TÜBAD TÜRKİYE BİLİMSEL ARAŞTIRMALAR DERGİSİ Uluslararası Hakemli Dergi | TURKISH SCIENTIFIC RESEARCHES JOURNAL TUSREJ ISSN : 2602-4632

TÜBAD Cilt VI, Sayı II, Aralık, 2021

Çevrimiçi Mahremiyet Farkındalık Ölçeğinin Geliştirilmesi: Güvenirlik ve Geçerlilik Çalışması

Özgen KORKMAZ[1]
Mehmet VERGİLİ[2]
Emel KARADAŞ[3]

Gönderim Tarihi: 08.06.2021 Yayın Tarihi: 31.12.2021

Öz

Çevrimiçi mahremiyet, günümüzde hızla gelişen teknolojilerle internet kullanımının artması ve buna bağlı olarak sürekli etkileşim, çevrimiçi olma durumlarıyla bağlantılı olarak oluşabilecek güvenlik açısından önemli bir kavramdır. Bu çalışmanın amacı geçerlik ve güvenirlik analizleri yapılarak Çevrimiçi Mahremiyet Farkındalık Ölçeği (ÇMFÖ) geliştirmektir. Araştırma kapsamında betimsel tarama modelinden yararlanılmıştır. Araştırmanın çalışma grubunu Amasya Üniversitesinin farklı bölümlerinde eğitim gören 514 üniversite öğrencisi oluşturmaktadır. Oluşturulan ölçeğin deneme formu 49 maddeden oluşmaktadır. Ölçeğin geçerliliğine yönelik madde faktör korelasyonları, açımlayıcı faktör analizi (AFA), doğrulayıcı faktör analizi (DFA), madde ayırt edicilik güçleri hesaplanmıştır. Güvenirliğe yönelik iç tutarlık ve kararlılık düzeyleri incelenmiştir. Yapılan bu analizler sonucunda 5'li likert tipinde 17 madde ve 3 faktörden meydana gelen ÇMFÖ oluşmuştur. Üç faktör toplam varyansın %47.709'unu açıklamaktadır. Ölçeğin tamamının güvenirlik katsayısı (Cronbach α) .794 olarak hesaplanmıştır. Elde edilen analiz sonuçları, oluşturulan ölçeğin güvenilir ve geçerli olduğunu destekler özelliktedir.

Anahtar Kelimeler: Farkındalık, Çevrimiçi Mahremiyet, Ölçek Geliştirme

Developing Online Privacy Awareness Scale: Reliability and Validity Study

Abstract

The aim of this study is to develop an Online Privacy Awareness Scale (OPAS) using validity and reliability analyzes. Within the scope of the research, descriptive survey model was utilized. The study group consists of 514 students studying at different departments of Amasya University. The first version of the scale is consisted of 49 items. For the validity of the scale, exploratory factor analysis, confirmatory factor analysis, item factor correlations, and item distinctiveness analyses were calculated. Internal consistency and stability levels in terms of reliability were examined. As a result of these studies, OPAS is a 5-point Likert-type scale consisting of 17 items and 3 factors. Three factors explain 47.709% of the total variance. The whole scale was calculated as Cronbach α = .794. It can be said that the results of the analysis provided support the validity and reliability of the scale.

Key Words: Awareness, Online Privacy, Scale Development

[1] Sorumlu Yazar : Özgen Korkmaz Prof.Dr, Amasya Üniversitesi, Türkiye, ozgenkorkmaz@gmail.com, ORCID : 0000-0003-4359-5692
[2] Mehmet Vergili, Milli Eğitim Bakanlığı, Türkiye, vergilimehmet@gmail.com, ORCID : 0000-0002-7221-5815
[3] Emel Karadaş, Amasya Üniversitesi, Türkiye, tongelemel@gmail.com, ORCID: 0000-0002-8478-6228

Giriş

21.yüzyılda hızla gelişen teknoloji ile birlikte insanlar bilgiye hızlı bir şekilde ulaşmakta ve farklı ortamlarda paylaşmaktadır (Taşdelen ve Çataldaş, 2017; Hazar, 2018). 2016 yılı itibariyle dünyada 3,4 milyara yakın bireyin internet kullanıcısı olduğu ve 2,3 milyarının sosyal ağlarda hesaba sahip olduğu ifade edilmektedir (Kalaman, 2017). İnternet her geçen gün büyümekte ve kullanıcılarına farklı seçenekler sunarak vazgeçilmez bir teknoloji haline gelmektedir (Mıhçı ve Çakmak, 2017). Mıhçı ve Çakmak (2017), çocuklar ve gençlerde bu durumun daha belirgin olduğunu ifade etmektedirler. Gelişen teknolojilerin geniş kitlelerce kullanımının insanoğlunun yaşamına faydalı birçok etkisinin olmasının yanı sıra, insan yaşamında birtakım sorunlara da neden olduğu görülmektedir (Genç, Kazez ve Fidan, 2013; Acılar, Olgun ve Görür, 2015). Günümüzde alışveriş, bankacılık, iletişim, kamusal faaliyetler gibi pek çok hizmetin dijital ortamlara taşınması, bireylerin bu ortamlara erişimini arttırmıştır (Kalaman, 2017). Bireyin kendini özgür hissettiği bu ortamların, sınırsız paylaşımlar yapmasını ve bilgilerini sorgulamadan paylaşmasını normalleştirdiği belirtilmektedir (Kalaman, 2017). Gençler ve çocuklar gelişen teknolojinin getirileri ile karşı karşıyadır (Çetinkaya, Güldüren ve Keser, 2016). Bu teknolojiler sayesinde bireyler, çevrimiçi ortamlara bağlanmakla birlikte mahremiyete yönelik tehlikelere açık hale gelebilir (Debatin, Lovejay, Horn ve Hughes, 2009; Çetinkaya, Güldüren ve Keser, 2016). Günümüzde hızla yaşanan teknolojik gelişmeler yaşamımızın bir parçası haline gelmiş, sürekli çevrimiçi ulaşılabilir olma durumu mahremiyet problemini ortaya çıkarmıştır. Bunlar birtakım ihlallere (özel hayat, özgür olma vb.) neden olabilmektedir (Karslıoğlu, 2014).

Mahremiyet kavramı bireylerin kişisel verilerinin değer kazanmasıyla son yıllarda önemini arttırmıştır (Furnell ve Phippen, 2012). Mahremiyet kavramının, toplum içinde zamanın etkisiyle değişim gösterdiği ifade edilmektedir (Acılar, Olgun ve Görür, 2015; Aslanyürek, 2016). Aslanyürek (2016), mahremiyet kavramını "gizli olması ve gizli kalması gereken şey" olarak ifade etmiştir. Kara (2013)'ya göre gizlilik kavramı, dijital verilere ve bilgi teknolojileriyle ilgili sistemlere yalnızca yetkiye sahip kişi veya kuruluşların giriş yapabildiği, gizli bilgi ve verilerin yetkisi bulunmayan kişi/kuruluşlarca ele geçirilememesi durumunu ifade eder. Mahremiyet kavramı, kişinin kendi yaşamı ve hayatına ilişkin bilgileri, başka kişilerle ne kadarını ne şekilde paylaşacağını sınırlama hakkına sahip olduğunu ifade eder (Yüksel, 2003). Mahremiyetin, son yıllarda internetin hızla gelişmesiyle dikkat çeken bir konu olması ve bireylerin gizliliğinin korunmasına ilişkin endişeler ortaya çıkardığı ifade edilmektedir (Caudill ve Murphy, 2000). Kalaman (2017), ticari şirketlerin veya devletlerin değişik yollarla hali hazırda mahremiyet ihlalleri yapabildiğini, internetin bireylerin yaşamına girmesiyle bu mahremiyet ihlallerinin nicelik ve nitelik olarak da etkilendiğini belirtmiştir. Zaman ve mekân kavramlarını değişime uğratan internet, mahremiyetin sınırlarını etkilemiş ve mahremiyetin korunmasını zorlaştırmaya başlamıştır (Kalaman, 2017). Aslanyürek (2016), gelişen teknolojiyle birlikte internet kullanımının arttığını, devletlerin, bilgisayar korsanlarının ve pazarlama şirketlerinin yaptığı gizlilik ihlallerini vurgulayarak güvenlik konusunda sorgulama yapılması gerektiğini belirtmiştir. Çevrimiçi mahremiyetin, günümüzde internet kullanıcılarının en büyük tedirginlik yaşadığı konulardan biri olduğunu ifade etmişlerdir (Acılar, Olgun ve Görür, 2015).

Çevrimiçi mahremiyet kavramı, internette bilgi toplamak, görüş bildirmek vb. amaçlarla bağlanan kişilerin bu süreçte bilgilerinin korunması için alınabilecek tedbirler olarak ifade edilmektedir (Strauss ve Rogerson, 2002; Wu, Lau, Atkin ve Lin, 2011). Bu bağlamda Strauss ve Rogerson (2002)

bilgiyi, bireyin kişisel bilgilerini; adı, adresi, ailevi bilgileri, kimlik numarası vb. olarak ifade etmektedirler. Bireyin kimlik, telefon numarası gibi bilgileri dijital ortamlarda büyük veri tabanlarına kaydedilmektedir (Kalaman, 2017). Aslanyürek (2016), çevrimiçi mahremiyet kavramını "internet üzerinde bilinçli veya bilinçsiz olarak paylaşılan kişiye özel bilgilerin gizliliği ve güvenlik seviyesi ile ilgili bir kavram" olarak ifade etmektedir. Çevrimiçi mahremiyet kavramı düşünüldüğünde, bireylerin şahsi verilerine diğer kişilerin erişimi için seçenekler sunmaları ve bu bilgileri başkalarının elde edemeyeceği biçimde kontrol etme olanakları olması gerekmektedir (Milne, Rohm ve Bahl, 2004). 2,5 milyardan fazla etkin kullanıcıya sahip olan internet ortamında devletlerin, servis sağlayıcıların, korsanların ve şirketlerin şahsi bilgileri toplaması birçok ihlale yol açmaktadır (Aslanyürek, 2016). Aslanyürek (2016), gelişen teknolojiyle aynı hızda ilerleyen internet kullanımının gittikçe artması ve mahremiyet alanında yapılan ihlallerin, bu ortamın güvenilir olma hakikatini yeniden düşünmemizi sağladığını ifade etmektedir. Karaarslan, Eren ve Koç (2014), bireylerin internete bağlandıkları andan itibaren çevrimiçi ortamlarda takip edildiklerini ifade etmektedirler. Bununla ilgili alınan tedbirlere rağmen yapılan işlemlerin izlenebileceği ve gizliliğin ihlal edilebileceğini ifade etmektedirler (Karaarslan, Eren ve Koç, 2014). Bununla birlikte verileri gizlemede artan zorluklar, bireylerin zamanla bu konuyu düşünmemelerine, bıkkınlık hissetmelerine ve çevrimiçi kimliklerini korumada zorlanmalarına sebep olmaktadır (Taddicken, 2014; Choi, Park ve Jung, 2018).

Bireylerin dijital ortamlarda bağımsız olduklarını düşünerek çoğu zaman mahremiyetlerinin bozulduğu konusunda kaygılanmadıkları veya bozulduğunun farkında olamadıkları ifade edilmektedir (Kalaman, 2017). Bireylerin çevrimiçi ortamlarda karşılaştıkları çerezlerin ilerleyen yaşamlarına nasıl tesir edeceği ve karşılarına neler çıkaracağı konusunda farkındalıklarının düşük olduğu ifade edilmektedir (Topbaş ve Gazi, 2016). Bireylerin teknoloji temelli tedbirler almasını sağlamak ve insan olgusunu da göz önünde bulundurarak bilgi güvenliği farkındalığı kazandırmak risklerin azalmasında oldukça önemlidir (Çetinkaya, Güldüren ve Keser, 2017). Mahremiyet alanında ortaya çıkabilecek tehditlerden bir diğeri de bireyin kendi kendine bilgilerini yaymasıdır (Yüksel, 2003). Bireyler çevrimiçi mahremiyetlerinden kaygı duymalarına rağmen, çevrimiçi ortamlardaki profillerinde kişisel bilgilerini ifşa ettikleri ifade edilmektedir (Jordaan ve Heerden, 2017). İnternetin güvenli kullanımı için alınacak önlemler arasında öğrencilerin farkındalıklarını artırmak ve bunlara yönelik ölçme aracı geliştirmek olduğu ifade edilmektedir (Mıhçı ve Çakmak, 2017). Farkındalık kavramını insanlar günlük hayatta sıklıkla kullanmaktadır (Yılmaz, 2015). Farkındalık kavramı Türk Dil Kurumunca "farkında olma/ görülmesi veya bilinmesi gereken şeylerden haberi bulunmak, kavranması gereken bir şeye dikkat etmek" şeklinde tanımlanmaktadır (TDK, 2019). Okur ve Yalçın-Özdilek (2013), bireyin farkındalığı olduğu konuyla ilgili belirli seviyede bilgileri olmasının önemini vurgulamaktadırlar.

Alanyazın incelendiğinde çevrimiçi mahremiyete dönük bazı ölçek çalışmalarına rastlanmıştır. Örneğin Tokgöz (2011), Karakaya (2014) ve Karslıoğlu (2014), çevrimiçi mahremiyet ile ilgili yapılan mevcut çalışmalar üzerinde yaptıkları incelemelerde, konunun daha çok devlet tarafından gerçekleştirilen faaliyetler açısından incelendiği, diğer alanlarının incelenmediği sonucuna varmışlardır. Mıhçı ve Çakmak (2017), yapmış oldukları Siber Sağlık Ölçekleri geliştirme çalışmalarında Çevrimiçi Mahremiyet Ölçeği ve Çevrimiçi Güvenlik Ölçeği farklı iki alt boyut olarak yer almaktadır. Siber sağlık çatısı altında 7 alt boyuttan oluşan ölçek geliştiren Mıhçı ve Çakmak (2017), bu alt boyutlara olan farkındalık düzeylerini ölçmeye çalışmışlardır. 7 alt boyuttan oluşan ölçek içerisinde Çevrimiçi Mahremiyet ölçeği 4 madde içermekte olup, ölçeğin Çevrimiçi Mahremiyet konusunda sınırlı olduğunu ifade edilmektedir (Mıhçı ve Çakmak, 2017). Alakurt (2017), tarafından uyarlanan Çevrimiçi Mahremiyet Kaygısı ölçeği internet ortamında gizlilik konusuna dikkat çekmeyi amaçlamış ve ölçeği Türk kültürüne göre uyarlamıştır. Keser ve Güldüren

(2015) tarafından geliştirilen Bilgi Güvenliği Farkındalığı ölçeğinde öğrencilerin bu konuya yönelik farkındalıklarını ve eksiklerini gösterecek bir ölçme aracı geliştirmeyi amaçlamışlardır. Yılmaz (2015), tarafından Dijital Veri Güvenliği Farkındalık ölçeği geliştirilmiştir. Erdoğdu, Gökoğlu ve Kara (2021), bilgi güvenliği farkındalığını ölçmek amacıyla Mobil Bilgi Güvenliği Farkındalık ölçeğini geliştirmişlerdir. Yapılan çalışmalara bakıldığında Çevrimiçi Mahremiyet konusunda sınırlı çalışmalar olduğu görülmektedir. Bu araştırmada Çevrimiçi Mahremiyet konusu daha kapsamlı incelenmiş, konu kendi bazında ele alınmıştır. Önceki çalışmaların sınırlılıkları ve kapsam geçerliliği ele alındığında Çevrimiçi Mahremiyet farkındalığıyla ilgili çalışmaların eksikliği görülmektedir. Bu sebeplerden ötürü yapılan araştırmada öğrencilerin Çevrimiçi Mahremiyet Farkındalıkları hakkında geçerliliği ve güvenilirliği kabul gören bir ölçme aracı geliştirmek amaçlanmıştır.

Yöntem

Üniversite öğrencilerinin çevrimiçi mahremiyet farkındalık düzeylerini belirlemeye yönelik bir ölçek geliştirmeyi hedefleyen bu çalışma betimsel tarama modelinde gerçekleştirilmiştir. Betimsel tarama modeli, bireylerin, grupların ortamlardan toplanan verilerin özelliklerini, durumunu, yetenekleri vb. tanımlayan ve özetleyen araştırma modelidir (Büyüköztürk, Çakmak, Akgün, Karadeniz ve Demirel, 2017).

Verilerin Toplanması ve Analizi

Bu araştırmanın çalışma grubunu, Amasya Üniversitesinde 2018-2019 öğretim yılında "İlahiyat, Matematik, Tarih, Şehir ve Bölge Planlama, Kentsel Tasarım ve Peyzaj Mimarlığı, Grafik Tasarım, Bilgisayar Destekli Tasarım, Bilgisayar Programcılığı, İngilizce Öğretmenliği, Okul Öncesi Öğretmenliği, Makine Mühendisliği, Bilgisayar ve Öğretim Teknolojileri Eğitimi, Psikolojik Danışmanlık ve Rehberlik" bölümlerinde öğrenim görmekte olan 514 öğrenci oluşturmaktadır. Ölçek çalışmalarında madde havuzundaki sayısın 10 katı katılımcıya ulaşılmasının önerildiği ifade edilmektedir (Korkmaz, Usta ve Kurt, 2014). Çalışma grubunun cinsiyet ve bölüm özelliklerine göre dağılımı Tablo 1'de yer almaktadır.

Tablo 1. Öğrencilerin Cinsiyete ve Bölüme Göre Dağılımı

Bölüm	Kadın	Erkek	Toplam
İlahiyat	48	26	74
Matematik	25	12	37
Tarih	28	9	37
Şehir ve Bölge Planlama	3	4	7
Kentsel Tasarım ve Peyzaj Mimarlığı	26	20	46
Grafik Tasarım	25	23	48
Bilgisayar Destekli Tasarım	5	20	25
Bilgisayar Programcılığı	7	19	26
Makine Mühendisliği	11	52	63
Bilgisayar ve Öğretim Teknolojileri Eğitimi	25	17	42
Psikolojik Danışmanlık ve Rehberlik	38	7	45
Okul Öncesi Öğretmenliği	18	7	25
İngilizce Öğretmenliği	27	12	39
Toplam	286	228	514

Ölçek Geliştirme Süreci

Bu araştırmada üniversite öğrencilerinin çevrimiçi mahremiyet farkındalıklarına yönelik ölçek geliştirmek amacıyla ilk aşamada çevrimiçi mahremiyet ve farkındalık kavramlarına dönük alanyazın taraması yapılmış (Caudill ve Murphy, 2000; Strauss ve Rogerson, 2002; Furnell ve

Phippen, 2007; Wu, Lau, Atkin ve Lin, 2011; Karaarslan, Eren ve Koç, 2014; Aslanyürek, 2016; Alakurt, 2017; Jordaan ve Van Heerden, 2017; Choi, Park ve Jung, 2018) ve mahremiyet kavramı ve kapsamı incelenmiştir. Bu bağlamda konuyla ilgili geliştirilmiş ölçek olup olmadığı araştırılmış fakat literatürde çevrimiçi mahremiyet farkındalığına yönelik geliştirilmiş bir ölçeğe rastlanmamıştır. Bu taramanın ardından literatürde konuyla ilgili Yılmaz (2015)'in geliştirmiş olduğu "Dijital Veri Farkındalığı" ölçeği, Kalaman (2017) ve Tokgöz (2011)'ün çalışmalarında yapmış oldukları anketler ve benzer araştırmalar (Genç, Kazez ve Fidan, 2013; Keser ve Güldüren, 2015; Güldüren, Çetinkaya ve Keser, 2016; Çetinkaya, Güldüren ve Keser, 2017; Mıhçı ve Çakmak, 2017) incelenmiştir. Yapılan alanyazın taraması sonucunda bireylerin çevrimiçi ortamda mahremiyetleri açısından nasıl davranmaları gerektiğine dönük esaslar belirlenerek her biri ölçek maddesi olarak ifade edilmiştir.

Alan uzmanları ile yapılan görüşmede anlamsal karmaşalar veya benzer anlamları içeren maddeler alan uzmanlarının dönütlerine uygun olarak yeniden düzenlemiştir. Bununla birlikte maddeler içinde yer alan ve farklı anlaşılabilecek kavramların yer aldığı maddeler yeniden düzenlenmiştir. Ayrıca bazı maddelerde bulunan öznel bilgiler geneli kapsayacak şekilde düzenlenmiştir. Uzmanların dönütleri sonrasında maddeler içerisinde yer alan VPN, DoNotTrackMe ve Ghostery gibi terimler teknik bilgi gerektirip herkes tarafından anlaşılamayabileceği yönündeki uzman görüşleri doğrultusunda yeniden gözden geçirilerek gerekli düzeltmeler yapılmıştır. Ayrıca uzman görüşleri doğrultusunda mobil uygulamaların erişim alanları, çift faktörlü şifre korumaları, gizli sekme ve web sitelerinin güvenliği konularına dönük yeni maddeler eklenmiştir. Yapılan alanyazın taraması, araştırmacılar ve alan uzmanlarının katkısı sonucunda madde havuzu 29 olumlu 20 olumsuz olmak üzere 49 maddeden oluşturulmuştur. Hazırlanan ölçeğin maddelerinin yanına, öğrencilerin farkındalık düzeylerini ölçmek amacıyla beşli likert tipi ölçekleme kullanılmıştır. Hazırlanan ölçek Bilgisayar ve Öğretim Teknolojileri alanında 3 uzman görüşüne sunulduktan sonra gelen dönütler doğrultusunda düzeltmeler yapılmıştır. Yapılan düzeltmelerin ardından 49 maddelik ölçek deneme formu oluşturulmuştur.

Verilerin Analizi

Pilot uygulama sonucunda toplanan veriler üzerinde, ilk olarak faktör analizi yapılıp yapılamayacağını belirlemek için Kaiser-Meyer-Olkin (KMO) ile Bartlett analizleri uygulanmıştır. Kaiser-Meyer-Olkin (KMO) verilerin faktör analizine uygun olup olmadığına dair bilgi verdiği ve KMO'nun .60'tan yüksek çıkmasının verilerin faktör analizi için uygun değerde olduğu ifade edilmektedir (Büyüköztürk, 2002; Büyüköztürk vd., 2017).

Yapılan KMO ve Bartlett analizleri sonucunda ölçek verilerinin faktör analizi için uygunluğu belirlenmiştir. Ölçeğin yapı geçerliliği ve faktör yapısını oluşturmak amacıyla açımlayıcı faktör analizi uygulanmıştır. Faktör analizi, "aynı yapıyı ya da niteliği ölçen değişkenleri bir araya toplayarak ölçmeyi az sayıda faktör ile açıklamayı amaçlayan istatistiksel bir teknik" olarak tanımlanmaktadır. (Büyüköztürk, 2018, s.133). Bunun yanı sıra Osberne, Costello ve Kellow (2008), faktör analizinin açık değişkenler birlikte değişimine neden olan gizli değişkenleri ortaya çıkaran bir teknik olduğunu ifade etmektedirler. Açımlayıcı faktör analizi sosyal bilimlerde yaygın olarak kullanılan ve uygulanan bir istatistiksel tekniktir (Osberne vd., 2008). Ölçeğin faktör yapısı temel bileşenler analizi tekniği kullanılarak belirlenmiştir. Ölçeğin faktör yükleri ise varimax dik döndürme tekniği kullanılarak incelenmiştir. Rotasyon işlemlerinde dik ve eğik döndürme yöntemleri kullanılır. Dik döndürme yöntemi, faktörlerin birbiri ile ilişkiye girmemesini sağlar. Eğik döndürme yöntemde ise faktörler birbirinden bağımsız değildir. Bu nedenle genelde dik döndürme yöntemi tercih edilir. Temel bileşenler analizi, değişken eksiltme ile kavramsal yapılar elde etmek için kullanılan bir istatistiksel tekniktir (Büyüköztürk, 2018). Temel eksen faktör analizine göre daha yaygın, pratik olması, diğer analizlerde kullanılmak üzere puan hesaplamak ve

verileri azaltmak için daha kullanışlı olması ve tüm maddeler için varyansların tamamını analize katması nedeniyle temel bileşenler analizi tercih edilmiştir. Yapılan analiz sonucunda faktör yükü .30'dan düşük ve birden çok faktöre dağılan maddeler ölçekten çıkarılarak analizler yenilenmiştir. Açımlayıcı ve doğrulayıcı faktör analizleri 514 öğrenciden oluşan örneklem üzerinden gerçekleştirilmiştir.

Açımlayıcı faktör analizinin ardından elenen maddeler ölçekten çıkarılarak kalan 17 madde kullanılarak ölçeğin doğrulayıcı faktör analizi incelenmiştir. Doğrulayıcı faktör analizi, belirlenen sayıda faktörün altında yer alan maddelerin bulundukları faktörü yeterinde temsil edip etmediğini belirlemeye yönelik kullanılan bir yöntemdir (Buyruk ve Korkmaz, 2014). Doğrulayıcı faktör analizi maksimum olasılık yöntemiyle incelenmiştir. Doğrulayıcı faktör analizi sonucunda ulaşılan modelin doğrulanabilmesi amacıyla RMSEA, S-RMR, GFI, AGFI, CFI, NFI ve IFI indeksleri kullanılmıştır. Uygulanan faktör analizinin sonucunda ölçeğin ayırt ediciliği bağımsız örneklem t testi uygulanarak belirlenmiştir. Madde ayırt ediciliği, maddelerin ölçülmek istenilen özelliğe göre kişileri ne düzeyde ayırdığını gösteren bir yöntemdir (Büyüköztürk vd., 2017). Bu araştırmada ulaşılan ham puanların büyükten küçüğe sıralanmasının ardından %27'lik üst-alt grupların ortalama farkına dayalı bir teknik kullanılarak maddelerin ayırt ediciliği hesaplanmıştır (Büyüköztürk vd., 2017). Ölçeğin ayırt ediciliği belirlendikten sonra, Pearson's r testi kullanılarak madde toplam korelasyonlarına bakılarak ölçeğin geçerliliği hesaplanmıştır. Ölçeğin güvenirliğini belirlemek amacıyla öncelikle iç tutarlılık katsayı yöntemi kullanılarak ölçeğin Cronbach's Alpha, Eş Yarılar Korelasyonu, Guttman Split-Half ile Spearman Brown güvenirlik katsayılarına bakılmıştır. Güvenirlik katsayısının .70 ve daha yüksek olması ölçekteki maddelerin güvenirliği için genel olarak yeterli olduğu ifade edilmiştir (Büyüköztürk, 2018). Ölçeğin güvenirliğini hesaplamak amacıyla ölçeğin kararlılık düzeyine bakılmıştır. Kararlılık analizi için test-tekrar-test yöntemi kullanılmıştır. İki uygulama arasındaki elde edilen puanların korelasyonu ile hesaplanan kararlılık katsayısı yönteminde, değerlerin .30 düzeyinin altında olması düşük, .30 – .70 düzeyinin arasında olması orta, .70 – 1.00 düzeyinin arasında olması ise yüksek ilişkiyi gösterdiği ifade edilmektedir (Büyüköztürk vd., 2017, Büyüköztürk, 2018).

Verilerin Toplanması

Çalışma grubunda belirlenen bölümler ve bu bölümlerin derslerine girmekte olan öğretim üyeleriyle görüşülüp uygun zaman ve dersler belirlenmiştir. Çoğaltılan ölçekler belirlenen derslerde araştırmacı ve öğretim üyeleriyle birlikte öğrencilere verilen 20 dakikalık süre içerinde uygulanarak veriler toplanmıştır. Verilerin toplanma süresi 3 hafta sürmüştür.

Bulgular ve Yorum

Ölçeğin Geçerliliğine İlişkin Bulgular

Çevrimiçi Mahremiyet Farkındalığı Ölçeğinin geçerliliğini belirlemeye yönelik yapı geçerliği, madde-faktör korelasyonları, madde ayırt edicilik değerleri hesaplanmıştır. Sonuçlara ilişkin bulgular aşağıda verilmiştir.

Yapı Geçerliliği

Açımlayıcı Faktör Analizine İlişkin Bulgular: Çevrimiçi Mahremiyet Farkındalığı Ölçeğinin yapı geçerliliğini test etmek amacıyla öncelikle veriler üzerinde KMO ile Bartlett analizi yapılmıştır. Yapılan analiz sonucunda KMO= .826; Bartlett değeri $\chi 2$ = 6742.313; sd=1176 (p= .000) olarak belirlenmiştir. Faktör analizinin yapılabilmesi için KMO değerinin .60'tan yüksek olması beklenmektedir (Büyüköztürk vd., 2017). Yapılan analizler sonucunda çıkan değerler çerçevesinde 49 maddeli ölçekte faktör analizi yapılabileceği sonucuna ulaşılmıştır.

Ölçeğin tek faktörlü olup olmadığını anlamak amacıyla temel bileşenler analizi, faktör yüklerini anlamak amacıyla varimax dik döndürme tekniği uygulanmıştır. Oluşan madde yükleri incelenerek madde yükü .30'dan düşük 26 madde ile birden fazla faktöre dağılan 6 madde ölçekten çıkarılmıştır. Bu işlemin ardından yeniden uygulanan faktör analizi ölçekte kalan 17 madde üzerinden yapılmıştır. Çıkarılan maddeler kapsam geçerliliği açısından incelenmiş ve kapsam geçerliliğini etkilemeyeceğine karar verilerek uzman görüşü alındıktan sonra ölçekten çıkarılmasına karar verilmiştir.

Yapılan analizlerle birlikte kalan 17 maddenin, 3 faktör altında toplandığı görülmüştür. Ölçeğin 17 maddelik son hali sonucunda KMO değerinin .782; Bartlett değerinin $\chi 2$ = 2519.513; sd= 136 (p= .000) olduğu görülmüştür. Ölçeğin kalan 17 maddesiyle yapılan analizlerle birlikte varimax dik döndürme tekniği sonrası yüklerin .511 ile .784 arasında olduğu görülmüştür. Yapılan analizler sonucunda ölçekte yer alan maddeler ile faktörlerin varyansın % 47.709 'ünü açıkladığı belirlenmiştir. Bu sonuçların ardından faktördeki maddeler incelenerek faktörlere isim verilmiştir. "Dikkat" ismi verilen ilk faktör altında yedi madde, "Güvenlik" ismi verilen ikinci faktör altında beş madde ve "İletişim ve Paylaşım" ismi verilen üçüncü faktör altında beş madde toplanmıştır. Yapılan analizlerle birlikte ölçekte kalan 17 maddenin varyansı açıklama miktarı, faktörlerin öz değerleri ile madde yüklerinin faktörlere göre dağılımına ait bulgular Tablo 2'de yer almaktadır.

Tablo 2. Açımlayıcı Faktör Analizi Sonuçları

	Maddeler		Ortak Varyans	F1	F2	F3
F1: Dikkat	M-14	Kullandığım çevrimiçi platformların gizlilik ayarlarını ve bildirimlerini kontrol ederim.	.366	.511		
	M-13	Kullandığım çevrimiçi ortamlarda (sosyal ağlar, alışveriş siteleri, oyunlar vb.) hesabımın gizlilik ayarlarını yaparım.	.379	.518		
	M-3	Çevrimiçi ortamlarda kullandığım parolaların güçlü olmasına (büyük-küçük harf, rakam, özel karakterler ve en az 8 karakter kullanımıyla) dikkat ederim.	.335	.547		
	M-10	E-posta veya sosyal ağlardan aldığım mesajların içeriğinin güvenilir olup olmadığını anlarım.	.541	.646		
	M-4	Çevrimiçi ortamlarda paylaştığım bilgilerin şirketler, devlet kurumları veya bilgisayar korsanları tarafından kullanılabileceğinin farkındayım.	.441	.664		
	M-5	Çevrimiçi ortamlarda tanımadığım kişilerden gelen mesaj veya e-postaların güvenlik riski oluşturup oluşturmadığını anlarım.	.486	.680		
	M-9	Çevrimiçi platformlarda paylaştığım bilgilerin kötü niyetli kişiler tarafından kullanılabileceğinin farkındayım.	.539	.730		
F2: Güvenlik	M-11	İnternet sitelerinin kullandığı çerez (cookies) dosyaları hakkında bilgim vardır.	.382		.550	
	M-15	Mobil cihazıma uygulama yüklerken uygulamanın hangi izinleri talep ettiğine dikkat ederim.	.588		.566	
	M-12	İnternet sitelerinin ve mobil uygulamaların güvenlik sertifikalarını ve veri şifreleme yöntemlerini kontrol ederim.	.424		.735	
	M-17	Ziyaret ettiğim web sitelerinin güvenliğini kontrol ederim.	.564		.759	
	M-16	Web tarayıcımdaki eklentilerin hangi bilgilere erişeceğine dikkat ederim	.590		.784	
F3: İletişim	M-8	Çevrimiçi ortamlarda tanımadığım kişilerle kişisel bilgilerimi (adres, doğum tarihi, yaş iş, telefon vb.) paylaşırım.	.641			.547

M-1	Arkadaşlarımla veya yakınlarımla yaptığım yazışmaların ekran görüntülerini izin almaya gerek duymadan paylaşırım.	.342		.613
M-2	Başkalarına ait bilgi, resim, video vb. içerikleri çevrimiçi ortamlarda izin almaya gerek duymadan paylaşırım.	.542		.633
M-6	Çevrimiçi ortamlarda tanımadığım kişilerin beni takip etmesine veya arkadaş olmasına izin veririm.	.393		.766
M-7	Çevrimiçi ortamlarda tanımadığım kişilerle iletişim kurarım.	.637		.767
	Özdeğer	3.052	2.698	2.360
	Açıklanan varyans	17.954	15.874	13.881

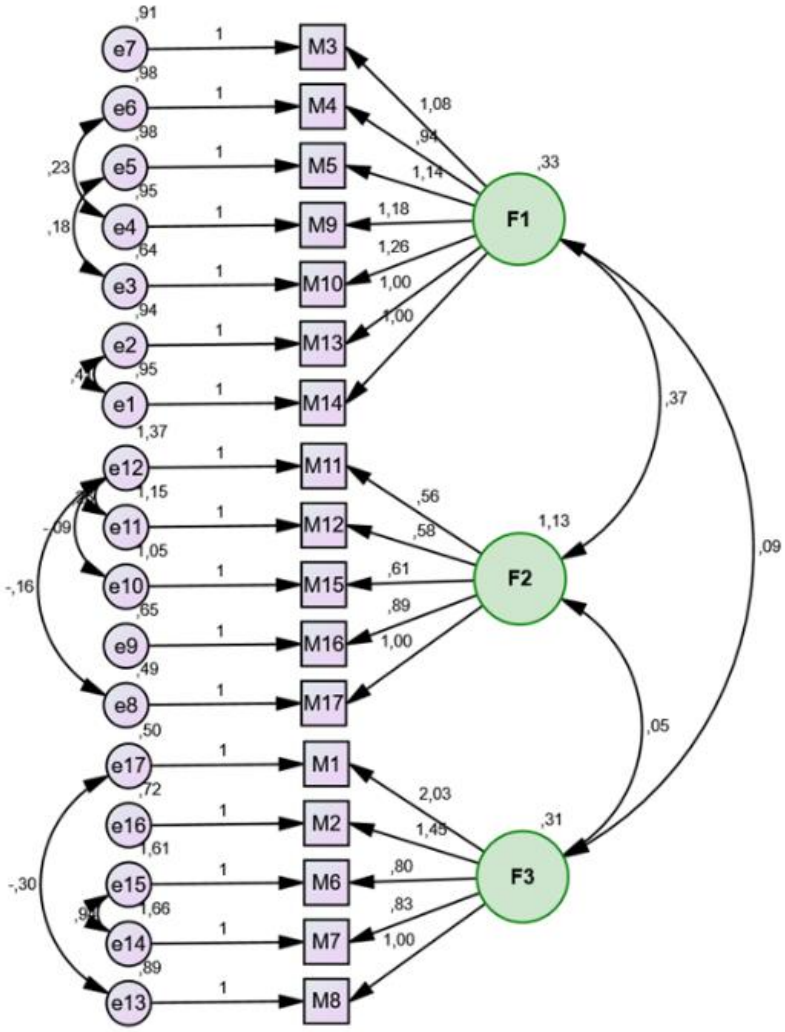
Tablo 2'de görüldüğü gibi ölçeğin "Dikkat" faktörünün altında 7 madde bulunmaktadır. Maddelerin faktör yükleri .511 ve .730 değerleri arasında değişmektedir. "Dikkat" faktörünün toplam varyansa sağladığı katkı miktarı %17.954'tür. "Dikkat" faktörünün ölçek içindeki öz değeri 3.052'dir "Güvenlik" faktörü altında 5 madde bulunmaktadır. Maddelerin faktör yükleri .550 ve .784 değerleri arasında değişmektedir. "Güvenlik" faktörünün toplam varyansa sağladığı katkı miktarı %15.874'tür. "Güvenlik" faktörünün ölçek içindeki öz değeri 2.698'dir. "İletişim ve Paylaşım" faktörü altında 5 madde bulunmaktadır. Maddelerin faktör yükleri .547 ve .766 değerleri arasında değişmektedir. "İletişim ve Paylaşım" faktörünün toplam varyansa sağladığı katkı miktarı %13.881'dir. "İletişim ve Paylaşım" faktörünün ölçek içindeki öz değeri 2.360'tır. "İletişim ve Paylaşım" faktörde yer alan maddeler yapı olarak olumlu anlam olarak ise olumsuzdur. Bundan dolayı bu faktörde yer alan maddeler analiz sırasında ters çevrilerek kodlanmalıdır.

Doğrulayıcı Faktör Analizine İlişkin Bulgular: Açımlayıcı faktör analizi sonucunda 17 maddeden oluşan üç faktörlü ölçeğin faktör yapılarını doğrulamak amacıyla doğrulayıcı faktör analizi Amos 23 programıyla analiz yapılarak incelenmiştir. Doğrulayıcı faktör analizi yapılarak model oluşturulmuştur. Oluşturulan modelin uyum indekslerinde iyileştirme yapılmak amacıyla maddeler arasındaki kovaryanslar incelenerek modifikasyon gerçekleştirilmiştir. Gerçekleştirilen modifikasyonlar Şekil 1'de gösterilmiştir. Doğrulayıcı faktör analizi maksimum olasılık yöntemiyle yapılmış olup $\chi2$(sd=108, N=514) = 343.186, $\chi2$/sd = 3.178; p< .001, RMSEA= .065, S-RMR= .064, GFI= .929, AGFI= .900, CFI= .903, NFI= .866 ve IFI= .904 uyum iyelik değerleri bulunmuştur. Uyum indekslerine ilişkin değer aralıkları Tablo 3'te özetlenmiştir (Kline, 2015; Şimsek, 2007).

Tablo 3. Uyum Değerleri ve Yorumları

İncelenen Uyum İndeksleri	Mükemmel Uyum	Kabul Edilebilir Uyum
$\chi2$/sd	$0 \leq \chi2/sd \leq 2$	$2 \leq \chi2/d<5$
RMSEA	$0 \leq$ RMSEA $\leq .05$	$.05 \leq$ RMSEA $\leq .08$
S-RMR	$0 \leq$ S-RMR $\leq .05$	$.05 \leq$ S-RMR $\leq .10$
GFI	$.95 \leq$ GFI ≤ 1	$.90 \leq$ GFI $\leq .95$
AGFI	$.95 \leq$ AGFI ≤ 1	$.90 \leq$ AGFI $\leq .95$
CFI	$.97 \leq$ CFI ≤ 1	$.95 \leq$ CFI $\leq .97$
NFI	$.95 \leq$ NFI ≤ 1	$.90 \leq$ NFI $\leq .95$
IFI	$.95 \leq$ IFI ≤ 1	$.90 \leq$ IFI $\leq .96$

Analiz sonucunda NFI değeri kabul edebilir değere çok yakın, diğer değerlerinde kabul edilebilir uyum gösterdiği görülmüştür. Elde edilen bu sonuçlar doğrultusunda açımlayıcı faktör analizi ile oluşturulan faktör yapılarının doğrulandığının göstergesidir. Analizler sonucunda faktör modeli ile faktör-madde ilişkisine ait t değerleri Şekil 1'de yer almaktadır.



Şekil 1. Doğrulayıcı Faktör Analizi Korelasyon Diyagramı (t Değerleri)

Madde Faktör Korelasyonlarına İlişkin Bulgular: Ölçekte var olan her bir faktörde yer alan maddeler ve faktörlerden elde edilmiş puanlar arasındaki korelasyon madde faktör korelasyonu yöntemi ile hesaplanmıştır. Bu analiz sonucunda ölçekteki maddelerin genel amaca hizmet etme durumu, her bir maddenin ölçekte olma ve olmama durumları arasındaki ilişki, bu sayede maddenin ölçeğe katkısı tespit edilmiştir. Ölçekte yer alan maddelerin hesaplanan madde-faktör korelasyon değerleri Tablo 4'te yer almaktadır.

Tablo 4. Madde – Faktör Korelasyonları

Dikkat		Güvenlik		İletişim ve Paylaşım	
Madde	r.	Madde	r.	Madde	r.
M3	.610**	M11	.630**	M1	.667**
M4	.617**	M12	.695**	M2	.679**
M5	.668**	M15	.643**	M6	.718**
M9	.680**	M16	.783**	M7	.733**
M10	.697**	M17	.788**	M8	.610**
M13	.654**				

M14	.647**

N = 514 **= p< .001

Tablo 4 incelendiğinde birinci faktördeki maddelerin madde faktör korelasyonları .610 ve .967; ikinci faktördeki maddelerin madde faktör korelasyonları .630 ve .788; üçüncü faktördeki maddelerin madde faktör korelasyonları .610 ve .733 arasında değiştiği görülmektedir. Ölçekte yer alan maddelerin bulundukları faktörler ile arasındaki ilişkinin pozitif ve anlamlı olduğu görülmektedir (p< .000). Bu sonuçlara göre maddelerin bulundukları faktörün ve ölçeğin amacına hizmet ettiği ifade edilebilir.

Madde Ayırt Ediciliğine İlişkin Bulgular: Ölçeği oluşturan maddelerin ayırt edicilik gücünün hesaplanması amacıyla maddelerin puanları büyükten küçüğe doğru sıralanmıştır. Bunun ardından sıralamada oluşan %27'lik üst-alt gruplarda bulunan 138'er kişiden oluşan gruplar belirlenmiştir. Oluşan grupların puanlarına madde ayırt edicilik gücünü hesaplamak amacıyla bağımsız örneklem t-testi yapılmıştır. Ölçekteki her bir maddenin ayırt edicilik güçlerini gösteren t değerleri ile anlamlılık düzeyleri Tablo 5'te verilmiştir.

Tablo 5. Madde Ayırt Edicilik Güçleri

Dikkat		Güvenlik		İletişim ve Paylaşım			
Madde	t	Madde	t	Madde	t	Faktör	t
M3	11.893	M11	9.530	M1	9.056	F1	23.185
M4	10.864	M12	9.215	M2	8.952	F2	20.608
M5	11.384	M15	11.719	M6	7.371	F3	13.784
M9	11.488	M16	15.101	M7	8.456		
M10	13.717	M17	16.813	M8	9.759		
M13	12.311					Toplam	43.386
M14	11.610					Df: 276; p< .001	

Tablo 5 incelendiğinde ölçekte bulunan 17 maddeye, faktörlere ve toplam puana ilişkin bağımsız örneklem t testi sonucunda elde edilen değerler 7.371 ile 16.813 arasında değiştiği görülmektedir. Ölçeğin geneline ait t değeri 43.386 olarak belirlenmiştir. Analiz sonucunda belirlenen farklar anlamlı düzeyde olduğu görülmektedir (p< .001). Buna göre ölçekteki maddelerin ve ölçeğin genelinin ayırt edicilik düzeyinin yüksek olduğu söylenebilir.

Ölçeğin Güvenirliğine İlişkin Bulgular

Çevrimiçi Mahremiyet Farkındalığı Ölçeğinin güvenirliğini belirlemeye yönelik iç tutarlılık ile kararlılık analizleri yapılmış ve bulgular aşağıda verilmiştir.

İç Tutarlılık Düzeyine İlişkin Bulgular: Ölçeğin faktörleri ve bütün halinin güvenirlik analizi; Cronbach's Alpha, Eş Yarılar Korelasyonu, Guttman Split-Half ile Spearman Brown güvenirlik katsayıları kullanılarak incelenmiştir. Faktörlere ve ölçeğin geneline ilişkin güvenirlik analizi sonuçları Tablo 6'da verilmiştir.

Tablo 6. Faktör İç Tutarlılık Katsayıları

Faktörler	Madde Sayısı	Cronbach's Alpha	Eş Yarılar Korelasyonu	Guttman Split-Half	Spearman Brown
Dikkat	7	.776	.558	.704	.719
Güvenlik	5	.696	.574	.722	.735
İletişim ve Paylaşım	5	.713	.486	.629	.661
Toplam	17	.794	.630	.769	.773

Tablo 6 incelendiğinde 3 faktör ve 17 maddeden oluşan ölçeğin Cronbach's Alpha değeri .794; Eş Yarılar Korelasyonu .630; Guttman Split-Half değeri .769; Spearman Brown değeri .773 olarak belirlenmiştir. Bununla birlikte faktörlerin güvenirlik değerleri incelendiğinde Cronbach's Alpha değeri .696 ile .776; Eş Yarılar Korelasyonu .486 ile .574; Guttman Split-Half değeri .629 ile .722; Spearman Brown değeri .661 ile .735 arasında olduğu görülmektedir. Bu sonuçlar faktörlerin her birinin ve ölçeğin bütününün tutarlı ölçümler yapabildiği söylenebilir.

Kararlılık Düzeyine İlişkin Bulgular: Ölçeğin geçerlilik düzeyini belirlemek amacıyla test tekrar test yöntemi kullanılmıştır. 17 maddeden oluşan ölçek formu daha önce veri toplanmış olan 22 kişilik gruba 4 haftanın ardından yeniden uygulanmıştır. Yapılan birinci ve ikinci uygulama sonucunda elde edilen puanlar arasındaki ilişki her bir madde, faktör ve ölçek bütünü için analiz edilmiştir. Ölçeğin kararlılık analizine ilişkin bulgular tablo 7'de verilmiştir.

Tablo 7. Test Tekrar Test Sonuçları

Dikkat		Güvenlik		İletişim ve Paylaşım			
Madde	r	Madde	r	Madde	r	Faktör	r
M3	.643 **	M11	.772 **	M1	.871 **	Dikkat	.693 **
M4	.468 *	M12	.628 **	M2	.804 **	Güvenlik	.737 **
M5	.779 **	M15	.444 *	M6	.831 **	İletişim ve	.863 **
M9	.490*	M16	.464 *	M7	.421 *	Paylaşım	
M10	.549*	M17	.768 **	M8	.473 **		
M13	.602**						
M14	.470*					Toplam	.791 **

N=22; ** p<.001; * p<.005

Tablo 7 incelendiğinde ölçekteki maddelerin korelasyon katsayıları .421 ile .871 arasında değiştiği, bu ilişkilerin pozitif ve anlamlı olduğu görülmektedir. Uygulanan test-tekrar-test yöntemi sonucunda ölçeği oluşturan faktörlerin elde edilen korelasyon katsayıları "Dikkat" için .693, "Güvenlik" için .737 ve "İletişim ve Paylaşım" için ise .863 olarak bulunmuştur. Ölçeğin bütününe ait korelasyon değeri .863'tür ve her bir ilişki anlamlı ve pozitiftir (p< .001; p< .005). Bu sonuçlara göre ölçeğin geçerlilik düzeyinin yüksek olduğu söylenebilir.

Tartışma, Sonuç ve Öneriler

Bu çalışmada bireylerin çevrimiçi ortamlardaki mahremiyet farkındalıkların düzeyini belirlemek amacıyla Çevrimiçi Mahremiyet Farkındalığı ölçeği geliştirilmiştir. Geliştirilmiş olan Çevrimiçi Mahremiyet Farkındalığı ölçeğindeki 17 madde beşli likert tipinde ölçeklendirilmiştir. Faktörleri isimlendirmek için her bir faktöre dağılan maddeler ve alanyazın incelenmiş ve ölçeğin faktörleri isimlendirilmiştir. "Dikkat" adının verildiği faktör 7 madde, "Güvenlik" adının verildiği faktör 5 madde ve "İletişim ve Paylaşım" adının verildiği faktör 5 maddeden oluşmaktadır. Benzer ölçeklerde (Keser ve Güldüren, 2014; Yılmaz, 2015; Alakurt, 2017; Mıhçı ve Çakmak, 2017) yer alan faktörlerin isimlendirilmesinde Saldırı, Tehditler, Korunma, Kullanım ve Güven kavramlarının kullanıldığı görülmüştür. Bu bağlamda yapılan ölçekler ve Çevrimiçi Mahremiyet Farkındalığı ölçeğinde faktörlere dağılan maddelerde incelenerek faktörler isimlendirilmiştir.

Ölçeğin geçerliliğini belirlemek amacıyla faktör analizi ve ayırt edicilik düzeyleri yöntemleri kullanılmıştır. Ölçeğin analize uygunluğunu ve faktör yapısını belirlemek için açımlayıcı faktör analizi uygulanmıştır. Yapılan analiz sonucunda ulaşılan değerler ile ölçeğin 3 faktöre dağıldığı görülmüştür. Faktörlerde yer alan açıklanan varyans, faktörlerin özdeğerleri ve maddelerin faktör yükleri miktarları incelendiğinde ölçeğin, yapı geçerliğine sahip bir ölçek olduğu söylenebilir. Açımlayıcı faktör analizinin ardından üç faktöre ayrılan ölçeğin faktör yapılarını doğrulamak amacıyla ölçek verileri üzerinde doğrulayıcı faktör analizi uygulanmıştır. Uygulanan doğrulayıcı

faktör analizi sonucunda, oluşturulan ölçek modelinin veriler tarafından doğrulandığı sonucuna ulaşılmıştır. Ölçeği oluşturan maddelerin, bulunduğu faktörle ölçmeye çalıştığı özelliği ne düzeyde ölçebileceğini belirlemek amacıyla madde-faktör korelasyonları incelenmiştir. İncelenen madde faktör korelasyonları sonucunda ulaşılan değerler, ölçekte bulunan maddelerin ve faktörlerin, ölçeğin geneli ile ölçeğin ölçmek istediği özelliği ölçebilme amacına anlamlı düzeyde hizmet ettiği görülmektedir. Bu analizlerin ardından maddelerin ayırt ediciliğinin belirlenmesi amacıyla %27'lik üst - alt gruplar arasındaki farkın bulunması amacıyla yapılan bağımsız örneklem t-testi sonucunda, ölçekte yer alan maddelerin ve ölçeğin bütününün ayırt ediciliğinin yüksek olduğu tespit edilmiştir. Ölçeğin güvenirliği belirlemek amacıyla iç tutarlılık ve kararlılık yöntemleri uygulanmıştır. Ölçeğin iç tutarlılık katsayılarının hesaplanması amacıyla; Cronbach's Alpha, Eş Yarılar Korelasyonu, Guttman Split-Half ile Spearman Brown güvenirlik katsayıları kullanılmıştır. Elde edilen iç tutarlılık katsayıları sonucunda ölçeğin güvenilir ölçümler yapabildiği sonucuna varılmıştır. Ölçeğin kararlılık düzeyini belirlemek amacıyla ilk uygulamanın üzerinden geçen dört haftanın ardından iki uygulamadan elde edilen verilere madde ve faktör bazında test-tekrar-test yöntemi uygulanmış, aradan geçen zamana rağmen ölçeğin güvenli ölçümler yapabildiği belirlenmiştir.

Alanyazın incelendiğinde mahremiyete yönelik bazı ölçek çalışmaları bulunmaktadır. Örneğin Mıhçı ve Çakmak (2017) tarafından yapılan Siber Sağlık Ölçekleri çalışması, ortaokul öğrencileri için geliştirilmiş ve 7 alt bölümden oluşmaktadır. Bu alt boyutlardan birisi Çevrimiçi Mahremiyet başlıklıdır ve dört maddeden oluşmaktadır. Alakurt (2017), internet kullanıcılarına yönelik Çevrimiçi Mahremiyet Kaygısı ölçeğinin uyarlama çalışmasını gerçekleştirmiştir. Bu çalışma E-posta Kullanımı, Çevrimiçi Güven ve Çevrimiçi Ödeme olmak üzere 3 faktörden oluşmaktadır. E-posta Kullanımı faktörü 6 madde, Çevrimiçi Güven faktörü 6 ve Çevrimiçi Ödeme faktörü 2 madde olmak üzere ölçek toplam 14 maddeden oluşmaktadır. Keser ve Gülderen (2015), öğretim elemanları için Bilgi Güvenliği Farkındalığı ölçeğini geliştirmişlerdir. Bu çalışma, Saldırı ve Tehditler ile Kişisel Verilerin Korunması faktörleri olmak üzere 2 faktör ve 34 maddeden oluşmaktadır. Gülderen, Çetinkaya ve Keser (2016), ortaokul öğrencilerine yönelik Bilgi Güvenliği Farkındalığı ölçeğini geliştirmişlerdir. Geliştirilen ölçek Saldırı ve Tehditler, Mahremiyet ile Kişisel Verilerin Korunması faktörleri olmak üzere 3 faktör ve 36 maddeden oluşmaktadır. Son olarak Yılmaz (2015), öğretmenler için Dijital Veri Güvenliği ölçeğini geliştirmiştir. Dijital Veri Güvenliği Farkındalığı ölçeği tek faktörlü yapıda oluşan 34 maddelik bir ölçektir. Erdoğdu, Gökoğlu ve Kara (2021), tarafından üniversite öğrencileri için geliştirilen Mobil Bilgi Güvenliği Farkındalık ölçeği 6 faktör ve 17 maddeden oluşmaktadır. Mobil Bilgi Güvenliği Farkındalık ölçeğinin faktörleri Başkalarına Ait Cihazları Kullanma, Yedekleme, Güncelleme, Erişim İzni, Şifre Koruması ile Anlık Mesajlaşma ve Gezinim olarak belirlenmiştir (Erdoğdu, Gökoğlu ve Kara, 2021). Alanyazında yer alan ölçekler geliştirildikleri düzey, faktör ve madde sayıları açısından incelenmiştir. Görüldüğü gibi alanyazında geliştirilen bu ölçeklerden üçü siber sağlık, veri güvenliği bilgi güvenliği odaklı geliştirilmiş ve yalnızca bir boyutunda çevrimiçi mahremiyete değinilmiştir. Bu çalışmada geliştirilen ölçekte ise Çevrimiçi Mahremiyet Farkındalığı kavramı Dikkat, Güvenlik ile İletişim ve Paylaşım olmak üzere üç faktörle açıklanmaya çalışılarak daha genel ve kapsayıcı bir çerçeve çizilmeye çalışılmıştır. Bu yönüyle ölçeğin diğer ölçeklerden ayrıldığı ve alanyazına katkı sağlayacağı söylenebilir.

Bireylerin hızla gelişen çevrimiçi ortamlarda bilgiye erişiminin ve paylaşımının giderek artması, bireylerin kişisel bilgilerinin gizliliği konusunda onları tehlikelere açık hale getirebilir ve tehlikeleri ortaya çıkarabilir (Debatin vd., 2009; Çetinkaya vd., 2016; Taşdelen ve Çataldaş, 2017; Hazar, 2018). İnternetin hızla yaygınlaşması sonucu değişken özelliklere sahip olması bireylerin mahremiyetlerini korumalarını zorlaştırmış ve mahremiyet tedirginliği yaşadıkları bir konu haline gelmiştir (Acılar vd., 2015; Kalaman, 2017). Çevrimiçi mahremiyet, bireyin kişisel bilgilerini (adı, adresi, ailevi bilgileri, kimlik numarası vb.) çevrimiçi ortamlarda koruması için alabileceği tedbirler

olarak ifade edilmektedir (Strauss ve Rogerson, 2002; Wu vd., 2011). Teknolojinin ve veri tabanlarının hızla gelişmesiyle birlikte bireylerin kişisel bilgilerinin depolanabilmesi, kopyalanabilmesi, taşınabilmesi gibi işlemlerin kolaylıkla yapılabilmesi, kişisel bilgilerin sadece yasalarla korunamayacağı gerçeği çevrimiçi mahremiyet farkındalığının önemini arttırmaktadır (Karaarslan vd., 2014; Aslanyürek, 2016; Choi vd., 2018). Bireylerin çevrimiçi mahremiyete yönelik kaygılarının çevrimiçi ortamlara olan güvenlerini etkilediği ifade edilmektedir (Beldad, Jong ve Steehouder, 2010; Okumuş ve Atılgan, 2021). Okumuş ve Atılgan, web sitelerinin sunmuş oldukları gizlilik politikalarının anlaşılır olmasının bireylerinin çevrimiçi ortamlara güvenlerini arttırdığını ifade etmişlerdir. Bireylerin çevrimiçi ortamlarda gösterdikleri güvenlik ve gizlilik hedeflerinin benzer olduğu ifade edilmektedir (Kayes ve Iamnitchi, 2017). Bireylerin çevrimiçi ortamlarda mahremiyet kavramını önemsemediği yapılan çalışmalarda ifade edilmiştir (Yıldız, 2012; Acılar vd., 2015). Ancak bireylerin çevrimiçi ortamlarda güvenliklerinin sağlanabilmesi, her şeyden önce mahremiyete ilişkin farkındalıklarının geliştirilmesi ile mümkün olabilir. Öte yandan bireylerin çevrimiçi mahremiyet konusunda ne kadar farkındalıklarının olduğunun belirlenmesinin önemli olduğu söylenebilir. Bu bağlamda geliştirilmiş olan Çevrimiçi Mahremiyet Farkındalığı Ölçeği bireylerin çevrimiçi ortamlarda bilgilerinin gizliliğinin farkındalık düzeyinin belirlenmesi amacıyla kullanılmasında yardımcı olacağı düşünülmektedir.

Sonuç olarak Çevrimiçi Mahremiyet Farkındalığı Ölçeğinin bireylerin çevrimiçi ortamlarda mahremiyete dönük farkındalık düzeylerini belirlemek için kullanılabilecek geçerli ve güvenilir bir ölçek olduğu söylenebilir. İncelenen alanyazında bireylerin çevrimiçi mahremiyet farkındalıklarını ölçen bir ölçeğe rastlanmamıştır. Bu ölçeğin alanyazına önemli katkılar sağlayabileceği düşünülmektedir. Ölçeğin geçerlilik ve güvenirlik çalışması üniversite öğrencileri üzerinden gerçekleştirilmiştir. Çevrimiçi Mahremiyet Farkındalığı Ölçeğinin farklı yaş gruplarındaki bireyler için uyarlanması önerilebilir.

Sınırlılıklar

Araştırma Amasya Üniversitesinde 2018 - 2019 bahar döneminde öğrenim görmekte olan 514 öğrenci ile sınırlıdır.

Alanyazında hem AFA hem de DFA'nın aynı veri seti kullanılarak yapılamayacağı yönünde bulgular yer almaktadır. Ancak bu araştırmada farklı bir veri seti oluşturulamadığından hem AFA hem de DFA aynı veri seti kullanılarak yapılmış, AFA yalnızca DFA'yı güçlendirmek amacıyla kullanılmıştır.

Kaynakça

Acilar, A., Olgun, H., & Gorur, A. (2015). Privacy concerns of public employees on the internet: A study in Bursa. *Research Journal of Business and Management*, *2*(3), 334-347.

Alakurt, T. (2017). Adaptation of online privacy concern scale into Turkish culture. *Pegem Journal of Education and Instruction*, *7*(4), 611–636.

Aslanyürek, M. (2016). İnternet ve sosyal medya kullanıcılarının internet güvenliği ve çevrimiçi gizlilik ile ilgili kanaatleri ve farkındalıkları. *Maltepe Üniversitesi İletişim Fakültesi Dergisi, 3*(1), 80-106.

Beldad, A., De Jong, M., & Steehouder, M. (2010). How shall I trust the faceless and the intangible? A literature review on the antecedents of online trust. Computers in human behavior, 26(5), 857-869.

Buyruk, B., & Korkmaz, Ö. (2014). FeTeMM farkındalık ölçeği (FFÖ): geçerlik ve güvenirlik çalışması. *Türk Fen Eğitimi Dergisi, 11*(1), 3-23.

Büyüköztürk, Ş. (2002). *Veri Analizi El Kitabı*. Ankara: Pegem A.Yayıncılık.

Büyüköztürk, Ş. (2018). *Sosyal Bilimler İçin Veri Analizi El Kitabı*. Pegem Atıf İndeksi, 001-214.

Büyüköztürk, Ş., Çakmak, E. K., Akgün, Ö. E., Karadeniz, Ş., & Demirel, F. (2017). *Bilimsel Araştırma Yöntemleri*. Pegem Atıf İndeksi, 1-360.

Caudill, E. M., & Murphy, P. E. (2000). Consumer online privacy: legal and ethical *Issues. Journal Of Public Policy & Marketing, 19*(1), 7-19.

Choi, H., Park, J., & Jung, Y. (2018). The role of privacy fatigue in online privacy behavior. *Computers In Human Behavior*, 81, 42-51.

Çetinkaya, L., Güldüren, C., & Keser, H. (2017). Öğretmenler için bilgi güvenliği farkındalık ölçeği (BGFÖ) geliştirme çalışması. *Milli Eğitim Dergisi, 46*(216), 33-52.

Debatin, B., Lovejoy, J. P., Horn, A. K., & Hughes, B. N. (2009). Facebook and online privacy: attitudes, behaviors, and unintended consequences. *Journal Of Computer-Mediated Communication, 15*(1), 83-108.

Erdoğdu, F., Gökoğlu, S., & Kara, M. (2020). "What about users?": Development and validation of the mobile information security awareness scale (MISAS). *Online Information Review*. *45* (2). 406-421

Furnell, S., & Phippen, A. (2012). Online privacy: a matter of policy? *Computer Fraud & Security, 2012*(8), 12-18.

Genç, Z., Kazez, H., & Fidan, A. (2013). Çevrimiçi etik dışı davranışlarının belirlenmesi için bir ölçek uyarlama çalışması. *Akademik Bilişim*, *1*(1), 194-197.

Güldüren, C., Çetinkaya, L., & Keser, H. (2016). Ortaöğretim öğrencilerine yönelik bilgi güvenliği farkındalık ölçeği (BGFÖ) geliştirme çalışması. *İlköğretim Online, 15*(2). 682-695

Hazar, E. (2018). Information, media and technology skills competency scale: a validity and reliability study. *Journal of Human Sciences, 15*(2), 1306-1316.

Jordaan, Y., & Van Heerden, G. (2017). Online privacy-related predictors of facebook usage intensity. *Computers In Human Behavior, 70*, 90-96.

Kalaman, S. (2017). Yeni medya ve mahremiyetin dönüşümü: facebook Türkiye örneği. *Uluslararası Hakemli İletişim ve Edebiyat Araştırmaları Dergisi, 14*(1),1-19.

Kara, M. (2013). *Siber Saldırılar – Siber Savaşlar ve Etkileri*. (Yayınlanmamış Yüksek Lisans Tezi). İstanbul Bilgi Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul

Karaarslan, E., Eren, M. B., & Koç, S. (2014). *Çevrimiçi Mahremiyet: Teknik ve Hukuksal Durum İncelemesi*. Türkiye'de İnternet Konferansı Bildirisi, İzmir.

Karakaya, A. (2014), *Yeni İletişim Ortamları ile Sömürgeciliğin Dönüşümü Gözetim Olgusu ve Bireylerin Farkındalık ve Teslimiyetleri Üzerine Bir Araştırma*. (Yayımlanmamış Yüksek Lisans Tezi). Marmara Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul.

Karslıoğlu, F. (2014). *Toplumsal Denetim Aracı Olarak İnternetin Dönüşümü*. (Yayınlanmamış Yüksek Lisans Tezi). İstanbul Bilgi Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul

Kayes, I., & Iamnitchi, A. (2017). Privacy and security in online social networks: A survey. Online Social Networks and Media, 3, 1-21.

Keser, H., & Güldüren, C. (2015). Bilgi güvenliği farkındalık ölçeği (BGFÖ) geliştirme. *Kastamonu Eğitim Dergisi, 23*(3), 1167-1184.

Kline, R. B. (2015). *Principles and practice of structural equation modeling*. New York*:* The Guilford Press.

Korkmaz, Ö., Usta, E., & Kurt, İ. (2014). Sanal ortam yalnızlık ölçeği (SOYÖ) geçerlik ve güvenirlik çalışması. *Hacettepe Üniversitesi Eğitim Fakültesi Dergisi, 29*(29-2), 144-159.

Mıhçı, P., & Çakmak, E. K. (2017). Öğrenci siber sağlık ölçekleri geliştirme çalışması. *Gazi Üniversitesi Gazi Eğitim Fakültesi Dergisi, 37*(2), 457-491.

Milne, G. R., Rohm, A. J., & Bahl, S. (2004). Consumers' protection of online privacy and identity. *Journal of Consumer Affairs, 38*(2), 217-232.

Okumuş, M., & Atilgan, S. S. (2021). Üniversite Öğrencilerinin Dijital Okuryazarlık Becerileri ile Dijital Mahremiyet Kaygısı Arasındaki İlişki. TRT Akademi, 6(12), 342-363.

Okur, E. ve Yalçın-Özdilek, Ş. (2013). Enerjinin etkin kullanımı ve teknolojik kirlilik farkındalık ölçeği. *Kastamonu Eğitim Dergisi, 21*(1), 271-286.

Osborne, J. W., Costello, A. B., & Kellow, J. T. (2014). *Best practices in exploratory factor analysis*. Louisville, KY: CreateSpace Independent Publishing Platform.

Strauss, J., & Rogerson, K. S. (2002). Policies for online privacy in the united states and the european union. *Telematics And Informatics, 19*(2), 173-192.

Şimşek, Ö.F. (2007). *Yapısal Eşitlik Modellemesine Giriş*. Ekinoks Yayınevi. Ankara, 18-71.

Taddicken, M. (2014). The 'privacy paradox'in the social web: the impact of privacy concerns, individual characteristics, and the perceived social relevance on different forms of self-disclosure. *Journal Of Computer-Mediated Communication, 19*(2), 248-273.

Taşdelen, B., & Çataldaş, İ. (2017). Üniversite öğrencilerinin sosyal medya ve mahremiyete yönelik görüşleri: Lefke Avrupa Üniversitesi örneği. *Gümüşhane Üniversitesi İletişim Fakültesi Elektronik Dergisi, 5*(2), 826-844.

Tokgöz, C. (2011), *Bilişim Çağında Toplumsal Denetim Aracı Olarak Gözetim Olgusu ve Yeni İletişim Ortamlarında Bireyin Gözetim Farkındalığı Üzerine Bir Araştırma*. (Yayımlanmamış Yüksek Lisans Tezi). Marmara Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul.

Topbaş, H., & Gazi, M. A. (2016). Sosyal ağlarda gizlilik kaygısının ölçülmesi: İnönü Üniversitesi öğrencilerine yönelik bir araştırma. *İnönü University International Journal Of Social Sciences (Inijoss), 5*(1 (9)), 143-160.

Türk Dil Kurumu (2019). http://sozluk.gov.tr

Wu, Y., Lau, T., Atkin, D. J., & Lin, C. A. (2011). A comparative study of online privacy regulations in the US and China. *Telecommunications Policy, 35*(7), 603-616.

Yıldız, A. K. (2012), Sosyal paylaşım sitelerinin dijital yerlilerin bilgi edinme ve mahremiyet anlayışına etkisi, *Bilgi Dünyası, 13*(2), 529-542.

Yılmaz, E. (2015). *Öğretmenlerin Dijital Veri Güvenliği Farkındalığı* . (Doktora Tezi). Anadolu Üniversitesi, Eğitim Bilimleri Enstitüsü, Eskişehir.

Yüksel, M. (2003), Mahremiyet hakkı ve sosyo-tarihsel gelişimi, *Ankara Üniversitesi SBF Dergisi*, 58(1), 181-213.