullanım alt faktörü ile olan çok yüksek düzeydeki ilişki, bireylerin dijital platformlarda etik ve bilinçli davranışlarını vurgulamaktadır. Bu tür ilişkilerin anlaşılması, dijital vatandaşlık eğitimi programlarının ve dijital sağlık yönergelerinin geliştirilmesinde rehberlik edebilir.

Çalışmanın sonuçlarına göre sağlık yönetimi bölümü öğrencilerinin dijital veri güvenliği ortalamaları ($\bar{x}$: 3,9) olarak tespit edilmiştir. Bıkmaz'ın (2017) sağlık yönetimi bölümü öğrencileri ile yaptığı çalışmada ise öğrencilerin dijital veri güvenliği

ortalamları ($\bar{x}=4,10$) bulunmuştur. Öncelikle, öğrenciler sağlık sektöründe çalışacakları için sağlık verilerini koruma sorumluluğuna sahiptirler. Verilerin güvenliğini sağlamak, hasta mahremiyeti ve etik standartlara uygunluğun önemli bir unsuru olduğundan, öğrencilerin dijital veri güvenliği konusunda yüksek bir bilinç düzeyine sahip olmaları oldukça önemlidir. Bu nedenle, öğrencilerin dijital veri güvenliği konusundaki farkındalıklarını artırmak amacıyla eğitim programlarında bu konuya daha fazla yer verilmesi, öğrencilerin mesleki sorumluluklarını yerine getirmelerine yardımcı olacaktır.

Çalışmamızda erkek öğrencilerin ($\bar{x}$: 4,08) dijital veri güvenliği farkındalığı, kadın öğrencilerden ($\bar{x}$: 3,93) istatistiksel olarak anlamlı düzeyde yüksek bulunmuştur. Bu bulgu, cinsiyetler arasında dijital güvenlik farkındalığı konusunda önemli bir eşitsizliği ortaya koymaktadır. Bu nedenle, kadın öğrencilerin dijital güvenlik farkındalığını artırmak amacıyla özel eğitim programları ve farkındalık kampanyaları düzenlenmelidir. Bu programlar, kadın öğrencilerin dijital dünyada karşılaştıkları spesifik risklere odaklanarak onların dijital güvenlik ve mahremiyet konularında daha bilinçli ve donanımlı olmalarını sağlamayı hedeflemelidir.

Sınıflar arasında dijital veri güvenliği farkındalığı açısından istatistiksel olarak anlamlı bir farklılık bulunmamaktadır (p : 0,326). Bu sonuçlar, dijital veri güvenliği farkındalığının sınıf düzeyine göre daha özelleştirilmiş eğitimlerle artırılabileceğini düşündürmektedir. Sınıf kademelerine uygun eğitim stratejileri, öğrencilerin dijital güvenlik konusundaki bilinç düzeyini artırabilir ve onları çevrimiçi ortamlarda daha güvenli ve bilinçli kılabilir. Eğitimciler, öğrencilerin ihtiyaçlarına ve gelişim düzeylerine uygun içeriklerle, dijital güvenliği daha anlamlı ve etkili bir şekilde öğretebilirler.

Günlük internet kullanımı süresi, dijital veri güvenliği farkındalığı açısından istatistiksel olarak anlamlı bir farklılık oluşturmaktadır (p : 0,021). Günlük 8 saat ve üzerinde internet kullanımı olan katılımcıların ($\bar{x}$: 4,09), dijital veri güvenliği farkındalığı, 2-4 saat ($\bar{x}$: 3,88) ve 4-6 saat ($\bar{x}$: 3,99) arasında internet kullanımı olan katılımcılardan istatistiksel olarak anlamlı düzeyde yüksek bulunmuştur. Günlük internet kullanım süresi ile dijital veri güvenliği farkındalığı arasındaki bu istatistiksel ilişki, dijital güvenlik eğitimlerinin kişilerin internet kullanım alışkanlıklarını dikkate

olarak planlanması gerektiğini vurgular. Bu durum, özellikle uzun süre internet kullanan bireylerin dijital güvenlik riskleri konusunda daha fazla bilinçlendirilmesine katkıda bulunabilir. Araştırma, internet kullanımının artmasıyla birlikte dijital güvenlik konusundaki farkındalığın arttığını göstermekle birlikte, bu ilişkinin nedenlerini daha derinlemesine anlamak için gelecekteki çalışmalara da yol gösterici olabilir. Bu tür çalışmalar, dijital veri güvenliği eğitimlerinin etkili bir şekilde tasarlanması için yol gösterici olabilir.

Ailenin gelir düzeyi, dijital veri güvenliği farkındalığı açısından istatistiksel olarak anlamlı bir farklılık oluşturmaktadır ($p:0,005$). Farklılığın tespiti için yapılan ikili karşılaştırmalar sonucunda; 16000 lira ve üstü aile geliri olan katılımcıların ($\bar{x}=4,15$), dijital veri güvenliği farkındalığı, 8500 lira (araştırma yapıldığı tarihte asgari ücret 8500 TL'ydi) altında aile geliri olan katılımcılardan ($\bar{x}=3,83$) istatistiksel olarak anlamlı düzeyde yüksek bulunmuştur. Ailenin gelir düzeyi ile dijital veri güvenliği farkındalığı arasındaki bu istatistiksel ilişki, ekonomik durumun bireylerin dijital güvenlik konusundaki bilinç düzeylerini etkileyebileceğini gösterebilir. Bu durum, dijital güvenlik eğitim ve farkındalık programlarının sadece teknik yönleri değil, aynı zamanda ekonomik koşulları da göz önünde bulundurması gerektiğini gösterir. Araştırma, düşük gelirli ailelerden gelen bireylerin dijital güvenlik konusundaki farkındalığını artırmak için özel stratejilere ihtiyaç olduğunu vurgular. Eğitimciler ve dijital güvenlik uzmanları, bu stratejileri tasarlamak için sosyal ve ekonomik bağlamı dikkate almalıdır (Hızmalı 2022).

Genel not ortalaması, dijital veri güvenliği farkındalığı açısından istatistiksel olarak anlamlı bir farklılık oluşturmamaktadır ($p:0,363$). Bu durum, genel akademik başarı ile dijital güvenlik bilinci arasında belirgin bir bağlantı olmadığını göstermektedir.

Bilgisayar ($\bar{x}:4,05$) ve tablete ($\bar{x}:4,17$) sahip olan öğrencilerin dijital veri güvenliği farkındalığı ortalamaları anlamlı düzeyde yüksek bulunurken, akıllı telefona sahip olma durumu, dijital veri güvenliği farkındalığı açısından istatistiksel olarak anlamlı bir farklılık oluşturmamaktadır ($\bar{x}:3,95$). Bilgisayar ve tablete sahip olan öğrencilerin daha yüksek farkındalığa sahip olması, muhtemelen bu cihazların daha geniş bir kullanım yelpazesi ve çeşitli dijital aktivitelerin gerçekleştirilmesi için

kullanılmasından kaynaklanabilir. Diğer yandan, telefon sahipliği ile dijital veri güvenliği farkındalığı arasındaki istatistiksel olarak anlamlı farklılık bulunmamış olması dikkat çekicidir. Bu durum, telefonların daha yaygın ve kişisel kullanıma yönelik olmasından kaynaklanabilir. Sosyal medya kullanımı, dijital veri güvenliği farkındalığı açısından istatistiksel olarak anlamlı bir farklılık oluşturmamaktadır (p:0,125). Korkmaz 'ın (2018) farklı bölümlerdeki öğrencilere uyguladığı çalışmada da benzer sonuçlara ulaşılmıştır.

Araştırmamızda, günlük sosyal medya kullanım süresi ile dijital veri güvenliği farkındalığı arasında anlamlı bir ilişki olduğu saptanmıştır. (p:0,019). Talan ve Aktürk'ün (2021) ortaöğretim öğrencileri üzerinde gerçekleştirdiği çalışmada, sosyal medya kullanım süresinin öğrencilerin veri güvenliği farkındalık düzeylerinde belirgin bir fark yaratmadığı tespit edilmiştir. Bu iki bulgu arasındaki ayrımın, örneklemelerin farklılığından kaynaklanabileceği düşünülmektedir. Ayrıca üniversite öğrencileri ile ortaöğretim öğrencileri arasındaki demografik farklılıklar, yaşam deneyimleri ve dijital teknoloji kullanım alışkanlıkları, dijital veri güvenliği farkındalığının algılanışını şekillendirebilir.

Dijital veri güvenliği farkındalığı ile dijital vatandaşlık düzeyinin alt faktörlerinden doğru kullanım (%69.7), çevrimiçi işlemler (%61.6), sağlık (%61.3), erişim (%60.7) ve toplumsal sorumluluk (%51.5) arasında pozitif yönlü, orta düzeyde ve istatistiksel olarak anlamlı ilişki bulunmaktadır. Yani, bireylerin dijital veri güvenliği konusundaki bilinci arttıkça, çevrimiçi ortamlarda doğru kullanım, sağlıklı dijital alışkanlıklar, eşit erişim ve toplumsal sorumluluk gibi unsurlarda da artış gözlemlenmektedir. Bu tür bir ilişkinin anlaşılması, dijital vatandaşlık eğitimi ve dijital güvenlik farkındalık programlarının tasarlanması ve uygulanması için önemlidir. Bu programlar, bireylere dijital dünyada güvenli, etik ve sorumlu davranışlar sergileme konusunda rehberlik edebilir ve bu şekilde daha sağlıklı dijital bir toplum oluşturabilir.

6.SONUÇ ve ÖNERİLER

6.1 Sonuçlar

Bu çalışma Sivas Cumhuriyet Üniversitesi SBF Sağlık Yönetimi Bölümü'nde öğrenim gören öğrencilerin dijital vatandaşlık ve dijital veri güvenliği farkındalıkları ve bu iki kavram arasındaki ilişkinin incelenmesi amacıyla yapılmıştır. Bu bölümde elde edilen bilgiler doğrultusunda ulaşılan sonuçlara yer verilmiştir.

- ✓ Bu bağlamda, öğrencilerin büyük bir çoğunluğunu %68,30'luk oranla kadın öğrenciler oluşturmaktadır. Ayrıca, öğrencilerin %30'u 3. sınıf öğrencisi olarak belirlenmiştir. Öğrencilerin büyük bir kısmı, %83,30'luk oranla normal öğretimde yer alırken, günlük internet kullanım alışkanlıkları da dikkat çekicidir. %33'lük bir kesim, günde 4-6 saat arasında internet kullanırken, %17,20'si bu süreyi 8 saatten fazla olarak belirtmiştir. Genel not ortalamasının %47,10 ile 2-3 arasında olması, öğrencilerin akademik performanslarına yönelik bir gösterge sunmaktadır.
- ✓ Korelasyon analizi sonucunda dijital veri güvenliği farkındalığı ile dijital vatandaşlık düzeyi arasında pozitif yönlü, yüksek düzeyde ve istatistiksel olarak anlamlı ilişki bulunmaktadır (%73.8, $p<0.001$).
- ✓ Öğrencilerin dijital bağlamdaki alışkanlıkları incelendiğinde, %90,50'lik bir oranla öğrencilerin akıllı telefona sahip olduğu görülmektedir. Öğrencilerin %98,20'si sosyal medya platformlarını aktif kullanmaktadır ve %29,90'ını sosyal medyada günlük 4-6 saat geçirmektedir. Öğrencilerin dijital veri güvenliği farkındalığı ($\bar{x}=3,9$) olarak tespit edilirken, dijital vatandaşlık ortalamaları ($\bar{x}=4,06$) olarak bulunmuştur. Dijital vatandaşlık ölçeğinin alt boyutları arasından doğru kullanım, çevrimiçi işlemler ve erişim boyutu ($\bar{x}:4,1$) olarak tespit edilmiştir. Sağlık faktörü ($\bar{x}=3,08$) bulunurken, toplumsal sorumluluk alt faktörü ortalaması ise ($\bar{x}=3,06$) ile en düşük düzeydedir.
- ✓ Erkek öğrencilerin ($\bar{x}=4,08$) dijital veri güvenliği farkındalığı, kadın öğrencilere göre ($\bar{x}=3,93$) yüksek bulunmuştur. 0-2 saat arasında internet kullanan öğrencilerin dijital veri güvenliği farkındalıkları ($\bar{x}=4,26$) ile en yüksek ortalamaya sahipken

günde 8 saat ve üzeri internet kullanan öğrencilerin dijital veri güvenliği farkındalığı ortalamaları ($\bar{x}=4,09$) olarak bulunmuştur. 16.000 lira ve üstü ile en yüksek düzeyde aile geliri olan katılımcıların ($\bar{x}=4,15$), dijital veri güvenliği farkındalığı, 8.500 lira altında aile geliri olan öğrencilerden ($\bar{x}=3,83$) yüksek bulunmuştur. Günlük 8 saat ve üzerinde sosyal medya kullanımı olan öğrencilerin ($\bar{x}=4,14$) dijital veri güvenliği farkındalığı en yüksek düzeyde tespit edilmiştir.

- ✓ Cinsiyetler arasında dijital vatandaşlık düzeyi açısından istatistiksel olarak anlamlı bir farklılık bulunmamaktadır. Günde 0-2 saat ve 8 saat üzeri internet kullanan öğrencilerin dijital vatandaşlık ortalamaları $\bar{x}=4,24$ ile en yüksek düzeydedir. Aile geliri 16.000 ve üzeri olan katılımcıların dijital vatandaşlık ortalamaları ($\bar{x}=4,22$) ile en yüksek düzeydedir. Günlük 8 saat ve üzerinde sosyal medya kullanımı olan katılımcıların dijital vatandaşlık düzeyi ($\bar{x}=4,27$) ile en yüksek düzeyde tespit edilmiştir.
- ✓ Dijital veri güvenliği farkındalığı ile dijital vatandaşlık düzeyinin alt faktörlerinden doğru kullanım (%69.7), çevrimiçi işlemler (%61.6), sağlık (%61.3), erişim (%60.7) ve toplumsal sorumluluk (%51.5) arasında pozitif yönlü, orta düzeyde ve istatistiksel olarak anlamlı ilişki bulunmaktadır.
- ✓ Dijital vatandaşlık düzeyi ile doğru kullanım alt faktörü arasında çok yüksek düzeyde (%93,2), çevrimiçi işlemler (%84,0), sağlık (%78.3) ve erişim (%83.0) alt faktörü arasında yüksek düzeyde, toplumsal sorumluluk (%54.9) alt faktörü arasında ise orta düzeyde anlamlı ilişki bulunmaktadır.

6.2. Öneriler

Çalışmamızda, dijital vatandaşlık ölçeği alt boyutlarından sağlık ($\bar{x}:3,8727$) ve toplumsal sorumluluk ($\bar{x}:3,6636$) faktörlerinin diğer faktörlere göre daha düşük seviyede olduğu belirlenmiştir. Bu bulgu, bu alanlarda farkındalık artırıcı müdahalelerin gerekli olduğunu göstermektedir.

Kadın öğrencilerin dijital vatandaşlık düzeyleri ($\bar{x}=3,93$) ve dijital veri güvenliği farkındalıkları ($\bar{x} = 4,04$) ortalama ile, erkek öğrencilere göre düşük seviyede tespit

edilmiştir Kadınların dijital vatandaşlık ve veri güvenliği farkındalıklarının düşük olması, cinsiyete dayalı eşitsizliklerin dijital ortamlarda da sürdüğünü göstermektedir. Bu nedenle, kadınlara yönelik özel eğitim ve destek programları oluşturularak dijital okuryazarlık ve güvenlik farkındalığı artırılabilir.

İkinci sınıf öğrencilerinin dijital vatandaşlık puanları ($\bar{x}$:3,88) ortalama ile en düşük seviyede iken, dördüncü sınıf öğrencilerinin dijital veri güvenliği farkındalıkları ($\bar{x}$:3,93) ortalama ile en düşük tespit edilmiştir. Bu durum, öğrencilerin eğitim seviyelerine göre dijital becerilerinde ve farkındalıklarında beklenen gelişimin sağlanamadığını göstermektedir. Bu nedenle, dijital vatandaşlık ve veri güvenliği konularında daha erken sınıflarda başlanarak daha etkili ve kapsamlı bir eğitim programının uygulanması, öğrencilerin bu alanlardaki bilgi ve farkındalık düzeylerini artırmak için önemli bir gereklilik olarak öne çıkmaktadır

Aile geliri 8500 (araştırma yapıldığı tarihte asgari ücret 8500 TL'ydi) lira ve altı olan grupların dijital vatandaşlık düzeyleri ($\bar{x}$:3,83) ortalama ile en düşük seviyede tespit edilirken, dijital veri güvenliği farkındalıkları ($\bar{x}$: 3,96) olarak belirlenmiştir. Aile geliri düşük olan grupların dijital vatandaşlık ve veri güvenliği farkındalıklarının düşük olması, ekonomik faktörlerin dijital dünyaya erişimde ve etkin kullanımda engel oluşturduğunu ortaya koymaktadır. Bu nedenle, düşük gelirli ailelerin çocuklarına yönelik dijital araç ve eğitim materyallerinin ücretsiz veya uygun fiyatlı temin edilmesi, bu grupların dijital dünyada daha etkin olmalarını sağlayabilir.

Normal öğretim öğrencilerinin dijital vatandaşlık puanları ($\bar{x}$ =3,96) ve dijital veri güvenliği farkındalıkları ($\bar{x}$ =4,05) ortalama ile ikinci öğretim öğrencilerine göre düşük seviyede tespit edilmiştir. Bu bulgu normal öğretim programında öğrenim gören öğrencilerin dijital dünyada etkin bir şekilde yer alabilmeleri için daha fazla desteğe ihtiyaç duyduklarını göstermektedir. Bu durum, dijital vatandaşlık ve veri güvenliği konularında daha kapsamlı ve uygulamalı eğitim programlarının gerekliliğini ortaya koymaktadır. Öğrencilerin dijital becerilerini geliştirmek, onların hem akademik başarılarına hem de gelecekteki mesleki yeterliliklerine önemli katkılar sağlayacaktır.

Öğrencilerin %98,20'sinin sosyal medya platformlarını aktif kullanması ve %33'ünün internette günlük 4-6 saat geçirmesi, internet bağımlılığı açısından ciddi bir soruna işaret etmektedir. Bu durumla mücadele etmek için dijital detoks programları düzenlenebilir, eğitim seminerleriyle farkındalık artırılabilir ve alternatif hobiler teşvik edilebilir. Ayrıca bu çalışma, internet bağımlılığı konusundaki mevcut durumu ortaya koyarken, gelecekte yapılacak araştırmalara da ışık tutabilir. Bu nedenle, internet bağımlılığı üzerine yapılacak daha kapsamlı ve uzun vadeli araştırmalar, literatüre önemli katkılar sağlayacaktır.

Çalışmamızda elde edilen bulgular, dijital vatandaşlık ve dijital veri güvenliği konularının sağlık yönetimi alanında birlikte ele alınmasının önemini ortaya koymaktadır. İlgili literatür incelendiğinde, dijital vatandaşlık üzerine yapılan çalışmaların genellikle öğretmenler ve öğretmen adayları gibi belirli gruplarla sınırlı olduğu, dolayısıyla sağlık yönetimi bağlamında bu konulara yönelik araştırma eksikliği olduğu görülmüştür. Ayrıca, uluslararası düzeyde dijital sağlık alanında çeşitli çalışmalar mevcut olmakla birlikte, dijital vatandaşlık ve dijital veri güvenliğini bir arada inceleyen çalışmalara rastlanmamaktadır. Mert Hızmalı'nın (2022) üniversite öğrencileri üzerine gerçekleştirdiği araştırma, dijital vatandaşlık ve dijital veri güvenliği konularını birlikte ele almaktadır ancak bu çalışma sağlık yönetimi alanına yönelik değildir. Bu bağlamda, sağlık yönetimi alanında dijital vatandaşlık ve dijital veri güvenliğini bütüncül bir şekilde ele alan araştırmalara ihtiyaç duyulmaktadır.

KAYNAKÇA

- AB. (2023). AB Genel Veri Koruma Tüzüğü (GDPR) Türkçeye çevrildi.
- AFAD. (2021). Afad acil mobil uygulama projesi.
- Aksakallı, İ. K. (2019). Bulut bilişimde güvenlik zafiyetleri, tehditleri ve bu tehditlere yönelik güvenlik önerileri. *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi*, 5(1), 8-34.
- Al Muhammadi, S., Al Saleh, M. (2017). Information security maturity model for nıst cyber security framework. *Computer Science Information Technology*, 7(3), 51-62.
- Alkali, Y. E., Amichai-Hamburger, Y. (2004). Experiments in digital literacy. *CyberPsychology & Behavior*, 7(4), 421-429.
- Ananthanarayan, S., Siek, K. A. (2012). *Persuasive Wearable Technology Design for Health and Wellness*. 6th International Conference on Pervasive Computing Technologies for Healthcare (PervasiveHealth) and Workshops, USA. 236-240.
- Arslan, B., Gündüz, M. S., Ve Sağıroğlu, Şeref. (2015). *Güncel mobil tehditler ve alınması gereken önlemler* (Konferans Bildirisi). International Symposium On Digital Forensics And Security, Ankara.
- Arslan, E. T., Demir, H. (2017). Üniversite öğrencilerinin mobil sağlık ve kişisel sağlık kaydı yönetimine ilişkin görüşleri. *Aksaray Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*, 9 (2), 17-36
- Aslan, S., ve Çakmak, Z. (2018). Sosyal bilgiler öğretmen adaylarının dijital vatandaşlık davranışlarının bazı değişkenler açısından incelenmesi. *Adıyaman University Journal of Educational Sciences*, 8(1), 72-99.
- Aslay, F. (2017). Siber saldırı yöntemleri ve Türkiye'nin siber güvenlik mevcut durum analizi. *International Journal Of Multidisciplinary Studies And Innovative Technologies*, 1(1), 24-28.
- Aydın, A. (2015). Dijital vatandaşlık. *Türk Kütüphaneciliği*, 29(1), 142-146.

- Bacanak, A., Karamustafaoğlu, O., Köse, S. (2003). Yeni Bir Bakış: Eğitimde Teknoloji Okuryazarlığı. *Pamukkale Üniversitesi Eğitim Fakültesi Dergisi*, 14(14), 191-196.
- Bayrak, T. (2017). Sosyal Medyada Dijital Etik: Twitter’da Şiddet İçerikli İletilerin İncelenmesi. *Yeni Medya Elektronik Dergisi*, 1(1), 32-46.
- Bernstein. (2021). Techtargget, what is digital health (digital healthcare) and why is it important
- Bıkmaz, Z. (2017). Sağlık yönetimi bölümü öğrencilerinin mobil güvenlik farkındalığı ve dijital veri güvenliği farkındalıklarının belirlenmesi. *Uluslararası Yönetim Bilişim Sistemleri ve Bilgisayar Bilimleri Dergisi*, 1(1), 22-30.
- Bilgi Teknolojileri ve İletişim Kurumu. (2017). Genel bilgi.
- Canbek, G., Sağıroğlu, Ş. (2006). Bilgisayar Sistemlerine Yapılan Saldırıları ve Türleri: Bir İnceleme. *Erciyes Üniversitesi Fen Bilimleri Enstitüsü Fen Bilimleri Dergisi*, 23(1), 1-12.
- Carda, K. B., (2022). Dijital dünya için dijital etik.
- CDC. (2023). Health Insurance Portability and Accountability Act of 1996 (HIPAA).
- Cender, G., ve Doğu, B. (2021). Öğretmen Adaylarının Dijital Vatandaşlık Düzeyleri. *Uluslararası Sosyal Bilgiler Eğitimi Dergisi*, 3(1), 1-23.
- Cernerhealth. (2024).
- Çiftçi, S. Sakallı, H. (2016). Sınıf öğretmen adaylarının dijital vatandaşlık düzeyi ile siber zorbalık koşulları arasındaki ilişkinin incelenmesi. *Eğitim teknolojisi kuramı ve uygulaması*, 6 (2), 100-119.
- Çolak, A., ve Öztürk, T. (2022). Sosyal bilgiler öğretmen adaylarının dijital vatandaşlık düzeylerinin çeşitli değişkenler açısından incelenmesi. *Uluslararası Sosyal Bilgilerde Yeni Yaklaşımlar Dergisi*, 6(2), 367-394.
- Çubukçu, A., Bayzan, Ş. (2013). Türkiye’de dijital vatandaşlık algısı ve bu algıyı internetin bilinçli, güvenli ve etkin kullanımı ile artırma yöntemleri. *Middle Eastern; African Journal Of Educational Research*, 5(1), 148-174.

- Damrongsak, M. Ve Brown, Kc (2008). Data security in occupational health. *Aaohn Dergisi*, 56 (10), 417-421.
- Demirdöğmez, M., Gültekin, N., ve Taş, H. Y. (2018). Türkiye’de e-ticaret sektörünün yıllara göre gelişimi. *Opus International Journal Of Society Researches*, 8(15), 2216-2236.
- Demirel, M. (2009,). *Yaşam boyu öğrenme ve teknoloji* (Konferans Bildirisi). In 9th International Educational Technology Conference. Ankara, Turkey.
- Doğantimur, F. (2009). Iso 27001 standardı çerçevesinde kurumsal bilgi güvenliği (Mesleki Yeterlilik Tezi). T.C. Maliye Bakanlığı Strateji Geliştirme Başkanlığı, Ankara.
- Duran, E., ve Özen, N. E. (2018). Türkçe Derslerinde Dijital Okuryazarlık. *Türkiye Eğitim Dergisi*, 3(2), 31-46.
- Durmaz, Ş. (2005). Bilişim suçlarının sosyolojik analizi. Gazi Üniversitesi Sosyal Bilimler Enstitüsü Kamu Yönetim Ana Bilim Dalı (Yüksek Lisans Tezi). 25-26, Ankara.
- Elmalı, F. (2020). Sosyal ağ siteleri: ergenler, riskler ve tehditlerden korunma stratejileri. *Abant İzzet Baysal Üniversitesi Eğitim Fakültesi Dergisi*, 20(1), 439-453.
- EPİC. (2024).
- Erturgut, M. (2003). Elektronik imza kanunu bakımından e-belge ve e-imza. *Bankacılar Dergisi*, 48, 66-79.
- Esenler Belediyesi. (2016). Hayat Kurtaran Kolye.
- Fingal, D. (2022). Infographic: Im a digital citizen.
- Fussell, R. S. (2005). *Protecting information security availability via self-adapting intelligent agents*. In MILCOM 2005-2005 IEEE Military Communications Conference 2977-2982.
- Gkioulos, V., Wangen, G., Katsikas, S. K., Kavallieratos, G., Kotzanikolaou, P. (2017). Security awareness of the digital natives. *Information*, 8(2), 42.

- Goodfellow, R. (2011). Literacy, Literacies and The Digital in Higher Education. *Teaching in Higher Education*, 16(1), 131-144.
- Henkoğlu, T., ve Yılmaz, B. (2013). Avrupa Birliği AB bilgi güvenliği politikaları. *Türk Kütüphaneciliği*, 27(3), 451-471.
- Hızmalı, M. (2022). *Üniversite öğrencilerinin dijital veri güvenliği farkındalıklarının dijital vatandaşlık bağlamında incelenmesi* (Yüksek Lisans Tezi). Trakya Üniversitesi Fen Bilimleri Enstitüsü, Edirne.
- İBM. (2024). Embark on a digital reinvention.
- İleri, Y. Y., ve Uludağ, A. (2017). E-Nabiz uygulamasının yönetim bilişim sistemleri ve hasta mahremiyeti açısından değerlendirilmesi. *Uluslararası Sağlık Yönetimi ve Stratejileri Araştırma Dergisi*, 3(3), 318-325.
- İşman, A., ve Güngören, C., (2014). Digital citizenship. *Turkish Online Journal of Educational Technology-TOJET*, 13(1), 73-77.
- İTS. (2024). Proje Tanımı.
- Kale, H. (2014). Kamu 'da Sosyal Politika. Mehmet Emin Esen (Ed). Bilişim toplumuna özgü bir suç tipi: bilişim suçları içinde (s.51-52). Ankara.
- Kandur, H. (2011). Türkiye’de kamu kurumlarında elektronik belge yönetimi: mevcut durum analizi ve farkındalığın artırılması çalışmaları. *Bilgi Dünyası*, 12(1), 2-12.
- Karaaslan, İ. A., Önür, N., Çoban, B. Pandemi Döneminde Sosyal Medya Kullanıcılarının Dijital Veri Güvenliğine Yönelik Farkındalıklarının Araştırılması. *The Journal of International Scientific Researches*, 8(2), 165-182.
- Karaduman, H. (2011). *6. Sınıf sosyal bilgiler dersinde dijital vatandaşlığa dayalı etkinliklerin öğrencilerin dijital ortamdaki tutumlarına etkisi ve öğrenme öğretme sürecine yansımaları* (Doktora Tezi). İstanbul.
- Karahisar. (2014). İnternette çocukları bekleyen riskler ve medya okuryazarlığı. *The Turkish Online Journal Of Design, Art And Communication*, 4(4), 82-95.
- Karakuş Yılmaz, T., (2020). Dijital Haklar ve Sorumluluklar. *Dijital Okuryazarlık: Araçlar, Metodolojiler, Uygulamalar ve Öneriler* (ss.127-180), Ankara: Nobel.

- Kaya, Ö. F., Öztürk, E. (2017). Veri ve ağ güvenliği için uygulama ve analiz çalışmaları. *İstanbul Ticaret Üniversitesi Fen Bilimleri Dergisi*, 16(31), 85-102.
- Korkmaz, E. V. (2018). Üniversite öğrencilerinin internet ve veri güvenliği farkındalıkları. *International Journal Of Social And Humanities Sciences Research (Jshsr)*, 5(25), 2222-2229.
- Korucu, O. (2021). *Veri Güvenliğinin İyileştirilmesi Sürecinde Risk Tabanlı Küresel Standart, Çerçeve ve En İyi Uygulama Yaklaşımları* (Yüksek Lisans Tezi). İstanbul Bilgi Üniversitesi, İstanbul.
- KVKK. (2010). Anayasal Bir Hak Olarak Kişisel Verilerin Korunmasını İsteme Hakkı, 1-5.
- Levi, A. (2003). Nasıl Bir E-Posta Güvenliği? Bilişim Güvenlik, Sabancı Üniversitesi. Mühendislik ve Doğa Bilimleri Fakültesi. 38-40.
- Lyons, R. (2012). Investigating student gender and grade level differences in digital citizenship behavior. Unpublished Doctoral Dissertation. Walden University, USA.
- McCumber, J. (2005). Assessing and managing security risk in IT systems. Washington: CRC.
- Mercimek, B., Dulkadir Yaman, N., Kelek, A., Odabaşı, H. F. (2015). Dijital dünyanın yeni gerçeği: troller. *Trakya Üniversitesi Eğitim Fakültesi Dergisi*, 6(1), 67-77.
- Mercuri, R. T. (2004). The HIPAA-potamus in health care data security. *Communications of the ACM*, 47(7), 25-28.
- MHRS. (2021). Hakkımızda. Erişim Adresi: mhhs.gov.tr/hakkimizda.html (Erişim Tarihi: 21 Aralık 2023)
- Mossberger, K., Tolbert, C. J., ve Hamilton, A. (2012). Measuring digital citizenship: mobile access and broadband. *International Journal Of Communication*, 6, 2492–2528.
- Nalbant, F. (2014). *Türkiye’de vatandaşlık anlayışının gelişimi*. III. Türkiye Lisansüstü Çalışmaları Kongresi. Sakarya.

- Näsman, Y., ve Nyholm, L. (2021). The movement of virtue from ethos to action. *Nursing Philosophy*, 22(2), e12339.
- NİST. (2023). An Introduction to the Components of the Framework.
- Ocak, M. A., (2013). Aile ve İnternet. Mehmet Akif Ocak (Ed.) Ministry of Family and Social Policies, Hangar Brand Communication and Advertising Services.
- Özcan, N. (2021). Dijital etik üzerine nitel bir araştırma. *Gençlik Araştırmaları Dergisi*, 9(25), 89–108.
- Özerbaş, M. A., Kuralbayeva, A. (2008). Türkiye ve Kazakistan öğretmen adaylarının dijital okuryazarlık düzeylerinin değerlendirilmesi. *Muğla Sıtkı Koçman Üniversitesi Eğitim Fakültesi Dergisi*, 5(1), 16–25.
- Ribble, M. (2023). Nine elements of digital citizenship. Digital citizenship: Using technology appropriately.
- Ribble, M., ve Bailey, G. (2004). Digital citizenship. Learning and Leading with Technology, 3(2), 12-15.
- Ribble, M., ve Bailey, G. (2007). The nine elements of digital citizenship International Society for Technology in Education. Digital Citizenship in schools, 13-37.
- Sağlık Bakanlığı Dijital Hastane. (2014). EHR-ESK. Erişim Adresi: dijitalhastane.saglik.gov.tr (Erişim Tarihi: 4 Ağustos 2024).
- Sağlık Bakanlığı. (2015). Tele Sağlık Hizmetleri.
- Sağlık Bakanlığı. (2024). Teleradyoloji Sistemi.
- Sakallı, H. (2015). *Sınıf öğretmeni adaylarının dijital vatandaşlık düzeyleri ile siber zorbalık eğilimleri arasındaki ilişkinin incelenmesi* (Yüksek Lisans Tezi). Adnan Menderes Üniversitesi Sosyal Bilimler Enstitüsü, Aydın.
- Sarı, İ., ve Taşer, S. (2018). Türkiye’de dijital vatandaşlıkla ilgili yapılan yüksek lisans ve doktora tezlerinin incelenmesi. *Anemon Muş Alparslan Üniversitesi Sosyal Bilimler Dergisi*, 6(6), 1063-1069.
- Schneier, B. (2000). Secrets and lies: digital security in a networked world. Wiley.
- Schugurensky, D. (2005). Citizenship and citizenship education.

- SGEP. (2017). Portal Hakkında. Erişim Adresi: siberakademi.bilgem.tubitak.gov.tr. (Erişim Tarihi: 23 Aralık2023).
- Shephard, B. 2002. Information security-who cares. Power System Management and Control, Fifth International Conference on (Conf. Publ. No. 488), 126s.
- Solutions, K. F. (2008). Healthcare information and management systems society (himss) analytics report: Security of patient data. HIMSS Analytics. U.S.
- Stevenson, N. (2010). Cultural citizenship, education and democracy: redefiningthe good society. *Citizenship Studies*, 14(3), 275–291.
- Subrahmanyam, K., ve Greenfield, P. (2008). Online communication and adolescent relationships. *The future of children*, 18(1), 119-146.
- Şenel, A., Gençoğlu, S. (2003). Küreselleşen dünyada teknoloji eğitimi. *Üniversitesi Endüstriyel Sanatlar Eğitim Fakültesi Dergisi*, 11(12), 45–65.
- T.C Sağlık Bakanlığı. (2023). E-nabız kullanım kılavuzu.
- T.C Ulaştırma ve Altyapı Bakanlığı. (2020-2023). Ulusal Siber Güvenlik Stratejisi, 5-95.
- T.C. Çevre, Şehircilik ve İklim Değişikliği Bakanlığı. (2024). Uzaktan Hasta Takibi Uygulaması. Erişim Adresi: akillisehirler.gov.tr (Erişim Tarihi 5 Ağustos 2024).
- Talan, T., ve Aktürk, C. (2021). Orta öğretim öğrencilerinin dijital okuryazarlık ve bilgi güvenliği farkındalığı seviyelerinin incelenmesi. *Kahramanmaraş Sütçü İmam Üniversitesi Sosyal Bilimler Dergisi*, 18(1), 158-180.
- Tan, B., Merey, Z. (2021). Ortaokul öğrencilerinin internet kullanımına ilişkin görüşlerinin dijital vatandaşlık kapsamında incelenmesi. *Journal Of Yüzüncü Yıl University, Faculty Of Education*, 18(1). 162-193.
- Tekerek, M. (2008). Bilgi güvenliği yönetimi. *Ksü Doğa Bilimleri Dergisi*, 11(1), 132-137.
- TSE (2023). Bilgi Güvenliği Yönetim Sistemi (BGYS) Belgelendirmesi.
- Tüik. (2023). Hanehalkı bilişim teknolojileri (bt) kullanım araştırması.
- Türkiye Sağlık Vakfı. (2023). Giyilebilir Sağlık Teknolojisi

Usom. (2023). Usom hakkında.

Uysal, B., Ulusinan, E. (2020). Güncel dijital sağlık uygulamalarının incelenmesi. *Selçuk Sağlık Dergisi*, 1(1), 46-60.

Varol, Ş., Orhan, F., Tuncer, S., Akyüz, S. (2016). Sağlık kurumlarında bilgi güvenliği bağlamında biyometrik sistemler. *Sağlık Akademisyenleri Dergisi*, 3(4), 155-162.

Veradigm. (2024). Who we are.

Vural, S.S., ve Kurt, A. (2018). Üniversite öğrencilerinin bakış açısıyla dijital vatandaşlık göstergelerinin incelenmesi. *Eğitim Teknolojisi Kuram ve Uygulama*, 8(1), 60-80.

Wagner, A. E. ve Brooke, C. (2007). Wasting time: the mission impossible with respect to technologyoriented security approaches electronic. *Journal Of Business Research Methods*, 5(2), 117- 124.

Yarwood, R. (2016). Citizenship. An Introduction To Human Geography, 5th Edition, 456-469. Plymouth, İngiltere.

Yıldızbaşı, E., Öztaş, D., Sanisoğlu, Y., Fırat, H., Yalçın, N., Şeker, E. D., Akçay, M. (2016). Bir Eğitim ve Araştırma Hastanesinde Merkezi Hekim Randevu Sistemini Kullanan Hastaların Memnuniyet Düzeylerinin Ölçülmesi. *Ankara Medical Journal*, 16(3), 293-302.

Yılmaz, E. (2015). *Öğretmenlerin dijital veri güvenliği farkındalığı* (Doktora Tezi). Anadolu Üniversitesi, Eskişehir.

Yılmaz, M. (2019). *Öğretmen adaylarının dijital vatandaşlık düzeylerinin belirlenmesi: Mersin Üniversitesi Eğitim Fakültesi örneği* (Yüksek Lisans Tezi). Mersin Üniversitesi Eğitim Bilimleri Enstitüsü, Mersin.

Yılmaz, M., Doğusoy, B. (2020). Öğretmen adaylarının dijital vatandaşlık düzeylerinin belirlenmesi. *Kastamonu Eğitim Dergisi*, 28(6), 2362–2375.