

“KİŞİSEL VERİLERİN GİZLİLİĞİ FARKINDALIK ÖLÇEĞİ” GELİŞTİRME ÇALIŞMASI

Mehmet Ercüment ARI¹

Özhan TINGÖY²

¹Doktora Öğrencisi, Marmara Üniversitesi, ercument.ari@gmail.com, ORCID: 0009-0009-5910-780X

²Prof. Dr., Marmara Üniversitesi, Üniversitesi, otingoy@marmara.edu.tr, ORCID 0000-0003-0402-5371

Arı, Mehmet Ercüment ve Özhan Tıngöy, “Kişisel Verilerin Gizliliği Farkındalık Ölçeği Çalışması”. ulakbilge, 95 (2025/4): s. 265-282. doi: 10.7816/ulakbilge-13-97-04

ÖZ

Bu çalışmada, geçerli ve güvenilir bir kişisel verilerin gizliliği farkındalık ölçeği geliştirilmesi amaçlanmaktadır. Çalışma karma yöntem araştırmasına dayalı keşfedici sıralı karma desenle yürütülmüştür. Araştırmanın katılımcılarını devlet ve vakıf üniversitelerinin farklı sınıf düzeylerinde ve farklı bölümlerinde öğrenim gören 704 üniversite öğrencisi oluşturmaktadır. Çalışmaya ait taslak formun oluşturulması amacıyla konuya ilişkin alan yazın taranmış ve alan uzmanı araştırmacılar tarafından 33 maddelik bir soru havuzu hazırlanmıştır. Uzman görüşleri alınan ve pilot uygulaması yapılan taslak forma son şekli verilerek esas uygulamaya geçilmiştir. Esas uygulama sonrasında elde edilen veriler SPSS ve LISREL istatistik programları kullanılarak çözümlenmiştir. Veri analizi sırasında yapı geçerliliğinin sağlanması için açımlayıcı ve doğrulayıcı faktör analizleri gerçekleştirilmiştir. Ölçeğin güvenilirliğin ölçülmesi Cronbach alpha iç tutarlık katsayısı ile hesaplanmıştır. Ayrıca ölçeğe ait toplam madde korelasyon değerleri ve ayırt edici geçerlilik değerleri de hesaplanmıştır. Doğrulayıcı faktör analizi bulguları ölçeğin beş faktörlü bir yapıya sahip olduğu, uyum indekslerinin kabul edilebilir (AGFI=0,82 ve GFI=0,85) ve mükemmel ($\chi^2/sd=2,36$, NFI=0,96, CFI=0,97, IFI=0,97, RMR=0,06 ve RMSEA=0,07) düzeyde uyumu gösterdiğini ortaya koymuştur. Araştırma sonucunda Cronbach alpha iç tutarlık katsayısı 0,75 olan 26 maddeden oluşan beşli likert tipte bir "Kişisel Verilerin Gizliliği Farkındalık Ölçeği" geliştirilmiştir. Araştırma sonuçları, geliştirilen ölçeğin uygulanabilecek geçerli ve güvenilir bir ölçme aracı olarak kullanılabileceğini ortaya koymaktadır.

Anahtar Kelimeler: Kişisel verilerin korunması, farkındalık, kişisel veri, mahremiyet, ölçek, üniversite öğrencileri,

Makale Bilgisi:

Geliş: 14 Mart 2024

Düzeltilme: 9 Ağustos 2024

Kabul: 9 Eylül 2024

Giriş

Günümüz internet ortamına bağlı bilgi ve iletişim teknolojilerinin baş döndürücü gelişmeleri, kişisel verilerin toplanması ve farklı metotlarla analiz edilmesi noktasında ciddi ölçüde destek sağlamıştır (Özkaya ve Toprak, 2022). İlerleyen teknoloji ve yaygınlaşan internet ağı, bireylerle ilişkili bilgi akışını ve bilgiye erişimi önemli ölçüde kolaylaştırmıştır (Çelik, 2017). Bilgi türlerinin ve şekillerinin değiştirilmesiyle oluşabilecek riskleri değişikliğe uğratmıştır (Çetin, 2014). Mobil internet ağları ve akıllı cihazların artan kullanımları dünya çapında kullanıcılara ait konum ve özel bilgilerin toplanarak kullanılması ihtimalini arttırıcı bir etken yaratmıştır (Alfnes ve Wasenden, 2022; Dinler ve Çalışkan, 2019). Dijitalleşme, küresel ağın farklı noktalarında depolanan bilgiler ve kişisel verileri düzensiz erişimle; bilgi güvenlik ve gizliliği ilkelerini ihlal riskini oluşturmuştur (Romansky ve Noninska, 2020). Dolayısıyla içerisinde yer aldığımız bu dijital dönem kişisel mahremiyetin korunmasında birçok zorluğu beraberinde getirmiştir (Shariff, Green ve Jettinghoff, 2021; Yajive Bayyapu, 2021). Bu dijital gelişim kişisel verilerin ihlal edilme tehlikesi (Bilir, 2020), kişisel verilerin güvenliği konusunda bireyleri endişelendirmiştir. Popüler medyada veri gizliliği tetikleyici bir konu haline gelmiş, gizlilik sorunlarına ve dijital haklara odaklanan raporlar çoğalmıştır (Calzada, 2022). Günümüzde kişisel verilerin gizliliğinin korunması, farklı alanlardaki veri sahipleri tarafından vazgeçilmez bir gereklilik haline gelmiştir (Majeed ve Hwang, 2023).

Kişisel veri; bilginin gerçek bir bireye ait olması ve bireyin belirli veya belirlenebilir olması unsurlarıyla yapısal olarak tanımlanmaktadır. Ayrıca bireylerin sosyal, ekonomik ve kültürel durumuna yönelik nesnel veya öznel bilgi niteliğinde olmalıdır (Genç, 2019). Heterojen yapıya sahip olup insanlarla ilgili verilerdir (Arınmış Uzun, 2021). Oğuz (2018) tarafından ise bir kişiyi belirlenebilir hale getiren her türlü kişisel bilgi olarak açıklanmaktadır. Örneğin vergi no, yaş, meslek, adres, kart bilgileri gibi bilgileri olarak kabul edilmektedir (Turan, 2015). Kişisel veriler, hassas kişisel veriler ve hassas olmayan kişisel veriler biçiminde iki grupta incelenebilmektedir. Hassas kişisel veriler, öğrenilmesi durumunda veri sahibine yönelik ciddi riskler oluşturabilecek ve bu nedenle özel koruma gerektiren önemli bilgileri kapsamaktadır. Bunun aksine hassas olmayan veriler ise genel geçer bilgiler olup, ortaya çıkılması durumuyla zarar oluşturmamaktadır. Öğrenilmesi durumunda tek başına veri sahibini tehdit etmeyen ve mağduriyet yaşatmayan nitelikte verileri içermektedir. Fakat bu ikilik ülkeler arasında veya bireyler arasında değişiklik göstermektedir (Arınmış Uzun, 2021; Genç, 2019; Shukur ve Fatlawi, 2022).

Yaşantımızın önemli bir parçası olma rolünü üstlenen yapay zekâ teknolojilerinin bireyler hakkında farklı veriler toplayıp bazı çıkarımlarda bulunması, kişisel verilerin korunması noktasında büyük riskler yaratmaktadır (Abudureyimü ve Oğurlu, 2021). Resim, video ve sesler aracılığıyla birbiriyle iletişime geçip, çevrimiçi olarak haberleşmede sosyal ağlar kullanılmaktadır (Cheung, Chiu ve Lee, 2011). Facebook, Twitter, Youtube gibi sosyal ağlarla bireylerin etkileşimlerine ait veriler elde edilmektedir (Nagy ve Pecho, 2009). Bireylerin bilinçli veya bilinçdışı kimliklerini tespit etme, profil oluşturma işlemlerini kolaylaşmaktadır (Eryılmaz, 2023). Bu durum sosyal medya kullanıcılarının diğer sosyal medya kullanıcısı bireylerden kişisel bilgilerini saklaması (Çakır, Özudoğru, Bozkurt ve Hava, 2015) gerekliliğini öne çıkarmaktadır. Kullanıcıların profillerinden paylaşılan bilgi ve fotoğrafların herkes tarafından görülebilmesi veya erişilebilmesi, özel yaşamın korunmasında bazı riskleri barındırmaktadır (Kılınç, 2012). Sosyal ağ siteleri kullanıcılarının kendi iradeleriyle yaptıkları paylaşımlarının başka kullanıcılar tarafından saldırı niteliğinde ele geçirilip farklı amaçlarla kullanılması (Atasoy, 2016), bireylerin kendi mahremiyetlerini kırarak farklı tehlikelere maruz bırakmaktadır (Kumar, Saravanakumar ve Deepa, 2016). Özetle hayatımızın kilit noktası haline gelen yapay zekâ, web uygulamaları ve sosyal medya araçları teknolojiler kişisel mahremiyetin sağlanması açısından ciddi problemleri ortaya çıkarmaktadır. Öte yandan çevrimiçi ortamda yapılan bankacılık, ticari, alışveriş, vatandaşlık işlemleri kişisel bilgilere yönelik gizlilik ve mahremiyet sorunlarını öne çıkarmaktadır (Eroğlu, 2018).

Köksalan (2022) dijitalleşmeyle beraber bireylerin kendilerine ait sosyal alanlarındaki mahremiyet dengesini sekteye uğrattığını vurgulamıştır. Bu durum ise bireylerin özel hayatın gizliliği ilkesini ihlal edici ve modern devlet yapısında hak ve özgürlüklerin korumasına yönelik güncel tartışmaları ortaya çıkarmaktadır (Özkaya ve Toprak, 2022). Hukuki açıdan bazı güvenlik tehditleri beraberinde getirmiş, kişisel veriler özel hayatın gizliliğinin korunması noktasında insan haklarıyla yakından ilişkilendirilmiştir (Çelik, 2017). Dolayısıyla kişisel verilerin korunması hakkı modern toplumlarda bireylerin en önemli haklarından biri haline gelmiştir. Özellikle dijital çağda kişisel verilerin korunması hakkı daha büyük önem kazanmış ve kritik hale gelmiştir. Dülger (2018) tarafından kişisel verilerin korunması hakkı, veri sahiplerinin veriler üzerindeki hakimiyeti temsil eder; verilere ulaşılması, verilerin toplanması ve aktarılması hususlarında söz hakkı taşımasını ifade etmektedir. Kişisel verilerin korunması, birçok ülkenin anayasal düzenlemeleri veya yasal süreçleri aracılığıyla güvence altına alınmıştır. Bu haklar genellikle temel insan hakları kapsamında ele alınmakta ve anayasal düzenlemelerle desteklenmektedir. Avrupa Birliği veri koruma düzenlemesinde

verilerin korunması iki temel ilke bireylerin bir sözleşmeye bağlı olmadan kişisel verilerine her daim sahip oldukları ve kontrol altına aldıkları kabul etmektedir. Ancak açık rıza (veri katılımı), unutulma (veri) hakları silme ve taşınabilirlik (veri aktarımı) üç kritik gizlilik hakkını ihlal etmektedir (Keve Sudhir, 2023).

Dijitalleşme çağ kişisel verilerin korunması ihtiyacını hukuk sistemleri süzgecinden geçirilerek temel bir insan hakkı olarak kabul görülmüştür. Buna bağlı olarak ise ülkeler kişisel verilerin korunmasına yönelik kanunları yürürlüğe koymaya başlamıştır (Bilir, 2023). Kişisel verilerin korunması hakkı; Anayasa’nın 20. maddesi ve Avrupa Birliği Temel Haklar Bildirgesi 8. maddesi içeriğinde temel bir hak olarak değerlendirilmektedir (Oğuz, 2018). İlk aşamada 2004 yılında kabul edilip 2005 yılında yürürlüğe konulan 5237 sayılı Türk Ceza Kanunu 135. ve 140. maddeleri düzenlemelerinde özel hayatın gizliliği vurgulanarak kişisel verilerin korunmasına ait yansımalar görülmektedir (Kart ve Ketizmen, 2019). 2010 Türkiye Cumhuriyeti Anayasa değişikliğiyle özel hayatın gizliliğini düzenleyen maddeye ek olarak ilk defa kişisel verilerin esasına ait içeriğe yer verilmiştir. Kişisel verilerle ilişkili maddeler sonrasında, kişisel verilerin işlenmesi ve korunmasına ilişkin temel düzenlemeler, 2016 tarihinde 6698 sayılı Kişisel Verileri Koruma Kanunu (KVKK) yürürlüğe konularak, ülkemizde yeni bir çağa giriş yapıldığı açıklanabilir. Benzer biçimde 08 sayılı “Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması” Avrupa Konseyi Sözleşmesi içeriğinde de yer almaktadır (Atlı, 2019). Böylelikle kişilere ait verilerin şeffaflığının korunması, güvenliğinin sağlanması, veri sahiplerinin haklarının korunması yasal biçimde amaçlanmıştır.

Dijital uygulamalar üzerinden gerçekleştirilen her bir işlem kişisel verilerimize ait bilgileri aktarmamıza araç görevi görmektedir. Farklı işlemlerle aktardığımız verilerin gizliliğinin ve güvenliğinin sağlanması son derece büyük bir önem taşımaktadır. Günümüz dünyasında öne çıkan sorunlardan biri olarak algılanan veri gizliliğinin değerlendirilmesi ve topluma ait her kesimin farkındalık kazanması gerekliliği kaçınılmazdır (Eroğlu, 2018). Bireylerin gereksiz bilgi paylaşımı yapmamaları, şifrelerini vermemeleri, web sitelerinin güvenilirliğini kontrol etmeleri, gerekli koruma yazılımlarını kullanmaları gibi sayılabilecek birçok veri koruma farkındalığına sahip olmaları atılabilecek adımlar arasındadır. Kişisel verilerin korunması öncelikli olarak bireylerin sorumluluğundadır. Bireylerin mahremiyetlerini çevrimdışı hayatta olduğu üzere çevrimiçi dünyada denetlettirmesini ve gizliliklerinin risk altında olduğunun farkında olmalarını gerekli kılmaktadır (Köksalan, 2022). Çevrim içi platformlarda büyük oranda zaman harcayan kullanıcıların kişisel bilgilerini daha fazla paylaşması mahremiyet açısından beklenen hassasiyete sahip olmadıkları çıkarımı yapılmaktadır (Sevinç, 2018). Bu noktada benzer biçimde bireylerin gereken hassasiyeti göstermelerine yönelik farkındalık oluşturmaları kaçınılmaz olacaktır.

Çevrimiçi ağlarda olası tehlikelerin farkın varılması ve ihtiyaç duyulan önlemlerin alınması şarttır. Dolayısıyla da sosyal medya kullanıcılarının bilinçli veri paylaşımı yetkinliği kazandırılmasına ve etkin bir kullanıcı olması eğilimi göstermeleri yönünde teşvik edici olunmasına işaret edilmektedir. Bireylerin kişisel verilerin korunmasına ait duyarlılık oluşturmaları ve farkındalık kazanmaları ancak onlara verilebilecek bir bilinç eğitimiyle sağlanabilir. Verilebilecek öğretimin tasarlanmasında ve planlanmasında ise uzmanlara yol haritası olabilmesi açısından durum tespiti yapılması ön koşullar arasındadır. Bireylerden alınabilecek geri dönüşler, ihtiyaca uygun bir eğitim zemini hazırlanmasında etkili olabilecektir. Dolayısıyla kişisel verilerin gizliliğine yönelik bir farkındalık ölçeği geliştirilmesinin, araştırmacı ve eğitimciler açısından da faydalı olabileceği, alan yazına katkı sağlayacağı düşünülmüştür. Buradan hareketle, çalışmada üniversite öğrencilerine yönelik bir “*Kişisel Verilerin Gizliliği Farkındalık Ölçeği*” geliştirilmesi amaçlanmış ve belirlenen araştırma sorularına aşağıda sırasıyla yer verilmiştir:

- ✓ Geliştirilen “Kişisel Verilerin Gizliliği Farkındalık Ölçeği” geçerli sonuçlar vermekte midir?
- ✓ Geliştirilen “Kişisel Verilerin Gizliliği Farkındalık Ölçeği” güvenilir sonuçlar vermekte midir?

Yöntem

Araştırmanın Deseni

Araştırma karma araştırma yöntemlerinden keşifsel sıralı tasarım desenine dayandırılarak yürütülmüştür. Keşfedici sıralı tasarım deseninden, bir ölçme aracının geliştirilmesi sürecinde yararlanılabilmektedir. Keşifsel sıralı tasarım desen; nitel verilerin toplandıktan sonra analiz edilmesi, bir ölçme aracı ortaya koyulmasını, ölçme aracıyla nicel verilerin toplanıp analiz edilmesi ve yorumlanmasına dayandırılmaktadır. Bu desende araştırmacı önce verilerini toplar, ölçme aracını hazırlar, seçeceği örneklem üzerinde bu aracı uygular ve analiz eder (Creswell ve Creswell, 2021). Bu süreç doğrultusunda; ilk aşamada alan yazından yola çıkılarak soru havuzu hazırlanmış, ölçme aracı taslak forma dönüştürülmüş, uygun bir örnekleme uygulanmıştır ardından ise geçerlilik ve güvenilirlik katsayısı hesaplamalarından yararlanılmıştır.

Verilerin Toplanması

Araştırmanın çalışma grubunu İstanbul İlinde yer alan devlet ve vakıf üniversitelerinde öğrenim gören üniversite öğrencileri oluşturmaktadır. Araştırma katılımcıları, 5 farklı üniversitede 2020-2021 öğretim yılında öğrenimine devam eden toplam 704 üniversite öğrencilerinden meydana gelmektedir. Katılımcı üniversite öğrencilerinin; 216'sı erkek ve 488'i kadın öğrencilerden oluşmaktadır. Öğrencilerin yaşı en düşük 17 ve en yüksek 52 olup, yaş ortalaması ise 22'dir.

Katılımcılar amaçlı örnekleme yöntemlerinden kolay ulaşılabilir durum örnekleme türünden yararlanılarak belirlenmiştir. Kolay ulaşılabilir durum örneklemesinde araştırmacı yakın olan ve erişilmesi kolay olan bir durumu seçer. Bu yöntem araştırmaya hız ve pratiklik kazandırır. Ayrıca bu yöntemin maliyeti de diğer yöntemlere göre daha azdır (Yıldırım ve Şimşek, 2018). Örneklem büyüklüğünün, ölçek madde sayısının en az 10 katı kadar olması gerektiğini vurgulanmıştır (Büyüköztürk, 2002; Costello ve Osborne, 2005; Yaşlıoğlu, 2017). Ölçekte yer alan soru sayısı göz önüne alındığında; çalışma grubunun açılımlayıcı faktör analizi için 329 ve doğrulayıcı faktör analizi için 274 katılımcıdan meydana gelmesi yeterli düzeyde katılımcıya ulaşıldığının göstergesidir.

Açılımlayıcı faktör analizi katılımcı öğrencilerin 263'ü kadın ve 66'sı erkektir. Öğrencilerin 118'i 1. sınıf, 75'i 2. sınıf, 110'u 3. sınıf ve 26'sı 4. sınıf öğrencisidir. Öğrencilerin 15'i sosyal bilgiler bölümünde 100'ü BÖTE bölümünde, 30'u İngilizce bölümünde, 52'si matematik bölümünde ve 132'si fen bilgisi bölümünde öğrenim görmektedir. Doğrulayıcı faktör analizi katılımcı öğrencilerin 199'u kadın ve 75'i erkektir. Öğrencilerin 181'i 1. sınıf, 33'ü 2. sınıf, 12'si 3. sınıf ve 48'i 4. sınıf öğrencisidir. Öğrencilerin bölümlere dağılımı incelendiğinde ise; sosyal bilgiler bölümde 45, BÖTE bölümde 153, İngilizce bölümde 34, matematik bölümde 14, psikolojik danışma ve rehberlik bölümde 5 ve fen bilgisi bölümde 23 öğrenci yer almaktadır.

Veri Toplama Aracının Geliştirilmesi ve Planlama Aşaması

Veri toplama aracının geliştirilmesi sürecine ait basamaklar alan yazında çalışmaları dikkate alınarak şekillendirilmiştir (Acar Güvendir ve Özer Özkan, 2022; DeVellis, 2022; Seçer, 2018; Şeker ve Gençdoğan, 2014). Mevcut ölçek geliştirme sürecine ait basamaklara Şekil 2'de yer verilmiştir.



Şekil 2. Kişisel Verilerin Gizliliği Farkındalık Ölçeğinin Geliştirilme Sürecine Ait Basamaklar

Şekil 2 incelendiğinde, kişisel verilerin gizliliği farkındalık ölçeğinin geliştirilmesine yönelik olarak gerçekleştirilen araştırmaya ait basamaklar görülmektedir. Basamakların her biri sırasıyla açıklanmaktadır.

Ölçek İhtiyacının Belirlenmesi: Gerçekleştirilen alan yazın taraması sonrasında kişisel verilerin gizliliği farkındalık ölçeğine ulaşılamamıştır ve ölçme aracının geliştirilmesine karar verilmiştir.

İlgili Literatürün İncelenmesi ve Çalışmaların İncelenmesi: Geliştirilmesi karar verilen ölçeğin konu alanına ait derin bir biçimde gerçekleştirilen alan taraması sonrasında elde edilen kaynaklar taranmıştır. Kişisel verilerin

gizliliği ve korunmasına ait yer alan makale, tez ve bildiriler incelenmiştir. Ayrıca konu alanına yönelik ölçme araçları irdelenmiştir ve konuya ilişkin içerikler de gözden geçirilmiştir.

Madde Havuzunun Oluşturulması: İncelenen literatür sonrasında alan bilgi ve iletişim teknolojileri, eğitim bilimleri, eğitim hukuku, dijital suçlar ve yazılım alanlarında uzman araştırmacılar tarafından 33 maddelik bir madde havuzu hazırlanmıştır. Güvenlik, paylaşım, endişe vb. koby başlıklarıyla ilişkili madde havuzu oluşturulmuştur.

Kapsam ve Görünüş Geçerliliğinin Sağlanması: Madde havuzu hazırlandıktan sonra uzman görüşüne başvurulmuştur. Hazırlanan maddelerin konu ile ilişkisi, kapsam düzeyi, ilave edilmesi ya da ölçekten çıkarılması gereken madde olup olmadığının incelenmesi istenmiştir. Ayrıca ölçek maddelerinde binişik, konu ile ilgili olmayan, açık ve anlaşılabilirlik açısından ölçek maddelerinin incelenmesi sağlanmıştır. Uzman incelemesi neticesinde ölçek maddelerinde her hangi bir düzeltmeye gidilmemiştir. Uzmanlardan yeni madde ekleme ya da çıkarılmasına dair dönütler alınmamıştır. Bununla beraber dil ve anlatım açısından kontrolleri sağlanmıştır.

Pilot Uygulamanın Gerçekleştirilmesi ve Taslak Formun Ortaya Konulması: 33 maddelik kişisel verilerin gizliliği farkındalık ölçeği taslak formu; 5= Tamamen Katılıyorum, 4= Katılıyorum, 3= Kararsızım, 2= Katılmıyorum ve 1= Tamamen Katılmıyorum olmak üzere 5'li likert olarak derecelendirilmiştir. Ayrıca ölçeğe ait amaç ve bilgileri açıklayan kısa ve öz bir yönerge taslak forma eklenmiştir. Uzman görüşü neticesinde şekillenen ve son kontrolleri sağlanan ölçek formu hedef kitleyi karşılayabilecek 5 üniversite öğrencisine yüz yüze uygulanarak ölçek maddelerinin anlaşılabilirliği, okunurluğu açısından denetlenmiştir. Öğrencilerin yüz yüze yapılan cevaplama işleminde de her hangi bir düzeltme işlemine gidilmemiştir.

Son Halini Alan Taslak Formun Esas Uygulamasının Yapılması: Pilot uygulaması gerçekleştirilen ve son değerlendirmeleri yapılan taslak form 704 üniversite öğrencisine uygulanarak, ölçeğin esas uygulaması gerçekleştirilmiştir.

Açımlayıcı ve Doğrulamalı Faktör Analizlerinin Gerçekleştirilmesi: Ölçeğe ait faktörlerin ve faktör yapısının ortaya konulması amacıyla açımlayıcı faktör analizi; ortaya konulan yapının doğrulanması amacıyla doğrulamalı faktör analizi yapılmıştır.

Güvenirlik Analizlerinin Gerçekleştirilmesi: Ölçeğe ve ölçekte yer alan her bir alt boyuta ait cronbach alpha kat sayısı değeri hesaplanarak, ölçeğin güvenilirliği ortaya konulmuştur.

Veri Toplama Aracı ve Veri Toplama Süreci

Araştırma kapsamında nicel veri toplama aracı olarak "Kişisel Verilerin Gizliliği Farkındalık Ölçeği" taslak formu aracılığıyla veri toplama işlemi gerçekleştirilmiştir. Çalışma verilerinin elde edilme süreci, katılımcı üniversite öğrencileriyle çevrim içi bir ortamda tamamlanmıştır. Veriler google form biçiminde e-posta ve diğer sosyal medya hesapları aracılığıyla elde edilmiştir. Veriler 2020-2021 eğitim öğretim yılı içerisinde toplanmıştır. Araştırmada veriler hazırlanan ölçek aracılığıyla elde edilmiştir. Formun uygulanma aşamasına geçilmesi öncesinde öğrencilere gereken açıklamalar ve formun doldurulmasına ait bilgilendirmeler yapılmıştır.

Veri Analizi

Çalışma verileri nicel analiz yöntemlerinden yararlanılarak analiz edilmiştir. Öğrencilerden elde edilen veriler, SPSS 24.0 istatistik programına aktarılmıştır. İstatistik programına aktarılan verilerin kontrolü sağlanmış ve istatistiksel analizleri gerçekleştirilmiştir. Anlamlılık sınır değeri olarak 0,05 ($p < 0,05$) kabul edilmiştir. Veri setinin 50 ve üzeri bir değerde olması nedeniyle verilerin normal dağılımlarının incelenmesinde Kolmogorov-Smirnov Testi uygulanmıştır (Can, 2020; Seçer, 2017).

Ölçeğe ait yapı geçerliliğinin sağlanması ve ölçekte yer alabilecek maddelere karar verilmesi amacıyla faktör analizi yapılmıştır. Faktör analizi aşamasına geçilmeden önce ise Kaiser-Meyer-Olkin (KMO) ve Barlett testi yapılarak verilerin faktör analizine uygunluğu kontrol edilmiştir (Büyüköztürk, 2019). Açımlayıcı Faktör Analizi (AFA) ölçeğin faktör yapısını belirlemek için uygulanmıştır. AFA, birbiri ile ilişkili çok sayıda maddeyi tipik yapı ya da faktörler altında birleştirmeye imkân verir. Faktör analizi bütün değişkenlerin birbiri ile belli bir dereceye kadar ilişkili olması varsayımına dayandığı dikkate alınarak (Colton ve Covert, 2007), bu çalışmada herhangi bir faktör altında yer almayan, ilişkili olmayan ya da binişik yapıya sahip olan maddeleri belirlemek için uygulanmıştır. Barlett's Testi ve Kaiser-Meyer-Olkin (KMO) testlerinin örneklemin yeterli olduğunu göstermesiyle beraber açımlayıcı faktör analizi gerçekleştirilmiştir. Bu analizde faktör yük değeri 0,40 üzerinde olan maddeler kabul edilmiştir. Ayrıca, döndürme işlemi yapılarak birden fazla faktöre ait maddelerin faktörler arasındaki yük farkının en az 0,10 olduğu maddeler ölçekten çıkarılmıştır (Büyüköztürk, 2019; Şeker ve Gençdoğan, 2014). Analizler sonucunda, ölçekten toplamda 7 maddenin çıkarılması uygun bulunmuştur.

Açımlayıcı faktör analizinin tamamlanması sonrasında, faktör yükleri ve alt boyutlarının doğrulanması amacıyla doğrulamalı faktör analizi aşamasına geçilmiştir. Kişisel Verilerin Gizliliği Farkındalık Ölçeği'nin (KVGFO) AFA sonucunda toplam 26 maddenin 5 faktör yapısına sahip olduğu belirlenmiştir. Söz konusu ölçeğin faktör yapılarının doğruluğunu test etmek amacı ile Doğrulamalı Faktör Analizi (DFA) yapılmıştır. DFA, önceden belirlenen bir model aracılığı ile gözlenen değişkenlerden yola çıkarak gizil değişken (faktör) oluşturmaya oluşturulmuş bir faktör yapısını belirlemeye yönelik bir işlemdir (Bayram, 2010; Büyüköztürk, Şekercioğlu ve

Çokluk, 2014). Dolayısı ile DFA belirlenen ölçütler çerçevesinde AFA ile ortaya konulan modeli test etmek ve uygunluğu sınamak amacı ile kullanılmıştır. İkinci örneklem grubundan elde edilen veri seti, LISREL programına aktararak doğrulayıcı faktör analizi gerçekleştirilmiştir. Bu analiz sonucunda, ölçek maddelerinin faktör yükleri ve uyum indeksleri doğrulanmış, ölçeğin tamamı ve alt boyutları için Cronbach alpha iç tutarlılık katsayısı hesaplanarak ölçeğin güvenilirlik değerine bakılmıştır. Ayrıca ölçeğin ölçmeye yöneldiği yapıyı ölçüp ölçmediğine ilişkin yapı geçerliğini yukarıda açıklanan faktör analizlerinin yanı sıra yakınsama ve ıraksama geçerliğinin bir başka versiyonu olan ayırt edici geçerlilik kullanılarak belirlenmeye çalışılmıştır.

Araştırma Etik Süreci

Araştırmanın etik süreciyle ilgili olarak, katılımcılara araştırmanın bilimsel amaçla kullanılacağı, verilerin gizliliğinin korunacağı bilgisi verilmiştir. Araştırmaya katılım sağlayan üniversite öğrencilerine çalışma amacı, gerçekleştirilme nedeni ve verecekleri cevapların nerede kullanılacağı hakkında açık bir biçimde bilgilendirme yapılmıştır. Ayrıca öğrenci adları ve soyadları gizli tutulmuş ve kodlama metodundan yararlanılmıştır. Gerçekleştirilen araştırma çerçevesinde, üniversite akademik etik kurulundan olan yasal izinler alınmıştır.

Bulgular

Açımlayıcı faktör analizine uygunluğu ve örneklem büyüklüğünün yeterli olduğunun gösterilmesi amacıyla öncelikle KMO (Kaiser-Meyer-Olkin Measure of Sampling Adequacy) ve Bartlett Küresellik Test değeri incelenmiştir ve analiz sonuçları Tablo 1’de sunulmuştur.

Tablo 1. KMO ve Bartlett Küresellik Testi Analiz Sonuçları

Kaiser-Meyer-Olkin		,823
Bartlett	Ki-Kare	4510,818
Küresellik	sd	528
Testi	p	,000

Tablo 1 incelendiğinde, veri setine ait KMO (Kaiser-Meyer-Olkin Measure of Sampling Adequacy) ve Bartlett Küresellik Test sonuçları görülmektedir. Analiz sonucunda toplanan verilerin AFA için yeterliği hakkında bilgi veren KMO değeri 0,823’dür. Bir diğer ölçüm olan Bartlett Küresellik testi (Yaklaşık Ki-Kare=45,818, $p<0,05$) değerinin anlamlı olduğu ve serbestlik derecesinin 528 olarak elde edilmiştir. Elde edilen KMO ve Bartlett testi sonuçları, veri setinin açımlayıcı faktör analizi için uygun olduğuna işaret etmektedir.

Varimax döndürme işleminden yararlanılarak gerçekleştirilen Açımlayıcı faktör analizi sonucunda; **Madde-9** (*Web’de açılan pop-up ekranları zaman kaybettirici olduğundan güvenli bir otomatik teklif ve seçenek kabul etme programı olsa hemen kullanırım.*), **Madde-11** (*İnternet alışverişlerimde; (her seferinde kredi kartı bilgimi girmemek için) bir sonraki alışverişimi hızlı tamamlamak adına, güvenilir olduğumu düşündüğüm sitenin, kredi kartı bilgilerimi kaydetme önerisini kabul ederim.*), **Madde-21** (*Sosyal medya şirketlerinin verilerimi kendi ülkelerinin kuruluşları ile paylaşması, bana sağladıkları fayda ile karşılaştırıldığında önemsizdir.*) ve **Madde-30** (*Bana gönderilen izinsiz mesajlar/e-mailler için şikâyet hakkım olduğumu biliyorum.*) numaralı maddelerin her hangi bir faktör altında yer almadığı belirlenmiştir. Söz konusu 4 madde (**9-11-21-4**) çıkarılarak analize devam edilmiştir.

İkinci analizde **Madde-5** (*Mobil uygulamalarda uygulamayı kullanmak için “kullanıcı sözleşmesi”ni mutlaka okumaya özen gösteririm.*) ve **Madde-31** (*Firmaların hazırladığı “Kişisel Veriler Aydınlatma Metinleri” içeriğindeki taahhütlerin doğruluğuna inanıyorum.*) binişiklik gösterdiği ve **Madde-32** (*Sosyal medya profillerimde yaşadığım mahalleyi/caddeyi paylaşmanın sakıncalı olduğunu düşünmüyorum.*) herhangi bir faktör altında yer almadığı gözlenmiştir. Bahsi geçen bu 3 madde de (**5-31-32**) ölçek taslağından çıkarılmıştır. Gerçekleştirilen analiz sonucunda 5 faktör yapıda bir ölçek ortaya çıkmıştır.

Açımlayıcı faktör analizi sürecinde tabi tutulan veri setine uygulanan döndürme işlemi sonucunda çıkarılan maddelerin ardından, ölçeğe ve ölçek alt boyutlarına ait açıklanana varyans değerleri Tablo 2’de sunulmuştur.

Tablo 2. Ölçek ve Ölçek Alt Boyutlarına Ait Açıklanan Varyans Değerleri

Faktörler	Madde Sayısı	Madde No	Açıklanan Varyans (%)
1	7	10, 17, 18, 19, 22, 23, 24	18,232
2	6	4, 7, 8, 14, 16, 33	11,769
3	6	1, 2, 13, 15, 20, 27	11,676
4	4	3, 6, 12, 25	8,809
5	3	26, 28, 29	8,158
Toplam	26		58,644

Tablo 2 incelendiğinde, açımlayıcı faktör analizi sonucunda çıkarılan maddelerin ardından, açıklanan toplam varyans oranları görülmektedir. Açımlayıcı faktör analizi sonrasında 26 maddeden meydana gelen ve 5 faktör altında gruplanan ölçeğe ait toplam varyansın %58,64'ünü açıklamaktadır. 1. Faktörde 7 madde (Madde No: 10, 17, 18, 19, 22, 23, 24) yer almış ve açıklanan toplam varyans %18.232 olmuştur. 2. faktörde toplam 6 madde (Madde No: 4, 7, 8, 14, 16, 33) yer almıştır. 2. Faktörün açıkladığı toplam varyans %11.769'dur. 3. Faktörde de toplam 6 madde (Madde No: 1, 2, 13, 15, 20, 27) yer almıştır. 3. Faktörün toplam açıkladığı varyans %11.676'dır. 4. Faktörde toplam 4 madde (Madde No: 3, 6, 12, 25) yer almıştır. 4. Faktörün toplam açıkladığı varyans 8.809'dur. 5. Faktörde ise 3 madde (Madde No: 26, 28, 29) yer almakta ve toplam açıklanan varyansın %8.158 olduğu gözlenmiştir. Açımlayıcı faktör analizi süreci sonrasında ölçekte kalan her bir maddenin faktör yükü ve faktörlere dağılımı Tablo 3'te sunulmuştur.

Tablo 3. Maddelerin Faktöre Dağılımı ve Faktör Yükleri

Maddeler	Faktörler ve Madde Yükleri				
	1	2	3	4	5
18- Alışveriş yaparken daha fazla indirim almak için kişisel verilerimi paylaşabilirim.	,857				
24- Özel mesajlarım dışında Facebook hesabıma ait tüm verilerimi iyi bir ücret karşılığında reklam ajanslarına satabilirim.	,829				
23-Oyun içi hediye veya ürünkarşılığı, (sosyal medya hesaplarım da dahil olmak üzere) kişisel bilgilerimi paylaşmaktan çekinmem.	,828				
22- Ünlü bir kişi olmadığım için kişisel verilerimin bilgim dışında paylaşılmasını önemsemem.	,798				
19-Netflix'den bedava yararlanabilmek için kişisel verilerimi paylaşabilirim.	,776				
10- Çağrı merkezi görüşmelerinde Kişisel Verilerin işlenmesi ile ilgili izin teklifleri zaman kaybettirici olduğunu düşündüğüm için hepsini dinlemeden onaylarım.	,728				
17-İnternette pop-up pencereleri ile önüme çıkan çerezler (cookie) hakkında bilgim olmasa da bunlara ilişkin şartları, o hizmeti almak için kabul ediyorum.	,603				
8-Instagramda, tespit edilmemeyi tercih ederim.		,768			
14- Benim kişisel verilerimi alıp kullanan şirketler bu verimi uygun güvenlik tedbirleri ile de koruduğuna inanmıyorum.		,698			
16-Applestore veya Playstore'a üyelik için ön şart olarak kredi kartı bilgilerinin girilmesi beni rahatsız ediyor.		,689			
33- Sosyal medyada profil oluşturabilmek için yaş sınırı olması gerektiğine inanıyorum.		,662			
4- Firmaların Web, Mobil Uygulamaları, mail veya sms gibi yollarla kişisel verilerin işlenmesine ilişkin izin talepleri genellikle beni rahatsız ediyor.		,660			

7-Instagramda storyleri izleyenlerin isimlerinin görülmesi beni rahatsız ediyor.	,582
1- Kişisel verilerin gizliliği benim için önemlidir.	,830
13- Kişisel verilerin korunması ile ilgili ne kadar tedbir alınsa da devletlerin kişilerin her türlü verisine eriştiğine inanıyorum.	,751
20- İnternette alışveriş yaparken ürün fiyatından önce şirketin kişisel veri güvenliği açısından güvenilir olup olmadığı önceliğimdir.	,677
2- Kişisel verilerin gizliliği ile bilgi güvenliği aynı şeydir.	,612
15- Eski bilgisayar veya cep telefonumu birine verirken, atarken, satarken veya elden çıkarırken kişisel verilerimin geri döndürülemeyecek şekilde imha ettiğime emin olurum.	,585
27- Sosyal medyada mahrem olan özel bilgilerin rahatça paylaşıldığını düşünüyorum.	,544
3- Hayatımda en az bir kere mail veya sms yolu ile firmaların kişisel verileri işleme izin taleplerine olumlu veya olumsuz geri dönüş yapmışlığım vardır.	,707
12- Herhangi bir süreç için (örnek iş görüşmesi, vb) gerekli olan kimlik fotokopimi, mail ile istendiğinde gönderirim.	,706
25- Sürekli olarak gittiğim cafe'nin veya spor salonunun bana daha kolay ve güvenli hizmet verebilmesi için biyometrik verilerimi (parmak izi, avuç içi, yüz tanıma vb.) işleme isteğini makul karşılarım.	,660
6-Whatsapp gruplarında her konuda fikirlerimi açıkça paylaşıyorum	,543
29- Toplumda güvenliği sağlamak için özel sektör tarafından, kişileri izleme teknolojisi daha fazla kullanılmalıdır.	,754
28- Toplumda güvenliği sağlamak için devlet tarafından, kişileri izleme teknolojisi daha fazla kullanılmalıdır.	,720
26- Google arama ve konum geçmişimin toplumsal huzuru sağlamak adına devlet(ler) ile paylaşılmasında bir sakınca görmem.	,614

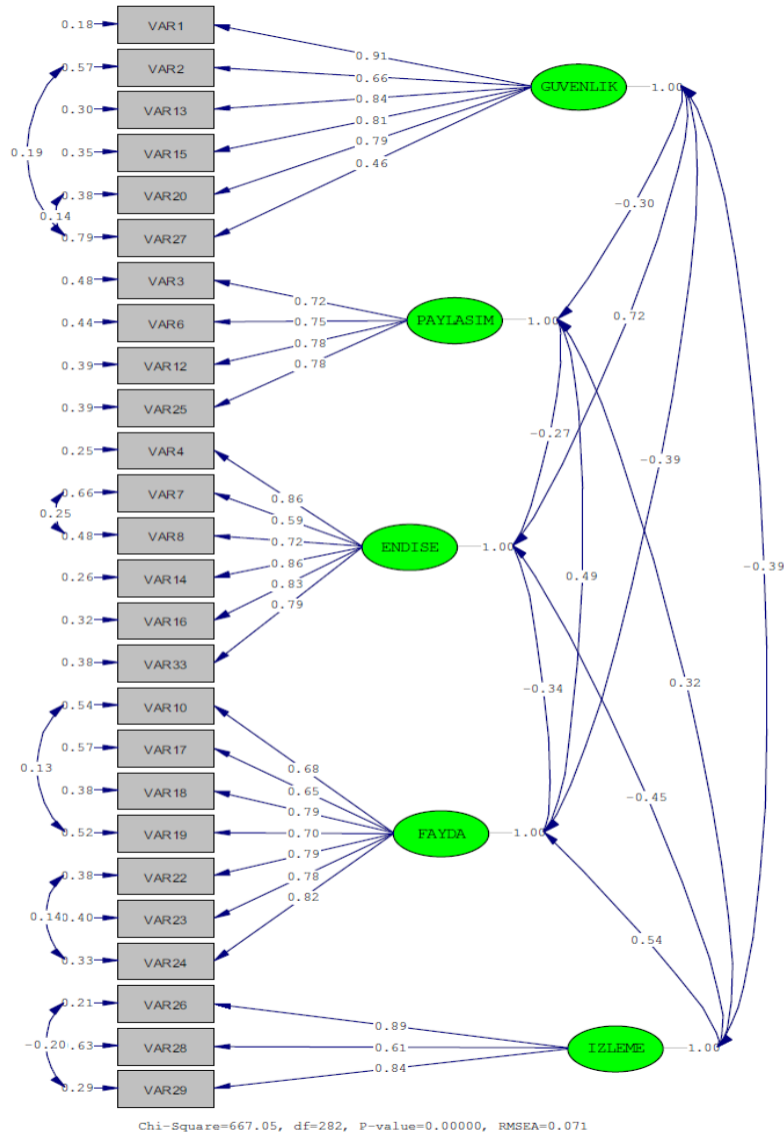
Tablo 3 incelendiğinde, gerçekleştirilen açımlayıcı faktör analizi aşamaları sonucunda ölçekte kalan maddelerin faktörlere dağılımları ve maddelerin yer aldığı faktöre ait yük değerleri görülmektedir. Ölçekte yapılan açımlayıcı faktör analizi sürecinde varimax türü dik döndürme işlemi sonucunda toplam 26 maddenin ölçekte kaldığı anlaşılmaktadır. Ölçekte yer alan maddelere ilişkin faktör yüklerinin 0,543 ve 0,857 değerleri arasındadır. Birinci faktöre ait yüklerinin 0,603 ile 0,857 değerleri arasında, ikinci faktöre ait yüklerinin 0,582 ile 0,768 değerleri arasında, üçüncü faktöre ait yüklerinin 0,544 ile 0,830 değerleri arasında, dördüncü faktöre ait yüklerinin 0,543 ile 0,707 değerleri arasında, beşinci faktöre ait yüklerinin 0,614 ile 0,754 değerleri arasında yer aldığı görülmektedir.

Maddelerin faktör yükleri incelendiğinde; 1. Faktörde en yüksek faktör yükü 0,857 ile "*Alışveriş yaparken daha fazla indirim almak için kişisel verilerimi paylaşabilirim.*" olarak ifade edilen 18. maddeye ait olduğu gözlenmiştir. En düşük faktör yükü ise 0,603 ile "*İnternette pop-up pencereleri ile önüme çıkan çerezler (cookie) hakkında bilgim olmasa da bunlara ilişkin şartları, o hizmeti almak için kabul ediyorum.*" olarak ifade edilen 17. Maddeye aittir. 2. Faktörde en yüksek faktör yükü 0,768 ile "*Instagramda, tespit edilmemeyi tercih ederim.*" olarak ifade edilen 8. Maddeye aittir. En düşük faktör yükü 0,582 ile "*Instagramdastoryleri izleyenlerin isimlerinin görülmesi beni rahatsız ediyor.*" olarak ifade edilen 7. Maddeye aittir. 3. Faktörde en yüksek faktör yüküne sahip madde 0,830 ile "*Kişisel verilerin gizliliği benim için önemlidir.*" şeklinde ifade edilmiş olan 1. Maddeye, en düşük faktör yükü ise 0,544 ile "*Sosyal medyada mahrem olan özel bilgilerin rahatça paylaşıldığını düşünüyorum.*" olarak ifade edilen 27. Maddeye aittir. 4. Faktörde en yüksek faktör yükü 0,707 ile "*Hayatımda en az bir kere mail veya sms yolu ile firmaların kişisel verileri işleme izin taleplerine olumlu veya olumsuz geri dönüş yapmışlığım vardır.*" şeklinde ifade edilmiş olan 3. Maddeye aittir. En düşük ise 0,543 ile "*Whatsapp gruplarında her konuda fikirlerimi açıkça paylaşıyorum.*" şeklinde ifade edilen 6. Maddeye aittir. 5. Faktörde ise en yüksek faktör yükü 0,754

ile “Toplumda güvenliği sağlamak için özel sektör tarafından, kişileri izleme teknolojisi daha fazla kullanılmalıdır.” şeklinde ifade edilen 29. Maddeye aittir. Bu faktörde en düşük faktör yükü ise 0.614 ile “Google arama ve konum geçmişimin toplumsal huzuru sağlamak adına devlet(ler) ile paylaşılmasında bir sakınca görmem.” olarak ifade edilen 26. Maddeye aittir.

Faktörlere dağılan ölçek maddeleri incelendiğinde 1. Faktörde yer alan maddelerin daha çok “Fayda-menfaat-çıkar” elde etme ile ilgili olduğundan bu “Fayda” boyutu olarak isimlendirilmiştir. 2. faktör altında yer alan maddelerin “endişe-sakınca-rahatsızlık duyma” ile ilgili olduğundan “Endişe” olarak adlandırılmıştır. 3. Faktör altında yer alan maddelerin “güvenlik-tedbir” ile ilişkili olduğundan “Güvenlik” olarak isimlendirilmiştir. 4. Faktör altında yer alan maddelerin “başkaları ile paylaşım” ile ilgili olduğundan “Paylaşım” olarak isimlendirilmiştir. 5. Faktör altında yer alan maddeler incelendiğinde ise “izleme-takip” ile ilişkili olduğundan “İzleme” olarak isimlendirilmiştir.

Açımlayıcı faktör analizi gerçekleştirilerek yapı geçerliliği sağlanan ölçeğin doğrulanması amacıyla doğrulayıcı faktör analizlerince önerilen modifikasyonlar yapıldıktan sonramodelin standardize edilmiş şeması ortaya konulmuştur. Maddelere ait elde edilen yük değerlerine ve yol haritasına Şekil 2’de sunulmuştur.



Şekil 2. Doğrulayıcı Faktör Analiz Madde Yükleri Yol Haritası

Şekil 2 incelendiğinde, doğrulayıcı faktör analizinden elde edilen ölçek ifadelerinin yük değerleri görülmektedir. Ölçekte bulunan madde yük değerlerinin 0,46 ve 0,91 değerleri arasında değiştiği anlaşılmaktadır. “Güvenlik” faktörüne ait madde yükler değerleri 0,46 ile 0,91 arasında, “Paylaşım” faktörüne ait madde yük değerleri 0,77 ile 0,78 arasında, “Endişe” faktörüne ait yük değerleri 0,59 ile 0,86 arasında, “Fayda” faktörüne ait

yük değerleri 0,65 ile 0,82 arasında ve **"İzleme"** faktörüne ait madde yükleri ise 0,61 ile 0,89 arasında yer almaktadır.

Standardize edilmiş yol analizi diyagramı detaylı incelendiğinde Güvenlik boyutunda en yüksek faktör yükünün (0,91, $t=18.96$, $p<.05$) 1. Madde en düşük faktör yükünün (0,46, $t=7.77$, $p<.05$) 27. Maddeye ait olduğu gözlenmiştir. Paylaşım alt boyutunda en yüksek faktör yükü (0,78, $t=14.33$, $p<.05$) 12. Maddeye en düşük faktör yükü (0,72, $t=12.87$, $p<.05$) 3. Maddeye aittir. Endişe alt boyutunda en yüksek faktör yükü (0,86 $t=17.41$, $p<.05$) 14. Maddeye en düşük faktör yükü (0,59, $t=10.27$, $p<.05$) 7. Maddeye aittir. Fayda alt boyutunda en yüksek faktör yükü (0,82, $t=15.74$, $p<.05$) 24. Maddeye, en düşük faktör yükü (0,65, $t=11.62$, $p<.05$) 18. Maddeye aittir. İzleme alt boyutunda en yüksek faktör yükü (0,89, $t=12.89$, $p<.05$) 26. Maddeye, en düşük faktör yükü (0,61, $t=9.44$, $p<.05$) 28. Maddeye aittir.

Analiz sonrasında, DFA model uyum indeks değerleri (Seçer, 2018) incelenmiş ve orijinal ve modifikasyon modellerine ait sonuçlar Tablo 4'te sunulmuştur.

Tablo 4. Ölçeğe Ait DFA Model Uyum İndeks Değerleri

	χ^2 /sd	RMSEA	NFI	NNFI	CFI	IFI	RMR	GFI	AGFI
Orijinal Model	3,26	0,09	0,93	0,95	0,95	0,95	0,06	0,79	0,74
Modifikasyon Model	2,36	0,07	0,94	0,96	0,97	0,97	0,06	0,85	0,82

Tablo 4 incelendiğinde, doğrulayıcı faktör analizinden elde edilen orijinal ve modifikasyon modeline ait uyum indeks değerleri görülmektedir. Orijinal modelde RMSEA= ,09, RMR=,06 indeksleri kabul edilebilir düzeyde ancak yüksek uyum indeksi elde edilmiştir. Diğer indekslerden NFI=0,93, CFI=0,95, IFI=0,95, GFI=0,79 ve AGFI=0,74 olmak üzere düşük uyum indeksi elde edilmiştir. Önerilen modifikasyonlar incelendiğinde 26 ile 29, 22 ile 24, 7 ile 8, 10, 11 19, 20 ile 27 ve 2 ile 27 maddelerin hata varyanslarında düzeltmeler yapılmıştır. Her bir düzeltme sonrasında ortaya çıkan model üzerinden modifikasyon işlemi gerçekleştirilmiştir. En son aşamada yapılan düzeltme sonucunda uyum indeksi değerleri tekrardan incelenmiştir ve ortaya çıkan model son model olarak kabul edilmiştir. Yapılan işlemler sonrasında RMSEA indeksinin 0,07 değerine düştüğü, RMR indeksinin değişmediği ve kabul edilebilir düzeyde uyum indeksi elde edildiği gözlenmiştir. NFI=0,96, CFI=0,97 ve IFI=0,97 indekslerinde mükemmel uyum indeksi elde edilmiştir. Modelin yalınlığı hakkında bilgi veren AGFI=0,82 ve GFI=0,85 olduğu bu indekslerin ise yüksek olmadığı ama kabul edilebilir bir uyum indeksi düzeyine sahip olduğu söylenebilir. İlk model ile modifikasyon sonucunda elde edilen modelin karşılaştırma imkânı veren AIC indeksindeki düşüş (İlk indeks=1068,36, 6 modifikasyon sonucu=831,63) modifikasyon sonucunda elde edilen modelin daha iyi bir model olduğu söylenebilir. Ayrıca χ^2/df uyum indeks değerleri ise modifikasyon önerisi sonrasında 3,26 değerinden 2,36 değerine düştüğü anlaşılmaktadır.

Bu çalışmada hem AFA için kullanılan örneklemden hem DFA için kullanılan örneklemden elde edilen puanların Cronbach alpha güvenirliği hesaplanmıştır. Ölçeğin tamamına ve ölçek faktörlerine ait Cronbach alpha iç tutarlılık katsayıları değerleri Tablo 5'te sunulmuştur.

Tablo 5. Faktörler ve Ölçeğin Tamamına Ait Güvenirlik Katsayıları

Faktör Adı	Madde Sayısı	Cronbach Alpha Değerleri Katsayısı (α)
Güvenlik	6	0,89
Paylaşım	4	0,84
Endişe	6	0,90
Fayda	7	0,90
İzleme	3	0,78
Toplam	26	0,75

Tablo 5 incelendiğinde, ölçeğe ve ölçeğe ait her bir faktör için hesaplanan güvenirlik kat sayısı değerleri görülmektedir. Buna göre ölçeğin tümüne yönelik Cronbach alpha güvenirlik katsayısının 0,75 değerinde olduğu anlaşılmaktadır. **"Güvenlik"** alt faktörüne ait güvenirlik katsayısının 0,89, **"Paylaşım"** alt faktörüne ait güvenirlik katsayısının 0,84, **"Endişe"** alt faktörüne ait güvenirlik katsayısının 0,90, **"Fayda"** alt faktörüne ait güvenirlik katsayısının 0,90 ve **"İzleme"** alt faktörüne ait güvenirlik katsayısının 0,78 değerinde olduğu tespit edilmiştir.

Ölçeğe ait maddelerin ortalama, standart sapma, madde toplam korelasyon değerlerine ait madde analiz sonuçlarına Tablo 6'da sunulmuştur.

Tablo 6. Ölçeğe Ait Madde Analiz Sonuçları

Faktör	Madd e	Ort.	SS	Madde Toplam Korelasyonu	Ort.	SS	Madde Toplam Korelasyonu
Güvenlik	M1	4,37	,87	0,678	3,97	1,31	0,811
	M2	3,64	1,06	0,470	3,54	1,17	0,692
	M13	4,10	,89	0,616	3,87	1,21	0,780
	M15	3,98	1,07	0,464	3,75	1,25	0,771
	M20	3,90	1,06	0,474	3,73	1,26	0,798
Paylaşım	M27	3,73	1,12	0,445	3,15	1,43	0,539
	M3	3,16	1,26	0,474	3,23	1,49	0,666
	M6	2,98	1,13	0,376	3,03	1,22	0,689
	M12	3,07	1,18	0,487	3,18	1,23	0,712
İzleme	M25	2,60	1,34	0,488	2,85	1,32	0,684
	M26	2,53	1,19	0,547	2,22	1,18	0,651
	M28	3,03	1,04	0,511	2,57	1,27	0,597
Endişe	M29	2,50	1,13	0,613	2,47	1,23	0,584
	M4	3,47	1,21	0,575	3,49	1,32	0,810
	M7	2,27	1,31	0,382	3,08	1,41	0,640
	M8	3,10	1,19	0,633	3,16	1,28	0,754
	M14	3,46	1,10	0,540	3,49	1,27	0,804
Fayda	M16	3,78	1,13	0,607	3,44	1,28	0,780
	M33	4,07	1,22	0,588	3,61	1,32	0,740
	M10	2,36	1,14	0,652	2,70	1,24	0,669
	M17	2,67	1,24	0,534	2,99	1,31	0,635
	M18	2,26	1,17	0,801	2,82	1,38	0,737
	M19	2,29	1,17	0,693	2,67	1,36	0,681
	M22	1,81	1,06	0,765	2,34	1,26	0,756
	M23	2,00	1,11	0,786	2,57	1,30	0,733
	M24	1,78	1,08	0,788	2,67	1,29	0,781

Tablo 6 incelendiğinde, ölçekte yer alan her bir maddeye yönelik madde toplam korelasyon değerleri, maddelere ait ortalama ve standart sapma değerleri görülmektedir. Açıklayıcı ve doğrulayıcı faktör analizleri sürecinde elde edilen maddelere ait madde-toplam korelasyon değerleri 0,30'un üzerindedir. Açıklayıcı faktör analizi süreci örneklemine ait madde-toplam korelasyon değerleri 0,376 ile 0,801 aralığında; doğrulayıcı faktör analizi süreci örneklemine ait madde-toplam korelasyon değerleri 0,539 ile 0,811 aralığında yer almaktadır. Kişisel Verilerin Gizliliği Farkındalık ölçeğinin ölçmeye yöneldiği yapıyı ölçüp ölçmediğine ilişkin yapı geçerliğini yukarıda açıklanan faktör analizlerinin yanı sıra yakınsama geçerliği (convergent validity) ve iraksama geçerliğinin (divergent validity) sonuçlarına ait Ortalama Açıklanan Varyans (OAV) ve Birleşik Güvenirlilik (CR) sonuç değerleri Tablo 7'de sunulmuştur.

Tablo 7. Yakınsama ve Ayırt Edici Geçerlik Analiz Sonuçları

	OAV	MPV	OPV	BG	1	2	3	4	5
1-Güvenlik	.577	.518	.228	.937	(.75)				
2-Paylaşım	.574	.241	.126	.927	-.30	(.76)			
3-Endişe	.610	.518	.227	.914	.72	-.27	(.78)		
4-Fayda	.558	.292	.200	.949	-.39	.49	-.34	(.74)	
5-İzleme	.623	.292	.187	.912	-.39	.32	-.45	.54	(.78)

Tablo 7 incelendiğinde, yakınsama geçerliği (convergent validity) ve iraksama geçerliğinin (divergent validity) bir başka versiyonu olan ayırt edici geçerlilik (discriminant validity) değerleri görülmektedir. Analiz sonuçları, tüm ölçek alt boyutlarının 0,50 üzerinde olduğunu göstermektedir. En düşük OAV 0,558 ile Fayda, en yüksek OAV değerinin ise 0,623 ile İzleme alt boyutuna ait olduğu gözlenmiştir. Her bir alt boyutun OAV değerlerinin MPV ve OPV değerlerinden daha yüksek olduğu belirlenmiştir. Birleşik Güvenirlilik (BG) indekslerinin OAV değerlerinden daha yüksek olduğu gözlenmiştir. Diğertaraftan OAV değerinin karekökü (koyu

yazılmış) gizil değişkenler arasındaki korelasyonlardan daha yüksek olduğu belirlenmiştir. Sonuçlar, AFA ile belirlenen 5 faktör yapısına dayalı ölçeğin DFA ile doğrulandığı yakınsama ve ayırt ediciliğinin de yüksek olduğu belirlenmiştir.

Tartışma ve Sonuç

Araştırmada, geçerli ve güvenilir bir "Kişisel Veri Gizliliği Farkındalık Ölçeği" geliştirilmesi amaçlanmıştır. Ölçek geliştirme süreci ilk aşamada madde havuzunun hazırlanması süreciyle başlamıştır. Madde havuzu oluşturulması sürecinde; kişisel veri gizliliği ve mahremiyet konu alanlarıyla ilişkili literatür taranmış, ihtiyaç duyulan kaynaklar incelenmiş ve alan uzmanları görüşleriyle soru maddeleri ortaya konulmuştur. Madde havuzunda yer verilen maddelerin açık ifadelerin net ve anlaşılır olması göz önünde bulundurulmuştur. Ayrıca birden fazla yargıyı ifade eden cümlelere yer verilmemiştir (Şeker ve Gençdoğan, 2014). Ayrıca ölçek maddelerinin her biri alan uzmanlarının görüşlerine sunulmuştur (Acar Güvendir ve Özer Özkan, 2015; Devellis, 2022; Gül ve Sözbilir, 2015; Seçer, 2018; Yeşilyurt ve Çapraz, 2018).

Hazırlanan ölçek taslak formu, açımlayıcı faktör analizi için 329 ve doğrulayıcı faktör analizi için 274 katılımcıya uygulanmıştır. Madde sayıları dikkate alındığında katılımcı sayısının yeterli olduğu anlaşılmaktadır (Comrey ve Lee, 2013; Şahin ve Boztunç Öztürk, 2018; Seçer, 2018). Ölçek taslak formunun uygulanmasıyla elde edilen veri seti açımlayıcı faktör analizi işlemine tabi tutulmuş ve değişkenler arasındaki ilişkiler değerlendirilerek yeni bir yapı ortaya konulmuştur (Can, 2022). Faktör analizi öncesinde KMO testi yapılarak, veri setinin faktör analizine uygunluğuna karar verilmiştir (Yaşlıoğlu, 2017). AFA için yeterliği hakkında bilgi veren KMO değeri 0,823 olarak elde edilmiş olup, KMO değerinin 0,80 ile 0,90 arasında olması örneklem yeterliliğinin iyi düzeyde olduğuna (Field, 2005) işaret etmektedir. Başka bir ifade ile örneklemden elde edilen verilerin faktör analitik modeli ile modellenebileceğini göstermektedir. Bir diğer ölçüm olan Bartlett Küresellik testi (Yaklaşık Ki-Kare=45,818, $p<0,05$) değerinin anlamlı olması verilerin faktör analizine uygun olduğunu göstermektedir (Tatlıdil, 2002).

Gerçekleştirilen açımlayıcı faktör analizi sırasında faktör yük değeri 0,45 üzerinde olan maddelerin ölçekte kalması uygun görülmüştür. Ölçekte yer alan maddelere ilişkin faktör yüklerinin 0,543 ve 0,857 değerleri arasında yer aldığı belirlenmiştir. Bu değerler ölçekte kalan maddeler ait faktör yüklerin oldukça iyi bir değerde olduğunu ortaya koymaktadır (Büyüköztürk, 2019; Seçer, 2018). Bununla beraber doğrulayıcı faktör analiziyle elde edilen madde yük değerlerinin 0,46 ve 0,91 değerleri arasında değiştiği kabul edilebilir olduğunun göstergesidir. DFA analizi sonucunda ortaya konulan uyum indeksi değerlerinin 0,85 ve 0,95 aralıklarında olması, uyum indeksi değerlerinin kabul edilebilir veya mükemmel bir uyuma eğilim gösterdiği tespit edilmiştir (Bayram, 2010; Candan, 2019; Jöreskog ve Sörbom, 1996; Kline, 2015; Seçer, 2018; Sümer, 2000; Tabachnick ve Fidell, 2007; Yılmaz ve Köseoğlu, 2009).

Açımlayıcı faktör analizi sonrasında ölçeğe ait açıklanan varyans oranının %40 ile %60 arasında olması yeterli kabul edildiği (Çokluk, Şekercioğlu ve Büyüköztürk, 2021) ve değer % 58,644 olması kabul görülebilir bir orandır. Ayrıca ölçeğe ait alt boyutlara dağılım gösteren madde sayısının en az 3 olması, faktörlerin yeterli madde sayısına sahip olduğu belirtilebilmektedir (Bandalos ve Finney, 2019). Geliştirilen ölçeğe ait Cronbach alpha katsayısı 0,75 değerinde belirlenmiş olup, Cronbach alpha iç tutarlılık katsayısının 0,70'den büyük değere sahip olması ölçme aracının güvenilir olduğuna işaret etmektedir (Kayış, 2018; Can, 2022). Ayrıca ölçekte yer alan maddelerin, madde-toplam korelasyonu değerlerinin tümünün 0,30'un üzerinde olması maddelerin ayırt edici olduğunu ve iç tutarlılığının yüksek olduğunu göstermektedir (Büyüköztürk, 2019). Açımlayıcı ve doğrulayıcı faktör analizleriyle ortaya konulan 5 faktörlü yapı isimlendirilmiştir. Yapılan isimlendirmede sürecinde, alt faktörlerin içerikleri incelenmiş ve maddeleri bir araya getiren ortak amaçlar belirlenmiştir. Ölçekte yer alan maddelerin farklı hedefleri ölçmesi gerekçesiyle; birinci faktöre "Güvenlik", ikinci faktöre "Paylaşım", üçüncü faktöre ise "Endişe", dördüncü faktöre "Fayda" ve beşinci faktöre ise "İzleme" adı verilmiştir.

Yakınsama geçerliği, göstergelerince iyi derecede ölçülen özelliğin güven derecesi iken ayırt edici geçerlik birbiri ile ilgisiz farklı özellikleri ölçme derecesi olarak ifade edilmektedir. (Hair, Balck ve Babin, 2005; Ramaker, Marinus, Stiggelbout ve Van Hilten 2002). Çalışmada elde edilen değerlerin 0,70 üzerinde olması, ölçek yapısının farklı nitelikleri ölçüme uygu olduğunu göstermektedir. OAV değerinin ise 0,70 ve üstü çok iyi olmakla birlikte 0,50 ve üstünde olması, ölçeğe ait değerlerin 0,50 değeri üzerini karşılaması yeterli olduğuna işaret etmektedir.

Alan yazın incelendiğinde doğrudan kişisel verilerin gizliliğine yönelik bir farkındalık ölçeğine rastlanmamıştır. Ancak geliştirilen ölçme aracıyla yakından ilişkili olabilecek bilgi güvenliğine ait farkındalık ölçeği geliştirmeyi amaçlayan araştırmalara odaklanılmıştır. Keser ve Güldüren (2015) tarafından

öğretim elamanlarına yönelik bir bilgi güvenliği farkındalık ölçeği geliştirilmiştir. Çalışmada gerçekleştirilen analizler sonrasında 2 alt boyuttan oluşan 34 maddelik ölçme aracı ortaya konulmuştur. Ölçme aracı saldırı ve tehditler ile kişisel verilerin korunmasına yönelik soruları içermektedir. Ölçeğe ait cronbach alpha güvenirlik katsayısı 0.97 değerindedir. Diğer bir çalışmada öğrencilerin bilgi güvenliği farkındalık düzeylerini belirlemeye yönelik bir ölçek ortaya konulmuştur. 36 maddeden oluşan ölçek mahremiyet, kişisel verilerin korunması, saldırı ve tehditler olmak üzere 3 alt boyuta ait sorular içermektedir. Ölçeğe ait cronbach alpha güvenirlik katsayısı 0.955 değerindedir (Güldüren, Çetinkaya & Keser, 2016). Yine benzer başka bir çalışmada öğretmenlere yönelik bilgi güvenliği farkındalık ölçeği geliştirilmiştir. 48 maddelik ölçek mahremiyet ve iletişim, saldırı ve tehditler ve genel güvenlik boyutlarından meydana gelmektedir. Ortaya konulan ölçme aracının cronbach alpha güvenirliği 0.980 olup geçerliliği ve güvenirliği sağlanmıştır (Çetinkaya, Güldüren ve Keser, 2017). Öte yandan ortaokul öğrencilerini hedef alan bilgi güvenliği farkındalık ölçme aracının geliştirildiği çalışmaya da ulaşılmıştır. Çalışmada 30 madde ve üç alt boyuttan (çevrimiçi güvenlik farkındalığı, çevrimiçi merak ve siber tehdit farkındalığı) oluşan 0,90 cronbach alpha güvenirlik katsayısına sahip geçerli ve güvenilir bir ölçme aracı geliştirilmiştir (Çetinkaya & Öktelik, 2022). Alan yazın çalışmaları doğrultusunda doğrudan kişisel verilerin gizliliği farkındalığının ortaya konulduğu bir ölçme aracına rastlanmamıştır. Çalışmada geliştirilen ölçek diğer ölçeklere kıyasla kişisel verilerin gizliliğini ön plana çıkaran bir ölçme aracıdır. Güvenlik, paylaşım, endişe, fayda ve izleme boyutlarından meydana gelerek alt boyutları yönüyle de diğer ölçekler ayrılmaktadır. Bununla beraber üniversite öğrencilerine yönelik bir ölçme aracı olması nedeniyle diğer ölçeklerin hedef grubundan farklıdır. Dolayısıyla çalışma kapsamında geliştirilen "Kişisel Verilerin Korunması Farkındalığı" ölçeğinin alan yazına önemli katkılar sunabileceği açıktır.

Araştırma sonuçları doğrultusunda, geçerli ve güvenilir bir "Kişisel Verilerin Korunması Farkındalığı" ölçeği ortaya konulmuştur. Ölçek 5 faktörlü yapıda, 26 maddelik, 5'li likert tipte ve 0,75 güvenirlik kat sayısına sahip bir ölçme aracı geliştirilmiştir (Ölçeğin son hali Ek.1). Ölçek bilgi ve iletişim teknolojileri, eğitim bilimleri, eğitim hukuku, dijital suçlar ve yazılım alanlarında bireylerin kişisel veri gizliliği farkındalığı tespitinde araç olarak kullanılabilir. Ayrıca, bireylerin kişisel veri gizliliği farkındalığı puanlarının farklı değişkenler üzerindeki etkileri incelenebilir. Bununla birlikte nitel verilerin yer aldığı çalışmalar yapılarak, katılımcılarla görüşmeler gerçekleştirilecek çalışmalar alana kazandırılabilir. Geliştirilen ölçeğin mevcut konu alanlarında araştırma yapmak isteyen tüm araştırmacı ve eğitimciler için alternatif bir ölçme aracı olabileceği açıktır.

Kaynaklar

- Abudureyimü, Y., ve Oğurlu, Y. (2021). Yapay zekâ uygulamalarının kişisel verilerin korunmasına dair doğurabileceği sorunlar ve çözüm önerileri. *İstanbul Ticaret Üniversitesi Sosyal Bilimler Dergisi*, 20(41), 765-782. <https://doi.org/10.46928/itcusbe.863505>
- Acar Güvendir, M. ve Özer Özkan, Y. (2015) Türkiye'deki eğitim alanında yayımlanan bilimsel dergilerde ölçek geliştirme ve uyarlama konulu makalelerin incelenmesi. *Elektronik Sosyal Bilimler Dergisi*, 52, 23-33.
- Acar Güvendir, M., ve Özer Özkan, Y. (2022). *Tüm yönleriyle ölçek geliştirme süreci*. Ankara: Pegem A Yayıncılık.
- Alfnes, F., ve Wasenden, O. C. (2022). Your privacy for a discount? Exploring the willingness to share personal data for personalized offers. *Telecommunications Policy*, 46(7), 102308. <https://doi.org/10.1016/j.telpol.2022.102308>
- Arınmış Uzun, S. (2021). Türkiye'de kişisel verilerin korunması ve vatandaş algısının ölçülmesi. *Bilişim Teknolojileri Dergisi*, 14(3), 207-221. <https://doi.org/10.17671/gazibtd.735471>
- Atasoy, K. (2016). Kişilik hakkı kapsamında sosyal medyada kişisel verilerin korunması ve veri sahibinin rızası. *Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi*, 22(3), 269-301.
- Athı, T. (2019). Kişisel verilerin önleyici, koruyucu ve istihbari faaliyetler amacıyla işlenmesi. *Necmettin Erbakan Üniversitesi Hukuk Fakültesi Dergisi*, 2(1), 4-22.
- Bandalos, D. L., ve Finney, S. J. (2010). *Factor Analysis: Exploratory and Confirmatory*. In G. R. Hancock ve R. O. Mueller (Ed.) *The Reviewer's Guide to Quantitative Methods in the Social Sciences* (pp. 93-114). New York, NY: Routledge.
- Bayram, N. (2010). *Yapısal eşitlik modellemesine giriş*. Bursa: Ekin Kitabevi.
- Bilir, F. (2020) 6698 sayılı kişisel verilerin korunması kanunu'na ilişkin değerlendirme ve internet çağında kişisel verilerin korunması. *Anayasa Yargısı Dergisi*, 37(2), 305-342.

- Bilir, F. (2023). Kişisel verilerin korunması yönündeki uygulama ve hukuki düzenlemelerin ortaya çıkışı. *Adalet Dergisi*(71), 631-651. <https://doi.org/10.57083/adaletdergisi.1391733>
- Büyüköztürk, Ş. (2019). *Sosyal bilimler için veri analizi el kitabı: istatistik, araştırma deseni SPSS uygulamaları ve yorum*. Ankara: Pegem Akademi Yayıncılık.
- Büyüköztürk, Ş., Şekercioğlu, G., veamp; Çokluk, O. (2014). *Sosyal bilimler için çok değişkenli istatistik: SPSS ve LISREL uygulamaları*. Ankara: Pegem Akademi Yayınları.
- Çakır, H., Hava, K., Gülen, Ş. B., ve Özüdoğru, G. (2015). Öğretmen adaylarının sosyal ağ sitelerinde güvenlik farkındalıklarının incelenmesi. *International Journal of Human Sciences*, 12(1), 1303-5134, <http://dx.doi.org/10.14687/ijhs.v12i1.3142>
- Calzada, I. (2022). Citizens' data privacy in China: The state of the art of the Personal Information Protection Law (PIPL). *Smart Cities*, 5(3), 1129-1150. <https://doi.org/10.3390/smartcities5030057>
- Can, A. (2022). *SPSS ile bilimsel araştırma sürecinde nicel veri analizi (10.baskı)*. Ankara: Pegem Atıf İndeksi.
- Candan, S. S. K. (2019). *Yapısal eşitlik modellemesi uygulamaları*. Yayınlanmamış Yüksek Lisans Tezi, Ege Üniversitesi Fen Bilimleri Enstitüsü, İzmir.
- Çelik, Y. (2017).Özel Hayatin gizliliğinin yansıması olarak kişisel verilerin korunması ve bu bağlamda unutulma hakkı. *Türkiye Adalet Akademisi Dergisi*, 32, 391-410.
- Çetin, H. (2014). Kişisel Veri güvenliği ve kullanıcıların farkındalık düzeylerinin incelenmesi. *Akdeniz İİBF Dergisi*, 14(29), 86-105.
- Çetinkaya, L., & Öktelik, B. (2022). Ortaokul düzeyi öğrencilerine yönelik bilgi güvenliği farkındalık ölçeği geliştirme çalışması. *Cumhuriyet Uluslararası Eğitim Dergisi*, 11(4), 696-708. <https://doi.org/10.30703/cije.1131545>
- Çetinkaya, L., Güldüren, C. ve Keser, H. (2017). Öğretmenler İçin Bilgi Güvenliği Farkındalık Ölçeği (Bgfö) Geliştirme Çalışması. *Milli Eğitim Dergisi*, 46(216), 33-52.
- Cheung, C. M., Chiu, P.-Y., ve Lee, M. K. (2011). Online social networks: Why do students use Facebook? *Computers in Human Behavior*, 27(4), 1337-1343, <https://doi.org/10.1016/j.chb.2010.07.028>
- Çokluk, Ö. Şekercioğlu, G. ve Büyüköztürk, Ş. (2021). *Sosyal bilimler için çok değişkenli istatistik Spss ve Lisrel uygulamaları*. (6. Baskı). Ankara: Pegem Akademi.
- Colton, D. ve Covert, R. (2007). *Designing and constructing instruments for socialresearch and evaluation*. San Francisco, CA: Jossey-Bass.
- Comrey, A. L., ve Lee, H. B. (2013). *A first course in factor analysis*. New Jersey: Psychology Press.
- Costello, A. B., ve Osborne, J. W. (2005). Exploratory factor analysis: Four recommendations for getting the most from your analysis. *Practical Assessment, Research, and Evaluation*, 10(7), 1-9.
- Creswell, J.W., ve Creswell, J.D. (2021). *Araştırma tasarımı: Nitel, nicel ve karma yöntem yaklaşımları (Çev. Engin Karadağ)*. (5. baskı).Ankara: NobelYayınları.
- DeVellis, R. F. (2022). *Ölçek geliştirme kuram ve uygulamalar (T. Totan, Çev.)*. Ankara: Nobel Akademi.
- Dinler, E.,ve Çalışkan, Z. (2019). Mülkiyetin tarihsel gelişimi üzerine bir deneme. *Sosyal Siyaset Konferansları Dergisi*, 77, 421-452.
- Dülger, M.V.(2018). İnsan ve temel hak ve özgürlükler bağlamında kişisel verilerin korunması. *İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi*, 5(1), 71-144.
- Eroğlu, Ş. (2018). Dijital yaşamda mahremiyet (gizlilik) kavramı ve kişisel veriler: hacettepe üniversitesi bilgi ve belge yönetimi bölümü öğrencilerinin mahremiyet ve kişisel veri algılarının analizi. *Hacettepe Üniversitesi Edebiyat Fakültesi Dergisi*, 35(2), 130-153. <https://doi.org/10.32600/huefd.439007>
- Eryılmaz, H. E. (2023). Yapay zekâ çağında kişisel veri mahremiyeti. *Umay Sanat ve Sosyal Bilimler Dergisi*, 1(2), 6-25.
- Field, A. (2005). *Discovering statistics using SPSS (2nd ed.)*. London: Sage Publication.
- Genç, C. (2019). *Kişisel verilerin korunması kapsamında bilgi güvenliği farkındalığı analizi ve e-devlet yapısının incelenmesi*. Yayınlanmamış Yüksek Lisans Tezi, İstanbul Okan ÜniversitesiFen Bilimleri Enstitüsü, İstanbul.
- Gül, Ş., ve Sözbilir, M. (2015). Fen ve matematik eğitimi alanında gerçekleştirilen ölçek geliştirme araştırmalarına yönelik tematik içerik analizi. *Eğitim ve Bilim*, 40(178), 85-102.

- Güldüren, C., Çetinkaya, L., ve Keser, H. (2016). Ortaöğretim öğrencilerine yönelik bilgi güvenliği farkındalık ölçeği (bgfö) geliştirme çalışması. *İlköğretim Online*, 15(2). <https://doi.org/10.17051/uo.2016.27218>
- Hair J., Black, W., ve Babin B. (2005). *Multivariate data analyses. (6th Ed.)* Nueva York: Prentice-Hall.
- Jöreskog, K., ve Sörbom, D. (1996). *LISREL 8: User's reference guide*. Chicago, IL: Scientific Software International Inc.
- Kart, A. ve Ketizmen, M. (2019). Kabahatler kanunu'nun içtima hükümleri açısından kişisel verilerin korunmasına ilişkin suç ve kabahatler ile kurul'un idari ceza kararlarına ilişkin bir değerlendirme. *Kişisel Verileri K. Dergisi*, 1 (2), 17-29.
- Kayış, A. (2018). *SPSS Uygulamalı Çok Değişkenli İstatistik Teknikleri. Ş. Kalaycı (Ed.), Güvenilirlik Analizi (Reliability Analysis). (S.402-419)*. Ankara: Dinami Akademi Yayıncılık.
- Ke, T. T., ve Sudhir, K. (2023). Privacy rights and data security: GDPR and personal data markets. *Management Science*, 69(8), 4389-4412. <https://doi.org/10.1287/mnsc.2022.4614>
- Keser, H., ve Güldüren, C. (2015). Bilgi Güvenliği Farkındalık Ölçeği (BGFÖ) Geliştirme. *Kastamonu Eğitim Dergisi*, 23(3), 1167-1184.
- Kılınç, Doğan. "Anayasal Bir Hak Olarak Kişisel Verilerin Korunması". Ankara Üniversitesi Hukuk Fakültesi Dergisi 61, no. 3 (Eylül 2012): 1089-1172. https://doi.org/10.1501/Hukfak_0000001684
- Kline, R. B. (2015). *Principles and practice of structural equation modeling*. New York City: Guilford Publications.
- Köksalan, E. (2022). *Kişisel veri gizliliği ve dijital çağda mahremiyet: Sesli sanal asistanlar*. Yayınlanmamış Yüksek Lisans Tezi, Çukurova Üniversitesi Sosyal Bilimleri Enstitüsü, Adana.
- Kumar, S., Saravanakumar, K., ve Deepa, K. (2016). On Privacy and Security in Social Media—A Comprehensive Study. *Procedia Computer Science*, 78, 114-119.
- Majeed, A., ve Hwang, S. O. (2023). Quantifying the vulnerability of attributes for effective privacy preservation using machine learning. *IEEE Access*, 11, 4400-4411. <https://doi.org/10.1109/ACCESS.2023.3235016>
- Nagy, J., ve Pecho, P. (2009). Social networks security. In Third International Conference on Emerging Security Information, *Systems and Technologies*, 321-325.
- Özkaya, Ö., ve Toprak, İ. (2022). Türkiye’de güvenlik faaliyetleri kapsamında kişisel verilerin işlenmesi. *Manas Sosyal Araştırmalar Dergisi*, 11(3), 1291-1305.
- Özkaya, Ö., ve Toprak, İ. (2022). Türkiye’de güvenlik faaliyetleri kapsamında kişisel verilerin işlenmesi. *Manas Sosyal Araştırmalar Dergisi*, 11(3), 1291-1305.
- Ramaker C, Marinus J, Stiggelbout A, ve Van Hilten B. (2002). Systematic evaluation of rating scales for impairment and disability in Parkinson's disease. *Movement Disorders*, 17, 867-876.
- Romansky, R. P., ve Noninska, I. S. (2020). Challenges of the digital age for privacy and personal data protection. *Mathematical Biosciences and Engineering*, 17(5), 5288-5303. <https://doi.org/10.3934/mbe.2020286>
- Şahin, M. G. ve Boztunç Öztürk, N. (2018). Scale development process in educational field: a content analysis research. *Kastamonu Eğitim Dergisi*, 26 (1) , 191-199.
- Seçer, İ (2017). *Spss ve lisrel ile pratik veri analizi, analiz ve raporlaştırma*. Ankara: Anı Yayınları.
- Seçer, İ. (2018). *Psikolojik test geliştirme ve uyarlama süreci: SPSS ve LISREL uygulamaları (2.Baskı)*. Ankara: Anı yayıncılık.
- Sefer, O.(2018). Kişisel verilerin korunması hukukunun genel ilkeleri. *Bilgi Ekonomisi ve Yönetimi Dergisi*, 13(2), 121-138.
- Şeker, H., ve Gençdoğan, B. (2014). *Psikolojide ve eğitimde ölçme aracı geliştirme (2.Baskı)*. Ankara: Nobel Yayıncılık.
- Sevinç, A. (2018). *Öğretmen adaylarının bilgi gizliliği yönetimi davranışları, internet bağımlılıkları ve sosyal medya kullanım alışkanlıkları arasındaki ilişkilerin incelenmesi* . Yayınlanmamış Doktora Tezi, Fırat Üniversitesi Eğitim Bilimleri Enstitüsü, Elazığ.
- Shariff, A., Green, J., ve Jettinghoff, W. (2021). The Privacy Mismatch: Evolved Intuitions in a Digital World. *Current Directions in Psychological Science*, 30(2), 159-166.
- Shukur, F., ve Fatlawi, A. (2022, September). Privacy and security awareness for sensitive/non-sensitive data based wearable devices. In 2022 International Conference on Emerging Trends in Smart Technologies (ICETST) (pp. 1-4).IEEE. <https://doi.org/10.1109/ICETST55735.2022.9922930>
- Tabachnick, B. G., ve Fidell, L. S. (2007). *Using Multivariate Statistics (5th ed.)*. New York: Allynand Bacon.
- Tatlıdil, H. (2002). *Uygulamalı çok değişkenli istatistiksel analiz*. Ankara: Akademi Mat.

Turan, M. (2015), “Hukukumuzda Kişisel Verilerin Korunması”, *Kalkınma Dergisi*, 80, 2-5.

Yaji, S., ve Bayyapu, N. (2021). Result attack: a privacy breaching attack for personal data through K-means algorithm. *Cyber-Physical Systems*, 7(1), 11-40. <https://doi.org/10.1080/23335777.2020.1811380>

Yaşlıoğlu, M. M. (2017). Sosyal bilimlerde faktör analizi ve geçerlilik: keşfedici ve doğrulayıcı faktör analizlerinin kullanılması. *İstanbul Üniversitesi İşletme Fakültesi Dergisi*, özel sayı, 74-85.

Yeşilyurt, S., ve Çapraz, C. (2018). Ölçek geliştirme çalışmalarında kullanılan kapsam geçerliği için bir yol haritası. *Erzincan Üniversitesi Eğitim Fakültesi Dergisi*, 20(1), 251-264.

Yıldırım, A., ve Şimşek, H. (2018). *Sosyal bilimlerde nitel araştırma yöntemleri*. Ankara: Seçkin Yayıncılık.

Yılmaz, V., ve Köseoğlu, H. E. (2009). *Lisrel ile yapısal eşitlik modellemesi*. Ankara: Pegem Akademi.

“PERSONAL DATA PRIVACY AWARENESS SCALE” DEVELOPMENT STUDY

Mehmet Ercüment ARI, Özhan TİNGÖY

ABSTRACT

This study aims to develop a valid and reliable personal data privacy awareness scale. The study was conducted with an exploratory sequential mixed design based on mixed method research. The participants of the study consisted of 704 university students studying at different grade levels and in different departments of state and foundation universities. In order to create the draft form of the study, the literature on the subject was reviewed and a 33-item question pool was prepared by field expert researchers. After the expert opinions were received and the pilot application was carried out, the draft form was finalized and the main application was started. The data obtained after the main application were analyzed using SPSS and LISREL statistical programs. Exploratory and confirmatory factor analyses were conducted to ensure construct validity during data analysis. The reliability of the scale was calculated with Cronbach's alpha internal consistency coefficient. Total item correlation values and discriminant validity values were also calculated. The confirmatory factor analysis findings revealed that the scale had a five-factor structure and the fit indices showed acceptable (AGFI=0.82 and GFI=0.85) and excellent ($\chi^2/sd=2.36$, NFI=0.96, CFI=0.97, IFI=0.97, RMR=0.06 and RMSEA=0.07) fit. As a result of the research, a five-point Likert-type “Personal Data Protection Awareness Survey” consisting of 26 items with a Cronbach's alpha internal consistency coefficient of 0.75 was developed. The results of the study reveal that the developed scale can be used as a valid and reliable measurement tool.

Keywords: Protection of personal data, awareness, personal data, privacy, scale, university students

Ek.1. “Kişisel Verilerin Ölçeğin Son Hali

Kişisel Verilerin Gizliliği (KVG) Farkındalık Ölçeği	Kesinlikle katılmıyorum	Katılmıyorum	Kısmen katılmıyorum	Katılıyorum	Kesinlikle katılıyorum
1. Alışveriş yaparken daha fazla indirim almak için kişisel verilerimi paylaşabilirim.	1	2	3	4	5
2. Özel mesajlarım dışında Facebook hesabıma ait tüm verilerimi iyi bir ücret karşılığında reklam ajanslarına satabilirim.	1	2	3	4	5
3. Oyun içi hediye veya ürün karşılığı, (sosyal medya hesaplarım da dahil olmak üzere) kişisel bilgilerimi paylaşmaktan çekinmem.	1	2	3	4	5
4. Ünlü bir kişi olmadığım için kişisel verilerimin bilgim dışında paylaşılmasını önemsemem.	1	2	3	4	5
5. Netflix’den bedava yararlanabilmek için kişisel verilerimi paylaşabilirim.	1	2	3	4	5
6. Çağrı merkezi görüşmelerinde Kişisel Verilerin işlenmesi ile ilgili izin teklifleri zaman kaybettirici olduğunu düşündüğüm için hepsini dinlemeden onaylarım.	1	2	3	4	5
7. İnternette pop-up pencereleri ile önüme çıkan çerezler (cookie) hakkında bilgim olmasa da bunlara ilişkin şartları, o hizmeti almak için kabul ediyorum.	1	2	3	4	5
8. Instagramda, tespit edilmemeyi tercih ederim.	1	2	3	4	5
9. Benim kişisel verilerimi alıp kullanan şirketler bu verimi uygun güvenlik tedbirleri ile de koruduğuna inanmıyorum.	1	2	3	4	5
10. Applestore veya Playstore’a üyelik için önşart olarak kredi kartı bilgilerinin girilmesi beni rahatsız ediyor.	1	2	3	4	5
11. Sosyal medyada profil oluşturabilmek için yaş sınırı olması gerektiğine inanıyorum.	1	2	3	4	5
12. Firmaların Web, Mobil Uygulamaları, mail veya sms gibi yollarla kişisel verilerin işlenmesine ilişkin izin talepleri genellikle beni rahatsız ediyor.	1	2	3	4	5
13. Instagramdastoryleri izleyenlerin isimlerinin görülmesi beni rahatsız ediyor.	1	2	3	4	5
14. Kişisel verilerin gizliliği benim için önemlidir.	1	2	3	4	5
15. Kişisel verilerin korunması ile ilgili ne kadar tedbir alınsa da devletlerin kişilerin her türlü verisine eriştiğine inanıyorum.	1	2	3	4	5
16. İnternette alış veriş yaparken ürün fiyatından önce şirketin kişisel veri güvenliği açısından güvenilir olup olmadığı önceliğimdir.	1	2	3	4	5
17. Kişisel verilerin gizliliği ile bilgi güvenliği aynı şeydir.	1	2	3	4	5
18. Eski bilgisayar veya cep telefonumu birine verirken, atarken, satarken veya elden çıkarırken kişisel verilerimin geri döndürülemeyecek şekilde imha ettiğime emin olurum.	1	2	3	4	5
19. Sosyal medyada mahrem olan özel bilgilerin rahatça paylaşıldığını düşünüyorum.	1	2	3	4	5
20. Hayatımda en az bir kere mail veya sms yolu ile firmaların kişisel verileri işleme izin taleplerine olumlu veya olumsuz geri dönüş yapmışlığım vardır.	1	2	3	4	5
21. Herhangi bir süreç için (örnek iş görüşmesi, vb) gerekli olan kimlik fotokopimi, mail ile istendiğinde gönderirim.	1	2	3	4	5
22. Sürekli olarak gittiğim cafe’nin veya spor salonunun bana daha kolay ve güvenli hizmet verebilmesi için biyometrik verilerimi (parmak izi, avuç içi, yüz tanıma vb.) işleme isteğini makul karşılarım.	1	2	3	4	5
23. Whatsapp gruplarında her konuda fikirlerimi açıkça paylaşıyorum	1	2	3	4	5
24. Toplumda güvenliği sağlamak için özel sektör tarafından, kişileri izleme teknolojisi daha fazla kullanılmalıdır.	1	2	3	4	5

25.	Toplumda güvenliği sağlamak için devlet tarafından, kişileri izleme teknolojisi daha fazla kullanılmalıdır.	1	2	3	4	5
26.	Google arama ve konum geçmişimin toplumsal huzuru sağlamak adına devlet(ler) ile paylaşılmasında bir sakınca görmem.	1	2	3	4	5