Original Article

Received/Accepted Dates

16.02.2025/07.03.2025

DOI 10.52096/usbd.9.38.25

International Journal of Social Sciences

IJSS

Uluslararası Sosyal Bilimler Dergisi

www.sobider.net e-ISSN: 2548-0685

Sosyal Medya İstihbaratı Farkındalığı Ölçeği (Smifö): Geçerlik ve Güvenirlik Çalışması

Burcu KEPEKÇİ

100/2000 YÖK Doktora Bursiyeri, Ankara Hacı Bayram Veli Üniversitesi, Lisansüstü Eğitim Enstitüsü Gazetecilik Anabilim Dalı, 100/2000 YÖK Doktora Bursiyeri, burcuemiroglu93@gmail.com, ORCID ID 0000-0003-4724-8743

Prof. Dr. Erol İLHAN

Ankara Hacı Bayram Veli Üniversitesi, İletişim Fakültesi, erolilhan06@gmail.com, ORCID ID 0000-0001-9428-4611

Özet

Günümüzde sosyal medyanın birey hayatının tam merkezinde konumlandırılmasıyla birlikte; iletişim biçimleri, mahremiyet, güvenlik ve gözetim algıları değişmiş ve dönüşmüştür. Özellikle bireylerin sosyal medya platformlarında bıraktıkları dijital izlerin, devlet kurumları, güvenlik birimleri ve özel sektör tarafından istihbarat amaçlı analiz edilmesi, bu alandaki farkındalık düzeyinin değerlendirilmesini gerekli kılmaktadır. Bu çalışma, sosyal medyadaki istihbarat faaliyetlerine yönelik farkındalığı ölçen bilimsel bir ölçek geliştirmeyi amaçlamaktadır.

Ölçeğin teorik altyapısını oluşturulurken, Korunma Motivasyon Teorisi ve Psikolojik Tepki Teorisi temel kavramsal çerçeve olarak alınmış ve ölçek soruları geliştirilmiştir. Üç alt boyut ve 11 maddeden oluşan beşli Likert tipi Sosyal Medya İstihbarat Farkındalığı Ölçeği (SMİFÖ), SPSS-27 ve AMOS-22 programlarıyla analiz edilmiştir. Açımlayıcı ve doğrulayıcı faktör analizleri sonucu ölçek; İstihbarati Gözetim, Dijital Paylaşım ve Dijital Güvenlik Farkındalığı boyutlarından oluşmuştur. Geçerlik ve güvenirlik analizleri ölçeğin psikometrik açıdan yeterli olduğunu göstermektedir. Bu çalışma sosyal medya istihbaratı konusundaki farkındalığın gelişmesine ve bu alanda yürütülen akademik araştırmalara özgün bir çerçeve sunmayı amaçlamaktadır.

Anahtar Kelimeler: Sosyal Medya İstihbaratı, Sosyal Medya İstihbaratı Farkındalığı Ölçeği, Ölçek Geliştirme

Social Media Intellıgence Awareness Scale (Smias): Validity and Reliability Study

Abstract

With social media positioned at the center of individual life, communication styles, privacy, security, and surveillance perceptions have changed and transformed. For intelligence purposes, analyzing digital traces left by individuals on social media platforms by state institutions, security units, and the private sector necessitates evaluating the level of awareness in this area. This study aims to develop a scientific scale measuring awareness of social media intelligence activities.

While creating the theoretical infrastructure of the scale, Protection Motivation Theory and Psychological Response Theory were taken as the basic conceptual framework, and the scale questions were developed. The five-point Likert-type Social Media Intelligence Awareness Scale (SMIAS), consisting of three sub-dimensions and 11 items, was

analyzed with SPSS-27 and AMOS-22 programs. As a result of explanatory and confirmatory factor analyses, Intelligence comprises dimensions of surveillance, digital sharing, and digital security awareness. Validity and reliability analyses show that the scale is psychometric. This study aims to provide an original framework for developing awareness about social media intelligence and academic research in this field.

Keywords: Social Media Intelligence, Social Media Intelligence Awareness Scale, Scale Development

GİRİŞ

İletişimin yeni bir biçimi olan sosyal medyanın amacı, görmek ve göstermek, gözetlemek ve gözetlenmektir. Bu nedenle sosyal medya platformlarında gündelik yaşama dair tüm tecrübeler görünürlük adına paylaşılmaktadır (Toprak vd., 2014: 156-161). Sosyal medya platformlarında kullanıcılar tarafından paylaşılan içeriklerden bir başka deyişle verilerden hareketle ciddi sayıda istatistiksel bilimsel araştırmalar ve yeni araştırma alanları doğmuştur (Aggarwal, 2011: 2-3). Bu yeni araştırma alanlarından birisi ise sosyal medya istihbaratıdır. Devletler, güvenlik birimleri ve özel sektör açık kaynak istihbaratı (OSINT) ve veri analitiği bağlamında sosyal medya önemli bir araç olarak karşımıza çıkmaktadır. Teknolojinin gelişmesi ve genişlemesi ile sosyal medya istihbaratı güvenlik, veri analizi, kamuoyu yoklamaları ve bireylerin çevrimiçi davranışlarını analiz etme amacıyla kullanılmaktadır (Dover, 2019).

Son 15 yıldır sosyal medya platformlarının yükselişi ile hayatımıza giren sosyal medya istihbaratı (SOCMINT) ulusal güvenlik, terörle mücadele, siber tehditlerin tespiti ve dezenformasyon analizleri gibi konularda önemli bir araçtır (Omand, Bartlett & Miller, 2012; Weimann, 2014). Geleneksel istihbarat türlerinden ve yöntemlerinden farklı olarak, SOCMINT kamuya açık veriler üzerinden anlık tehdit değerlendirmesi yapma, stratejik karar verme ve harekete geçme süreçlerini hızlandırmış ilgili birimlerden daha hızlı ve etkili öngörü sağlayarak olayların veya olguların tespitini kolaylaştırmıştır (Bertram, 2016; Omand, 2017: 350-370).

Sosyal medya istihbaratında elde edilen veriler multidisipliner veri analizi yöntemleri kullanılarak birbirinden farklı alanlara (güvenlik, iletişim, pazarlama, siyaset, reklamcılık vb.) uyarlanarak gerçekleşen olaylar ve olgular hakkında çeşitli cevapları içerebileceği gibi gelecekte olabilecek olaylar ve olgular hakkındaki tahminleri içerebilecek bilgi parçacıklarını da oluşturmaktadır. Sosyal medya istihbaratının nihai amacı, analiz sürecindeki bilinmezliği azaltmaktır. Sosyal medya istihbaratı dijital alanın avantajlarını artırıp dezavantajlarını ise en aza indirerek yasal çerçeveler içinde sanal ortamda toplumu izlemeyi hedeflemektedir (Sezgin vd., 2023: 190). Genellikle kolluk

kuvvetleri ve istihbarat teşkilatları, kovuşturmalar ve terörle mücadele soruşturmaları için sosyal medyadan veriler toplamaktadırlar (Brown, 2015: 6). Sosyal medya istihbaratı, kamu güvenliğini artırmak için teknolojinin uygulanması ve yönetiminde keşif için yeni bir alanı temsil etmektedir (Antonius & Rich, 2013: 51). Özellikle gözetim toplumunda sosyal medya verileri üzerinde çalışılması, toplumdaki sorunların çözülebilmesi, önceden tespit edilebilmesi, ortaya çıkmadan önlem alınabilmesi için sosyal medya platformlarında paylaşılan içerikler çeşitli metotlarla (dil işleme, duygu analizi, sosyal ağ analizi vd.) analiz edilerek istihbarat çarkına dahil edilmektedir (Dover, 2019; Cerrah & Dağlar Macar, 2022: 94).

Sosyal medya istihbaratının ulusal güvenlik politikalarındaki rolü, bireylerin sosyal medya üzerindeki mahremiyet stratejileri ve gözetim karşısındaki tutumları gibi konular, literatürde önemli bir yer tutmaktadır (Bayerl & Akhgar, 2015; Trottier, 2017; Lyon, 2018). Bu kapsamda, bireylerin sosyal medya istihbaratına yönelik farkındalık düzeylerini ölçmek amacıyla geliştirilen ölçek, literatürdeki boşluğu doldurmayı hedeflemektedir. Bu çalışma, bireylerin sosyal medya istihbaratına yönelik farkındalığını ölçmeye yönelik bir ölçek geliştirmeyi amaçlamaktadır. Bu bağlamda, Koruma Motivasyon Teorisi (KMT; Rogers, 1975) ve Psikolojik Tepki Teorisi (PTT; Brehm, 1966) temel alınarak ölçek soruları oluşturulmuştur. Ölçek sorularında, kullanıcıların sosyal medya istihbaratına ilişkin geliştirdikleri savunma mekanizmalarını Koruma Motivasyon Teorisi ile açıklanmaya çalışılacaktır. Ölçek sorularında kullanıcıların ifade özgürlüğü ve gözetim algısı arasındaki ilişkisini ele almak için Psikolojik Tepki Teorisi'nden yararlanılacaktır.

1. Ölçme Aracının Geliştirilmesi

Bu çalışma, bireylerin sosyal medya istihbaratına yönelik farkındalık düzeylerini ölçmeye yönelik geçerli ve güvenilir bir ölçek geliştirmek amacıyla gerçekleştirilmiştir. Ölçek geliştirme sürecinde, literatür taraması, kavramsal çerçevenin oluşturulması, madde havuzunun hazırlanması, uzman görüşü ile kapsam geçerliliğinin sağlanması, pilot çalışma, test-tekrar test uygulaması ve güvenirlik analizleri gibi aşamalar takip edilmiştir.

1.1. Kavramsal Çerçevenin Oluşturulması ve Madde Havuzunun Geliştirilmesi

Sosyal medya istihbaratının ulusal güvenlik politikalarındaki rolü, bireylerin sosyal medya üzerindeki mahremiyet stratejileri ve gözetim karşısındaki tutumları gibi konular, literatürde önemli bir yer tutmaktadır (Bayerl & Akhgar, 2015; Trottier, 2017; Lyon, 2018). Bu kapsamda,

bireylerin sosyal medya istihbaratına yönelik farkındalık düzeylerini ölçmek amacıyla geliştirilen ölçek, literatürdeki boşluğu doldurmayı hedeflemektedir. Bu bağlamda, Koruma Motivasyon Teorisi (KMT; Rogers, 1975) ve Psikolojik Tepki Teorisi (PTT; Brehm, 1966) temel alınarak ölçek soruları oluşturulmuştur. Ölçek sorularında, kullanıcıların sosyal medya istihbaratına ilişkin geliştirdikleri savunma mekanizmaları Koruma Motivasyon Teorisi ile açıklanmaya çalışılacaktır. Ölçek sorularında kullanıcıların ifade özgürlüğü ve gözetim algısı arasındaki ilişkiyi ele almak için Psikolojik Tepki Teorisi'nden yararlanılacaktır.

Bireylerin tutum, kanaat, kaygı, beklenti ve farkındalık gibi gözlemlenemeyen ve ölçülemeyen özelliklerini açığa çıkarmak için ölçme araçları geliştirilmektedir. Bir toplumun ya da bireyin tutum, davranış ve inançlarının nedenlerini anlamak ve bu nedenler üzerinde etkili olan faktörlerin önem derecelerini belirlemek için en uygun istatistiksel yöntemlerden biri ölçek geliştirme sürecidir (Anderson, 1991: 241). Sosyal medya istihbaratına yönelik yapılan çalışmalar incelendiğinde, kullanıcıların bu konudaki farkındalık düzeylerini ölçmeye yönelik özgün bir ölçek geliştirilmediği görülmektedir. Bu durum, alanda gerçekleştirilecek bilimsel araştırmalarda kullanılabilecek geçerliliği ve güvenirliği kanıtlanmış bir ölçme aracına duyulan ihtiyacı gözler önüne sermektedir. Sosyal medya istihbaratı, literatürde çeşitli bağlamlar ile ele alınmış olmasına rağmen sosyal medya istihbaratı kavramına dair kullanıcıların farkındalık düzeylerini ve bu bağlamdaki tutumlarını ölçmeye yönelik geliştirilmiş kapsamlı ve sistematik bir ölçek geliştirilmemiştir. Bu nedenle, bu çalışmada geliştirilen ölçek, bireylerin gözetim algıları, güvenlik kaygıları ve sosyal medya kullanım alışkanlıkları ile ilişkili değişkenleri içerecek şekilde tasarlanmıştır. Ölçeğin teorik altyapısı Korunma Motivasyon Teorisi (KMT; Rogers, 1975) ve Psikolojik Tepki Teorisi (PTT; Brehm, 1966) temel kavramsal çerçeve olarak kullanılmıştır.

Korunma Motivasyon Teorisi (KMT), tehdit içeren her türlü durum için geçerlidir (Haag vd., 2021: 27). KMT bireylerin olası bir tehdide karşı tetikleyicilere karşı verdikleri reaksiyonlar için yaygın olarak kullanılan bir çerçevedir. Tetikleyiciler, bireyleri kendilerine ya da başkalarına zarar verebilecek davranışlardan uzak durmaya ve koruyucu önlemler almaya yönelten korku temelli mesajları içermektedir (Yıldız vd. 2022: 864). İlk kez Rogers (1975) tarafından insanların algılanan bir sağlık tehdidiyle ilgili olarak nasıl bir süreç izlediği ve nasıl tutumlar izlediğine yönelik sağlık psikolojisi bağlamında bir modelleme geliştirilmiş olup günümüzde siber güvenlik, dijital mahremiyet, sosyal medya kullanımı, fiziksel aktivite ve risk yönetimi gibi farklı alanlara

uyarlanmıştır (Maddux & Rogers, 1983; Floyd, Prentice-Dunn & Rogers, 2000; Plotnikoff vd., 2010). Birçok farklı alanlarda yaklaşık 30.000'den fazla çalışmada KMT geliştirilip test edildikten sonra koruma motivasyonuna yol açan bilişsel aracılık süreci hakkında daha somut bilgiler edinilmiştir (Shillair, 2020: 1).

KMT'ye göre bireyler, karşılaştıkları tehditleri, tehdit değerlendirmesi ve başa çıkma değerlendirmesi olmak üzere iki temel süreç üzerinden değerlendirir (Shillair, 2020). Örneğin bir birey, sosyal medya hesaplarının siber bir saldırı olasılığı ile karşı karşıya kaldığında ilk olarak tehdidin önemini değerlendirme sürecine girmektedir. Tehdit değerlendirmesi aşamasında, birey tehdidin önemini ve olası riskleri analiz etmektedir. Şayet daha önce benzer bir durumla karşılamışsa veya bu durumu yaşayanlar hakkında bir bilgiye sahipse, tehdide karşı daha ciddi yaklaşacaktır. Birey kendisine "Bu risk benim için ne kadar geçerli?" sorusunu sorarak tehdide maruz kalma olasılığını değerlendirmektedir. Örneğin hesap şifresinin tahmin edilebilir olduğunu biliyorsa veya başka bir alanda şifresini paylaşmışsa tehdit algısı daha çok artacaktır. Değerlendirme sürecini tamamladıktan sonra birey başa çıkma değerlendirmesi aşamasına geçer. Bu aşamada tehdit karşısında uygulanabilecek stratejileri ve önlemleri değerlendirir. Örneğin, şifreye rakam veya gizli karakterlerden ekleme veya iki faktörlü kimlik doğrulama kullanma metotlarını değerlendirir. Eğer bu önlemler doğrultusunda siber saldırının etkisiz olacağına inanırsa tehdit karşısında koruyucu bir yanıt geliştirme eğiliminde olur. Fakat siber tehditlerin önüne geçemeyeceğini ve önlemlerin bir işe yaramayacağını düşünürse, tehdit karşısında pasif bir tutum sergileyebilir veya riskli davranışlarını değiştirmeme eğiliminde olabilir. Bir başka deyişle sosyal medya kullanıcısı tehdit seviyesini yüksek görmesine rağmen başa çıkma değerlendirmesi sürecinde başarısız olacağına inanırsa pasif bir konumda olur. Fakat hem tehdidi büyük hem de korunma yöntemlerini etkili olarak algıladığında, koruyucu davranışlar sergileyecektir.

Son yıllarda KMT esas alınarak yapılan çalışmalar sonucunda algılanan tehdidin insanların güvenli e-posta servislerini kullanma niyetlerini olumlu yönde etkilediğini göstermiştir. Algılanan şiddet, kablosuz ağ kullanıcılarının güvenlik özellikleri yükleme kararlarını etkilemektedir. Bu aşamada insanlar casus yazılım önleme yazılımı kullanıp kullanmayacaklarının kararını vermektedirler. Çalışmalar neticesinde algılanan duyarlılığın koruyucu yazılım yükleme niyetlerini olumlu yönde etkilediği sonucunda ulaşılmıştır. Bir başka deyişle algılanan tehdit, bireylerin teknolojik kararlarını yönlendiren çok önemli bir faktördür (Zhang ve Zhang, 2024: 2).

Sosyal medya platformlarının güvenlik kurumları ve devletler tarafından istihbarat ve veri toplama amaçlı kullanılması, kullanıcılarda bir gözetim tehdidi algısı yaratmaktadır. Bu durumun önüne geçmek için farklı stratejiler geliştirmektedirler (Tsai vd., 2011). Kullanıcıların gözetim farkındalığı arttıkça, kişisel bilgilerini koruma yönünde aldıkları önlemler de güçlenmektedir (Acquisti, Brandimarte & Loewenstein, 2015). Örneğin ölçekte kullanılan, "Sosyal medya platformlarında dijital gözetime maruz kalmamak için gözetim karşıtı araçlar (VPN, anonim tarayıcılar, reklam engelleyiciler) kullanıyorum." maddesi, bireylerin gözetim tehdidine karşı bilinçli bir şekilde mahremiyet önlemleri almasını değerlendirmektedir. Sosyal medya kullanıcısının gözetlenebileceği tehdidine karşı kendisi ile uygulamış olduğu çözüm arasında açık bir ilişki kurmaktadır.

Literatürde ülkeler arasındaki gizlilik endişelerini karşılaştıran çalışmalar incelendiğinde farklılıkların kökeninde kültürel faktörlerin olduğuna ulaşılmıştır. Bir başka deyişle ulusal kültür gizlilik endişelerini doğrudan etkilemektedir (Zhang, Chen ve Wen, 2002; Lowry, Cao ve Everard, 2011). Nemati ve arkadaşlarının 2014 yılında yapmış olduğu çalışmada, farklı uluslardaki (ABD ve Çin) gizlilikle başa çıkma ve bilgi paylaşımı davranışı incelenmiştir. Çalışmada ABD'li katılımcılar gizlilikle başa çıkma stratejileri kullanma olasılıklarının Çinli katılımcılara göre daha yüksek olduğunu belirtmişlerdir. Yazarlar bu durumun Çinli katılımcıların kolektivist bir toplum yapısına sahip olduğundan dolayı gizliliğe dair endişelerinin arka planda kaldığını savunmuştur. Ayrıca uluslar arasındaki politik ve yasal farklılıklar veya sosyal medya platformlarındaki ve gizlilik kontrollerindeki farklılıklar da gizlilikle başa çıkma stratejilerini etkileyebilmektedir (Nemati vd., 2014: 242). KMT'ye göre, algılanan tehdit düzeyi ne kadar yüksekse, koruma motivasyonları da o kadar güçlüdür ve bireyler, kendilerini güvende hissetmek için proaktif savunma mekanizmaları geliştirirler (Rogers & Prentice-Dunn, 1997).

Hasan vd. 2024 yılında KMT teorisinden yararlanarak e-hizmet kullanıcılarının kendilerini siber dolandırıcılığa karşı koruma niyetini etkileyen faktörleri araştırmışlardır. Çalışmanın sonucunda siber güvenlik etkinliği, kaynak güvenilirliği ve yanıt etkinliğinin koruma davranışını olumlu yönde etkilediğine ulaşılmıştır. Bu durumu örnekle açıklamak gerekirse kullanıcı, anti-virüs kullanmanın cihazlarını korumada kendisine yardımcı olabileceğine inanırsa koruma davranışının da buna paralel olarak arttığı sonucuna ulaşmışlardır (Hasan vd, 2024). Bu çalışmadan hareketle ölçekte yer alan "Sosyal medya platformlarının istihbarat amacıyla kullanıldığında önemli bir

kaynak olduğunu düşünürüm." sorusuyla kullanıcının sosyal medya platformlarını kendisini ve yaşadığı coğrafyayı koruyucu bir araç olarak tanımlaması, korunma motivasyonunu artıran bir unsur olarak değerlendirilecektir.

Psikolojik Tepki Teorisi (PTT), bireylerin özgürlüklerinin tehdit altında olduğunu düşündüklerinde buna karşı bir direnç veya uyum geliştirme eğiliminde olduklarını savunur (Brehm, 1966). Dijital gözetim ve sosyal medya istihbaratının ifade özgürlüğü üzerindeki etkileri, bireylerin paylaşım alışkanlıklarını değiştirmesine veya oto-sansür uygulamalarına neden olabilmektedir (Stoycheff, 2016). Örneğin, "Sosyal medya platformlarında takip edilme korkusuyla aykırı sayılabilecek görüşlerimi asla paylaşmam." maddesi, bireylerin ifade özgürlüğü ile gözetim baskısı arasındaki ilişkiyi ölçmeye yöneliktir. Sosyal medya kullanıcılarının, devletin gözetim politikalarına bağlı olarak bilinçli veya bilinçsiz şekilde oto-sansür uygulamaları geliştirdiği gösterilmiştir (Penney, 2017). Özellikle kriz anlarında bireylerin sosyal medya kullanım alışkanlıkları değişmekte, politik ve toplumsal konulara dair görüşlerini ifade etmekten kaçınabilmektedirler. "Sosyal medya platformlarında herhangi bir kriz-kaos anında paylaşımda bulunurken gözetlenebileceğimi düşünerek paylaşımlarımda sansür kullanırım." maddesi, bireylerin devlet gözetiminin arttığı dönemlerde paylaşımlarını sınırlama eğiliminde olup olmadıklarını ölçmeye yöneliktir.

Sosyal medya gözetimi, sosyal medya kullanıcılarının ifade özgürlüğü, güvenlik anlayışı ve mahremiyet algıları ile doğrudan ilişkilidir. Literatürde, siber güvenlik ve mahremiyet farkındalığını ölçmeye yönelik çeşitli ölçekler geliştirilmiş olsa da doğrudan sosyal medya istihbaratına dair farkındalık düzeyini ölçmeye odaklanan bir ölçek bulunmamaktadır. 2014 yılında Keser ve Güldüren, Bilgi Güvenliği Farkındalık Ölçeği (BGFÖ) Geliştirme Çalışması ile üniversitede görev yapan öğretim elemanlarının bilgi güvenliği farkındalık düzeylerini belirlemeye yönelik bir ölçek geliştirmişlerdir. Yapı geçerliliği çalışmalarında ölçekte yer alan 34 madde 2 faktör (saldırı/tehditler ve kişisel verilerin korunması) altında toplanmış Cronbach alfa iç tutarlılık katsayısı .97 olarak hesaplanmıştır (Keser ve Güldüren, 2014). 2022 yılında Arpacı ve Ateş, Siber Suç Farkındalığı Ölçeği (SSFÖ) geliştirmişlerdir. 41 maddeden oluşan ölçeğin Cronbach alfa iç tutarlık kat sayısı ölçeğin tamamı için .97 olarak hesaplanmıştır. Ölçekte 3 alt boyut (siber ortamda yer alan suçlar, gizlilik ve güvenlik, siber ortama ve kişisel verilere yönelik suçlar) altında toplanmıştır. Karakuyu ve Ocak, 2024 yılında Dijital Vatandaş Farkındalık Ölçeği geliştirmişlerdir. Geliştirilen ölçekte 5 alt boyuttan (dijital güvenlik, dijital sağlık, dijital eğitim,

dijital saygı ve dijital uygulamalar) ve 37 maddeden oluşmaktadır. Çalışmanın güvenirlik katsayısı 0,935 olarak belirlenmiştir (Karakuyu ve Ocak, 2024).

Literatürde sosyal medya platformlarının istihbarat amaçlı kullanımı ve bireylerin bu duruma yönelik farkındalıkları sistematik olarak ele alınmamıştır. Bu eksikliği gidermek amacıyla geliştirilen ölçek, bireylerin sosyal medya istihbaratı ve gözetim karşısındaki savunma mekanizmaları (KMT) ile gözetim olgusunun özgürlük anlayışları üzerindeki etkisini (PTT) analiz etmeyi amaçlamaktadır. Çalışmada sosyal medya kullanıcılarının dijital gözetim, mahremiyet ve güvenlik arasındaki dengeyi nasıl yorumladıkları, istihbarat faaliyetlerine yönelik tutumları ve bu bağlamdaki farkındalık düzeyleri ölçek aracılığıyla değerlendirilecektir.

Ölçek geliştirme sürecinin ilk aşamasında, sosyal medya istihbaratı, dijital gözetim, mahremiyet algısı ve ifade özgürlüğü gibi kavramlar ele alınmış ve bu alanlarla ilgili uluslararası ve ulusal akademik çalışmalar detaylı bir şekilde incelenmiştir. Literatür taraması sürecinde, bireylerin sosyal medya istihbaratına yönelik algılarını şekillendiren temel unsurlar belirlenmiş ve ölçeğin teorik çerçevesi oluşturulmuştur. Literatürde yer alan çalışmalar doğrultusunda 33 maddeden oluşan bir madde havuzu oluşturulmuştur. Madde havuzu oluşturulurken, maddelerin açık, yalın ve ölçülebilir olmasına özen gösterilmiştir. Ayrıca, her bir maddeyi teorik çerçeveyle ilişkilendirecek şekilde ölçek tasarlanmıştır.

2. Uzman Görüşü ile İçerik Geçerliği Analizi

Oluşturulan madde havuzunun geçerliliğini değerlendirmek ve ölçeğin ölçmeyi amaçladığı kavramları kapsayıp kapsamadığını test etmek amacıyla, akademisyenlerden görüş alınmıştır. 3'ü iletişim fakültesinden, 1'i eğitim bilimleri fakültesinden ve 1'i iktisadi ve idari bilimler fakültesinden olmak üzere toplam 5 akademisyene ölçek maddeleri sunulmuş ve kapsam geçerliği açısından değerlendirmeleri istenmiştir. Uzmanlardan, ölçek maddelerinin anlaşılırlığı, açıklığı, ilgili kavramı ölçme yeterliliği ve ölçek genelinde dengeli bir yapı sergileyip sergilemediği hakkında geri bildirimleri alınmıştır. Uzman görüşleri doğrultusunda ifadeler; farkındalık ifadesi olup olmadığı ve çalışmanın amacı ve kapsamı açısından ifadeler değerlendirilmiştir.

3. Pilot Çalışma ve Ön Test Uygulaması

Yenilenen ölçek, ölçek maddelerinin anlaşılabilirliğini ve istatistiksel olarak uygunluğunu test etmek amacıyla 70 kişilik bir katılımcı grubuna uygulanmıştır. Pilot çalışmaya katılan bireyler

rastgele belirlenmiş sosyal medya kullanıcılarından oluşmaktadır. Katılımcılar, yaş, cinsiyet, eğitim durumu gibi değişkenler açısından çeşitlilik göstermektedir. Pilot çalışmada yer alan maddeler, beşli Likert tipi ölçek yapısına uygun olarak "Kesinlikle katılmıyorum (1)" ile "Kesinlikle katılıyorum (5)" arasında derecelendirilmiştir. Katılımcıların ifadeleri dikkatli okuyup okumadıklarını değerlendirebilmek amacıyla, 14. madde kontrol sorusu olarak "Bu maddeyi boş bırakıp bir sonraki maddeye geçiniz." biçiminde tasarlanmıştır. Bu uygulama, ölçeğin geçerlik düzeyini artırmaya ve yanıtların özenli bir şekilde verilmesini sağlamaya yönelik bir strateji olarak benimsenmiştir

Ölçeğin pilot çalışması için toplam 33 madde, taslak ölçek haline dönüştürülmüştür. Katılımcıların ölçek sorularına verdikleri yanıt puanlanmasında, olumlu maddeler için 5, 4, 3, 2, 1; olumsuz maddeler için ise 1, 2, 3, 4, 5 şeklinde puanlama sisteminden yararlanılmıştır. Sosyal Medya İstihbaratı Farkındalık Ölçeğinden katılımcıların alabileceği en yüksek skor 165 puan olup, minimum skor ise 33 olacaktır. Pilot uygulamanın amacı, ölçeğin zamana bağlı güvenilirliğini test etmektir. Bu doğrultuda, ölçek aynı 64 kişilik katılımcı grubuna 2 haftalık aralıklarla iki kez uygulanmıştır. 64 katılımcıdan birinci uygulamada yanıt olarak verdikleri rumuz/ad-soyadı bilgilerinin ikinci uygulamada eşleşmesi gerektiği hususunda özellikle belirtilmiştir.

SPSS 27 programı kullanılarak pilot çalışmanın geçerlik ve güvenirlik analizleri gerçekleştirilmiştir. Bu aşamada ölçeğin güvenilirliğini değerlendirmek amacıyla, her bir ifadenin madde-toplam puan korelasyonları ile Cronbach Alpha iç tutarlılık katsayısı hesaplanmıştır. Gerçekleştirilen pilot çalışmada yüksek korelasyona sahip olan maddeler ile madde-toplam korelasyonu 0.80'in üzerinde olan maddeler belirlenerek ölçeğin nihai formuna dahil edilmiştir.

4. Ölçeğin Uygulanması

Geliştirilen Sosyal Medya İstihbaratı Farkındalığı Ölçeği (SMİFÖ), ölçeğin geçerlilik ve güvenilirlik analizlerini gerçekleştirmek amacıyla geniş bir katılımcı kitlesine uygulanmıştır. Çalışma kapsamında dördü demografik özellikler, iki sosyal medya kullanım düzeyi ve on beş sosyal medya gözetimi ve istihbarat algısına yönelik beşli Likert tipte olmak üzere toplam yirmi bir soru ve ifadeden oluşan bir anket oluşturulmuştur. Kontrol maddesi ile toplam 34 maddeden oluşan ölçek, 1 Mart 2025 - 1 Nisan 2025 tarihleri arasında çevrimiçi anket yöntemi ile veri toplanarak uygulanmıştır. Bu çalışma için etik kurul izni Ankara Hacı Bayram Veli Üniversitesi

Etik Komisyonu'nun 28.01.2025 tarihinde 02 numaralı toplantısında görüşülmüş olup 2025/82 araştırma kodu ile oybirliğiyle alınmıştır.

Örneklem büyüklüğü, madde ya da faktör sayısı gibi göreli kriterlere dayalı olarak belirlendiğinden, ölçek çalışmalarında genellikle madde sayısının 5 ila 10 katı kadar katılımcıya ulaşılması önerilmektedir (Kass & Tinsley, 1979). Kline (1994) ise, örneklem büyüklüğüne ilişkin mutlak bir ölçüt olarak en az 200 katılımcının yeterli olacağını belirtmekle birlikte, daha büyük örneklemlerle çalışmanın daha sağlıklı sonuçlar vereceğini ifade etmektedir. Bu doğrultuda yürütülen uygulamada, sosyal medya kullanıcılarından oluşan 200 kişilik bir örnekleme erişilmiştir. Katılımcılar, ölçeği tamamen gönüllülük esasına dayalı olarak doldurmuşlardır. Katılımcılar rastgele seçilmiş olup, belirli bir yaş, cinsiyet veya eğitim düzeyi kriterine bağlı olmaksızın, sosyal medya kullanımıyla ilişkili geniş bir demografik yelpazeyi temsil etmeleri amaçlanmıştır.

Ölçek uygulamasının ardından, toplam 220 ölçek incelemeye alınmış, kontrol maddesindeki tutarsız cevaplar nedeniyle 20 ölçek değerlendirme dışı bırakılmıştır. Kontrol maddesi, katılımcıların anketi dikkatli bir şekilde doldurup doldurmadığını belirlemek amacıyla ölçeğe eklenmiştir. Tutarsız veya rastgele doldurulduğu tespit edilen yanıtlar, güvenilirliği artırmak amacıyla analiz kapsamına alınmamıştır. Bu aşamada elde edilen veriler, istatistiksel analizler için hazırlanmış ve ölçeğin yapı geçerliği, iç tutarlılığı ve faktör analizi testlerine tabi tutulmuştur.

5. Bulgular

Araştırmada elde edilen verilerin analizinde SPSS-27 yazılımı kullanılmıştır. Ölçeğin faktör yapısını ortaya koymak amacıyla keşfedici faktör analizi gerçekleştirilmiş; belirlenen faktörlerin model uyumu ise AMOS-22 programı aracılığıyla doğrulayıcı faktör analizi ile test edilmiştir. Tüm istatistiksel analizler %5 anlamlılık düzeyinde (α=0,05) yürütülmüştür.

5.1. Verilerin Faktör Analizi İçin Uygunluğunun Değerlendirilmesi

Sosyal medya istihbaratı farkındalığı ölçeğinin yapı geçerliliğini değerlendirmek amacıyla faktör analizine başvurulmuştur. Analiz öncesinde verilerin faktör analizine uygunluğunu belirlemek üzere Kaiser-Meyer-Olkin (KMO) katsayısı hesaplanmış ve Bartlett's Küresellik Testi uygulanmıştır. Literatürde, örneklem yeterliliği ve veri setinin faktör analizine elverişliliği için KMO değerinin 0.60'ın üzerinde olması gerektiği belirtilmektedir (Büyüköztürk, 2009, s. 117).

Bu çalışmada açımlayıcı faktör analizi sonucunda KMO değeri .706 olarak saptanmıştır. Ayrıca Bartlett's testinin anlamlılık düzeyi [$\chi^2 = 2685.365$, $p = .000$] olarak bulunmuş ve bu sonuca göre verilerin faktör analizine uygun olduğu anlaşılmıştır. İlgili KMO ve Bartlett's test sonuçları Tablo 1'de sunulmuştur.

Tablo 1: KMO ve Bartlett's test değerleri.

Kaiser-Meyer-Olkin		,706
Bartlett's Testi	χ 2	2685,365
	Serbestlik derecesi	105
	Sig.	,000

KMO katsayısı ve Barlett küresellik testi sonuçları incelendiğinde ölçeğin faktör analizine uygun olduğu görülmektedir. Ölçekteki faktörlerin kendileriyle yüksek ilişki içerisinde olan maddelerin belirlenebilmesi için Tablo 2'de faktör analizi yapılmıştır.

Tablo 2: Sosyal medya istihbaratı farkındalık ölçeği maddeleri ve faktör yükleri.

Maddeler	**F1**	**F2**	**F3**	**F4**	**F5**	**Boyut Güv.**	**Ölçek Güv.**
SMİF15. Sosyal medya verilerinin, istihbarat faaliyetleri için önemli bir kaynak olduğunu düşünüyorum.	,999					,932	,763
SMİF13. Kriz zamanlarında, izlenme korkusu nedeniyle paylaşımlarımda sansür uygulama eğilimindeyim.	,873						
SMİF4. Sosyal medya bilgilerimin, benim bilgim olmadan kamu kurumları veya şirketler tarafından ele geçirilip depolanamayacağını düşünüyorum.		,979				,932	

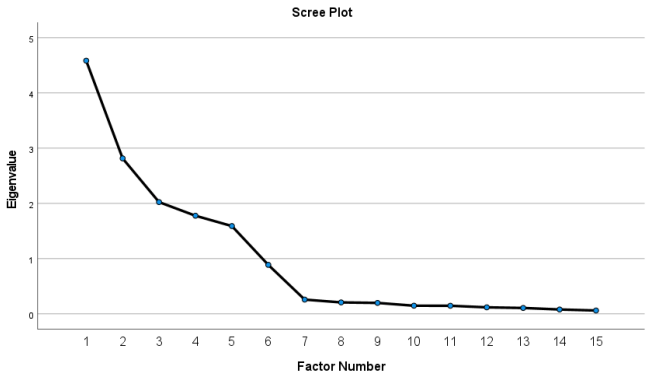
SMİF5. Ticari şirketlerin, sosyal medya verilerime benim iznim olmadan erişemeyeceğini düşünüyorum.	,930			
SMİF6. Sosyal medya platformlarında dijital olarak izlenme hissediyorum.	,894			
SMİF1. Sosyal medya platformlarında kişisel bilgilerime benim iznim dışında kimse tarafından erişilemediğini düşünüyorum.	,744			
SMİF3. Yasa dışı bir faaliyet olmadığı sürece, kamu kuruluşlarının sosyal medya aracılığıyla beni gözetlemediğini düşünüyorum.	,681			
SMİF2. Gizlilik ayarlarımı doğru kullandığımda, bilgilerime yalnızca izin verdiğim kişilerin ulaşabildiğini düşünüyorum.	,627			
SMİF9. Sosyal medya profilimin tamamen açık olması, kişisel kimliğimin ortaya çıkmasına neden olmaktadır.		,987		
SMİF7. Dijital gözetimden kaçınmak için VPN, anonim tarayıcı veya reklam engelleyici gibi teknolojik araçlar kullanıyorum.		,862		,918
SMİF10. Gönderi oluştururken, paylaşımlarımın içerik ve konum bilgilerini dikkatle seçiyorum.			,971	,941

SMİF11. Sosyal medyada takip edilme endişesi nedeniyle, bazı görüşlerimi paylaşmaktan kaçınıyorum.		,904			
SMİF12. Herhangi bir kriz (doğal afet, kaza, saldırı vb.) anında, sosyal medyada bilgi kaynağı olmayı isterim.		,880			
SMİF16. Sosyal medyanın istihbarat amaçlı kullanılmasının, ifade özgürlüğünü kısıtlayabileceğini düşünüyorum.			,971		
SMİF17. Ulusal güvenliği sağlamak amacıyla, sosyal medya platformlarının gözetlenmesi gerektiğini düşünüyorum.			,879	,923	
Açıklanan Varyans:	**%30,56**	**%18,77**	**%13,49**	**%11,85**	**%10,60** **Toplam: %85,26**
KMO: ,706	**χ^2:2685,365**				**Sd:105 Sig: ,000**

Keşfedici faktör analizi neticesinde, maddelerin 5 faktörden oluşan, toplam varyansın %85,26'sını açıklayan bir yapıda olduğu görülmüştür. 1.faktör toplam varyansın %30,56'sını, 2.faktör toplam varyansın %18,77'sini, 3.faktör toplam varyansın %13,49'unu, 4.faktör toplam varyansın %11,85'ini, 5.faktör toplam varyansın %10,60'ını açıklamaktadır. Yapılan keşfedici faktör analizi sonucunda 13 ve 15 numaralı maddeler 1.faktörün altında, 1, 2, 3, 4, 5 ve 6 numaralı maddeler 2.faktörün altında, 7 ve 9 numaralı maddeler 3.faktörün altında, 10, 11 ve 12 numaralı maddeler 4.faktörün altında, 16 ve 17 numaralı maddeler 5.faktörün altında toplanmıştır. 8 ve 14 numaralı maddeler yetersiz faktör yükü dolayısıyla ölçekten çıkarılmıştır. 5 faktör için ve toplam puan için uygulanan güvenilirlik analizlerine ve ölçeğin toplam puanına göre Cronbach's Alpha değerlerinin yeterli seviyede olduğu görülmektedir.

5.2. Faktör Sayısının Belirlenmesi

Çalışmanın ilk aşamasında ölçeğe ait faktör sayısı tespit edilmiştir. Ölçeğe ait faktör sayısını belirleyebilmek için Şekil 1'de gösterilen yamaç-birikinti grafiği oluşturulmuştur.

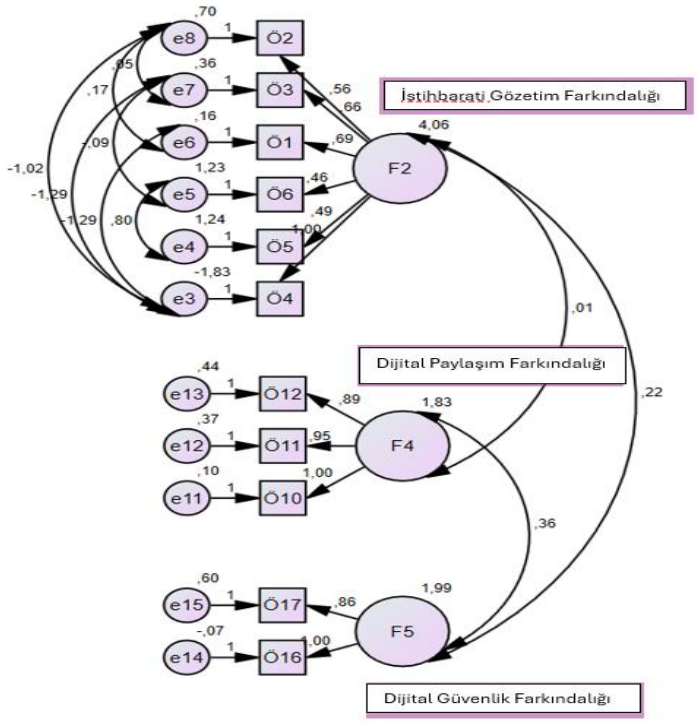


Şekil 1. Faktör sayısını gösterir çizgi grafiği.

Şekil 1'de görüldüğü 1, 2 ve 3 numaralı faktörlerde yüksek ivmeli hızlı düşüşler gözlemlenmektedir. Grafikte gözle görünebilen bu dik yamaç, söz konusu faktörlerin veri setindeki varyansın büyük kısmını açıkladığını göstermektedir. Grafikte 3. faktörden itibaren düşüş ivmesinin azaldığı görülmektedir. Grafikte 5. ve 7. faktör arasında yeniden dikkat çekici bir düşüş yaşandığı görülmektedir. Buna karşın, 7. faktörden sonra grafik belirgin şekilde yataylaşmakta, özdeğerler birbirine çok yakın seyretmekte ve anlamlı katkı azalmaktadır. 7 numaralı faktörden itibaren ise düşüş hızı yavaşlayarak eğim plato yapmaktadır. 7 numaralı faktörden sonra bileşenlerin varyansa yaptıkları katkı neredeyse birbirine çok yakındır. 1, 2 ve 3 numaralı faktörlerin ölçeğin toplam varyansın %62,82'sini açıkladığı göz önünde bulundurularak 1. ila 3. faktörlerin veri setindeki yapıyı açıklamada belirleyici olduğu, sonraki faktörlerin ise anlamlı katkılarının sınırlı olduğu saptanmıştır.

5.3. Doğrulayıcı Faktör Analizi

Doğrulayıcı Faktör Analizi bir ölçekte çok sayıda gözlenen veya ölçülen değişken tarafından temsil edilen gizil yapıları içeren, çok değişkenli istatistiksel analizleri tanımlamak için kullanılmaktadır (Aytaç ve Öngen, 2012: 16). Doğrulayıcı Faktör Analizi (DFA); Açıklayıcı Faktör Analizi (AFA) aracılığıyla tespit edilen alt boyutların (faktör), hipotez yardımı ile oluşturulmuş alt boyutlara uygunluğunu değerlendirmek amacıyla kullanılmaktadır (Evci & Aylar, 2017: 398).



Şekil 2: Doğrulayıcı faktör analizi.

Doğrulayıcı Faktör Analizi neticesinde elde edilen değişkenlerin ilişkilendirilmesi yapılmış, oluşturulan DFA modeline ait uyum ve anlamlılık katsayılarının kabul arasında olduğu saptanmıştır. Şekil 1'de oluşturulmuş olan 11 maddeli ve 3 faktörlü yapıya ait verilerin uyumlu olduğu görülmektedir. Gerçekleştirilen analiz sonucunda, faktör yüklerinin .46 ile 1.00 arasında değiştiği ve tüm maddelerin ait oldukları faktörlerle anlamlı ilişkiler kurduğu belirlenmiştir. Faktörler arası ilişkilere bakıldığında; F2 ile F4 arasında oldukça düşük (,01), F2 ile F5 arasında orta düzeyde (,36) ve F4 ile F5 arasında düşük düzeyde (,22) pozitif korelasyonlar elde edilmiştir. Bu bulgular, ölçeğin alt boyutlarının kuramsal olarak birbirinden ayrıldığını ve her bir faktörün bağımsız bir yapıyı temsil ettiğini göstermektedir.

Tablo 3: Doğrulayıcı faktör analizi değerleri.

Faktörler	**İfadeler**	**Faktör Yükü**	**Standart Hata**	**t değeri**	**p değeri**

Dijital Güvenlik Farkındalığı

İstihbarati Gözetim Farkındalığı	Sosyal medya platformlarında kişisel bilgilerime benim iznim dışında kimse tarafından erişilemediğini düşünüyorum.	0.7	0.057	8.675	***
İstihbarati Gözetim Farkındalığı	Gizlilik ayarlarımı doğru kullandığımda, bilgilerime yalnızca izin verdiğim kişilerin ulaşabildiğini düşünüyorum.	0.56	0.058	11.428	***
İstihbarati Gözetim Farkındalığı	Yasa dışı bir faaliyet olmadığı sürece, kamu kuruluşlarının sosyal medya aracılığıyla beni gözetlemediğini düşünüyorum.	0.66	0.052	13.327	***
İstihbarati Gözetim Farkındalığı	Sosyal medya bilgilerimin, benim bilgim olmadan kamu kurumları veya şirketler tarafından ele geçirilip depolanamayacağını düşünüyorum.	0.46	0.054	8.609	***
İstihbarati Gözetim Farkındalığı	Ticari şirketlerin, sosyal medya verilerime benim iznim olmadan erişemeyeceğini düşünüyorum.	0.49	0.057	9.831	***
İstihbarati Gözetim Farkındalığı	Sosyal medya platformlarında dijital olarak izlenme hissediyorum.	1.0	-	-	-
Dijital Paylaşım Farkındalığı	Sosyal medya üzerinden izlenme hissinin, çevrimiçi özgürlüğümü kısıtladığını düşünüyorum.	0.89	0.04	23.463	***
Dijital Paylaşım Farkındalığı	Dijital gözetimden kaçınmak için VPN, anonim tarayıcı veya reklam engelleyici gibi teknolojik araçlar kullanıyorum.	0.95	0.042	21.352	***

Dijital Paylaşım Farkındalığı	Sosyal medya profilimin tamamen açık olması, kişisel kimliğimin ortaya çıkmasına neden olmaktadır.	1.0	-	-	-
Dijital Güvenlik Farkındalığı	Sosyal medya verilerinin, istihbarat faaliyetleri için önemli bir kaynak olduğunu düşünüyorum.	0.86	0.153	5.621	***
Dijital Güvenlik Farkındalığı	Sosyal medyanın istihbarat amaçlı kullanılmasının, ifade özgürlüğünü kısıtlayabileceğini düşünüyorum.	1.0	-	-	-

İlk faktör altında toplanan altı madde, bireylerin sosyal medya ortamında kamu kurumları veya özel şirketler tarafından izlenme, verilerinin izinsiz erişilmesi ya da depolanması gibi dijital gözetim süreçlerine yönelik algılarını yansıtmaktadır. Bu nedenle bu faktör, "İstihbaratî Gözetim Farkındalığı" olarak adlandırılmıştır. Maddelerin faktör yükleri 0.46 ile 1.00 arasında değişmekte olup tamamı istatistiksel olarak anlamlıdır ($p < .001$). Özellikle dijital olarak izlenme hissine dair ifadenin 1.00 gibi yüksek bir faktör yüküne sahip olması, bu boyuttaki farkındalığın belirgin düzeyde olduğunu ortaya koymaktadır.

İkinci faktörde yer alan üç madde, bireylerin sosyal medya kullanımında içerik paylaşımı öncesinde gösterdiği öz denetimi, mahremiyet kaygısını ve dijital görünürlüğe ilişkin tutumlarını kapsamaktadır. Bu boyut, bireyin sosyal medya ortamındaki paylaşım sınırlamaları ve kişisel görünürlük kontrolü ile olan ilişkisini temsil etmektedir. Maddelerin yüksek faktör yükleri (0.89–1.00) ve özellikle VPN, reklam engelleyici, anonim tarayıcı gibi araçların kullanımına ilişkin farkındalık düzeyi dikkate alındığında bu faktör, "Dijital Paylaşım Farkındalığı" olarak adlandırılmıştır. Bu isimlendirme, faktörün sadece teknik gizlilik davranışlarını değil, aynı zamanda paylaşım davranışı üzerindeki bilişsel ve duygusal etkileri kapsamasından dolayı tercih edilmiştir.

Üçüncü faktörde yer alan iki madde ise sosyal medya verilerinin istihbarat faaliyetlerinde kullanılması ve bu durumun bireylerin ifade özgürlüğü üzerindeki etkisiyle ilgilidir. Yüksek faktör yüklerine sahip bu maddeler (0.86 ve 1.00), bireylerin sosyal medya aracılığıyla veri

toplanmasının, kamu denetimi ya da güvenlik gerekçesiyle sınırlandırıcı etkiler yaratabileceğine dair farkındalıklarını yansıtmaktadır. Bu nedenle, bu faktör "Dijital Güvenlik Farkındalığı" olarak adlandırılmıştır. Bu isim, hem bireysel dijital hakların korunmasına dair farkındalığı hem de istihbarat odaklı veri kullanımına karşı geliştirilen bilişsel duyarlılığı içermektedir.

Gerçekleştirilen analizin değerlerine göre 11 maddenin faktör yükü 0,46 ile 1 arasında değişmektedir. Literatürde faktör yük değerleri ile ilgili olarak minimum 0,40'in üzerinde olmasının madde seçiminde yeterli olduğu söylenmektedir (Kozak, 2017). Genel olarak analiz bulguları, üç faktörlü yapının hem kuramsal olarak anlamlı hem de istatistiksel olarak güçlü olduğunu göstermekte; ölçeğin geçerli ve güvenilir bir ölçme aracı olduğunu desteklemektedir.

Tablo 4: Sosyal medya istihbaratı farkındalık ölçeği çok faktörlü modeline ilişkin sonuçları.

Faktörler	**İfadeler**	**Faktör Yükü**	**Standart Hata**	**t**	**p**
Faktör 1	4	,999			
	5	,667	,057	8,675	***
	6	,645	,054	8,609	***
	1	,962	,052	13,327	***
	3	,911	,058	11,428	***
	2	,803	,057	9,831	***
Faktör 2	10	,973			
	11	,904	,040	23,463	***
	12	,876	,042	21,352	***
Faktör 3	16	,999			
	17	,843	,153	5,621	***

***p<0.05

Tablo 4'de Sosyal Medya İstihbaratı Farkındalık Ölçeğinin Çok Faktörlü Modeline İlişkin sonuçlarına yer verilmiştir. Analiz sonucunda bütün faktör yüklerinin 0.30'un üzerinde çıkması

sonucu kabul edilebilir seviyede olduğuna ulaşılmıştır. Standart hata değerleri de değerlendirildiğinde, faktör yüklerinin istatistiksel olarak anlamlı olduğu ve modelin güçlü bir faktör yapısına sahip olduğu gözlemlenmiştir. Diğer değişkenler arası korelasyonlar incelendiğinde modeldeki değişkenlerin ilgili faktörleri güçlü bir şekilde temsil ettiği sonucuna ulaşılmıştır.

Tablo 5: Yapısal modelin uyum iyiliği değerleri.

	Yapısal Modeli Değerleri	Tavsiye Edilen Değerler
χ2/df	1,311	≤ 5
RMSEA	,040	≤0,1
CFI	,995	≥0,80
IFI	,995	≥0,80
TLI	,992	≥0,80
NFI	,980	≥0,80
GFI	,962	≥0,80
SRMR	,083	≤0,10
χ2: 2192,798; df:55; p:0,000		

Doğrulayıcı faktör analizi (DFA) kapsamında yürütülen yapısal eşitlik modellemesi (Structural Equation Modeling) sonucunda, modelin genel uyumu istatistiksel olarak anlamlı bulunmuştur (p = 0.000). Analiz bulgularına göre, ölçeği oluşturan 11 madde, üç alt boyuttan oluşan yapısal modele anlamlı düzeyde yüklenmektedir (Tablo 5). Modelin uyum indekslerini artırmak amacıyla yapılan modifikasyonlarda, modelin uyumuna olumsuz etki eden değişkenler tespit edilmiş ve yüksek artık korelasyonlara sahip hata terimleri arasında ek kovaryans yolları tanımlanarak model iyileştirilmiştir.

SONUÇ

Bu çalışmada, sosyal medya kullanıcılarının sosyal medya istihbaratına ilişkin farkındalık düzeylerini belirlemeye yönelik bir ölçme aracı geliştirilmesi amaçlanmış ve bu doğrultuda Sosyal Medya İstihbarat Farkındalığı Ölçeği (SMİFÖ) yapılandırılmıştır. Ölçeğin yapı geçerliğini test etmek amacıyla, öncelikle 33 maddeden oluşan pilot form, aynı sosyal medya kullanıcılarından oluşan bir gruba iki hafta arayla iki kez uygulanmıştır. Elde edilen geri bildirimler ve madde analizleri doğrultusunda ölçek yenilenmiş ve nihai haliyle 200 kişilik bir örneklem grubuna uygulanmıştır.

Ölçeğin faktör yapısını ortaya koymak amacıyla öncelikle açımlayıcı faktör analizi gerçekleştirilmiş ve üç faktörlü bir yapı elde edilmiştir. Bu faktör yapısının doğruluğunu test etmek amacıyla yapılan doğrulayıcı faktör analizi sonucunda, modelin veriyle oldukça yüksek düzeyde uyum gösterdiği belirlenmiştir. Elde edilen model uyum indeksleri (χ^2/df, CFI, TLI, RMSEA, SRMR) ölçüt değerlere uygun bulunmuş ve bu doğrultuda, AFA ile ortaya konan yapının DFA ile de desteklendiği, yani ölçeğin yapı geçerliğinin sağlandığı sonucuna ulaşılmıştır. Ölçeğin iç tutarlılığını ve güvenirliğini belirlemek amacıyla tüm ölçek ve alt faktörler için Cronbach's α katsayıları hesaplanmıştır. Yapılan analiz sonucunda, faktörlerden ikisinin yüksek düzeyde, diğer ikisinin ise oldukça yeterli düzeyde güvenirlik sergilediği görülmüştür. Ölçeğin genel güvenirlik düzeyi ise $\alpha = 0.706$ olarak bulunmuş ve bu değer doğrultusunda geliştirilen ölçeğin güvenilir bir ölçme aracı olduğu sonucuna varılmıştır.

Bu çalışmada geliştirilen Sosyal Medya İstihbarat Farkındalığı Ölçeğinin yapı geçerliğini değerlendirmek amacıyla uygulanan doğrulayıcı faktör analizi sonucunda, ölçeğin üç faktörlü bir yapıya sahip olduğu belirlenmiştir. Ölçek maddeleri, teorik temellere uygun şekilde anlamlı faktör yükleriyle yerleşmiş ve elde edilen değerler ölçeğin geçerliğini desteklemiştir. Faktör yapısı hem istatistiksel hem de kavramsal açıdan tutarlılık göstermektedir.

İlk faktörde yer alan altı madde, bireylerin sosyal medya üzerinden gözetlenme, verilerinin izinsiz erişilmesi ve kamu ya da özel kurumlar tarafından izlenme olasılığına ilişkin algılarını yansıtmaktadır. Bu nedenle ilgili boyut "İstihbaratî Gözetim Farkındalığı" olarak adlandırılmıştır. İkinci faktördeki üç madde, bireylerin sosyal medyada içerik paylaşımı öncesindeki öz denetimleri ile ilgilidir; bu nedenle "Dijital Paylaşım Farkındalığı" ifadesi uygun görülmüştür. Üçüncü faktörde yer alan iki madde ise sosyal medya verilerinin istihbarat amaçlı kullanımına ve bu durumun ifade özgürlüğü üzerindeki etkilerine dair farkındalığı ölçmektedir. Bu doğrultuda bu boyut, "Dijital Güvenlik Farkındalığı" olarak isimlendirilmiştir.

Elde edilen bulgular, Sosyal Medya İstihbarat Farkındalığı Ölçeğinin bireylerin dijital ortamlardaki gözetlenme, veri güvenliği ve paylaşım davranışlarına ilişkin farkındalık düzeylerini geçerli ve güvenilir bir şekilde ölçebilecek nitelikte olduğunu ortaya koymaktadır. Bundan sonraki araştırmalarda, farklı sosyal medya platformlarda yürütülen gözetim uygulamaları ile karşılaştırmalar yapılabilir; ayrıca sosyal medya istihbaratı farkındalığının, teknoloji kullanımı, dijital okuryazarlık, ifade özgürlüğü ve kişisel veri güvenliği gibi değişkenlerle ilişkisi çeşitli

ölçekler aracılığıyla incelenebilir. Çalışmanın, sosyal medya ve istihbarat ilişkisine yönelik bireysel algıların anlaşılmasına katkı sağlayarak alandaki akademik literatüre özgün bir katkı sunması beklenmektedir.

KAYNAKÇA

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science*, 347(6221), 509–514. https://doi.org/10.1126/science.aaa1465

Aggarwal, C. C. (2011). An introduction to social network data analytics. In C. C. Aggarwal (Ed.), *Social network data analytics* (pp. 1–15). Springer. https://doi.org/10.1007/978-1-4419-8462 3_1

Anderson, L. W. (1991). Tutumların ölçülmesi (N. Çıkrıkçı, Çev.). *Ankara Üniversitesi Eğitim Bilimleri Fakültesi Dergisi*, 24(1), 241–250.

Arpaci, I., & Ateş, E. (2023). Development of the cybercrime awareness scale (CAS): A validity and reliability study in a Turkish sample. *Online Information Review*, 47(4), 633–643. https://doi.org/10.1108/OIR-01-2022-0023

Aytaç, M., & Öngen, B. (2012). Doğrulayıcı faktör analizi ile Yeni Çevresel Paradigma Ölçeği'nin yapı geçerliliğinin incelenmesi. *JSSA*, 5(1), 14–22.

Bayerl, P. S., & Akhgar, B. (2015). *Open source intelligence investigation: From strategy to implementation*. Springer.

Bertram, S. (2016). Terrorist use of social media and challenges to state security. *Journal of Terrorism Studies,* 4(2), 53–68.

Brehm, J. W. (1966). *A theory of psychological reactance*. Academic Press.

Cerrah, A. E., & Dağlar Macar, O. (2022). Ulusal güvenlik tehdidi boyutunda sosyal medya incelemesi. *Working Paper Series,* 3(3), 94–106.

D'Arcy, J., & Greene, G. (2014). Security culture and the employment relationship as drivers of employees' security compliance. *Information Management & Computer Security,* 22(1), 2–18. https://doi.org/10.1108/IMCS-08-2013-0064

Dover, R. (2019). The perpetual and pervasive impact of intelligence on the modern world. *Intelligence and National Security,* 34(3), 345–361. https://doi.org/10.1080/02684527.2018.1558694

Evci, N., & Aylar, F. (2017). Derleme: Ölçek geliştirme çalışmalarında doğrulayıcı faktör analizinin kullanımı. *Sosyal Bilimler Dergisi,* 4(10), 389–412.

Floyd, D. L., Prentice-Dunn, S., & Rogers, R. W. (2000). A meta-analysis of research on protection motivation theory. *Journal of Applied Social Psychology,* 30(2), 407–429.

Haag, S., Siponen, M., & Liu, F. (2021). Protection Motivation Theory in information systems security research. *ACM SIGMIS Database,* 52(2), 25–67.

Hasan, S., Ahmad, R., Katuk, N., Ghazali, N. N., Aripin, J. A., & Ali, F. (2024). Staying one step ahead: Exploring Protection Motivation Theory to combat cyber-fraud among e-services users. *Procedia Computer Science,* 234, 1364–1371.

Holt, T. J., & Bossler, A. M. (2016). *Cybercrime in progress: Theory and prevention of technology enabled offenses.* Routledge.

Karakuyu, A., & Ocak, G. (2024). Dijital vatandaş farkındalık ölçeği geliştirme çalışması. *Cumhuriyet International Journal of Education,* 13(2), 316–326.

Kass, R. A., & Tinsley, H. E. A. (1979). Factor analysis. *Journal of Leisure Research,* 11, 120–138.

Keser, H., & Güldüren, C. (2014). Bilgi Güvenliği Farkındalık Ölçeği (BGFÖ) geliştirme çalışması. *Kastamonu Üniversitesi Kastamonu Eğitim Dergisi,* 23(3), 1167–1184.

Kline, P. (1994). *An easy guide to factor analysis*. Routledge.

Kozak, M. (2017). *Veri analizi: Bilimsel araştırma: Tasarım, yazım ve yayım teknikleri* (8. bs.). Detay Yayıncılık.

Lowry, P. B., Cao, J., & Everard, A. (2011). Privacy concerns versus desire for interpersonal awareness in driving the use of self-disclosure technologies: The case of instant messaging in two cultures. *Journal of Management Information Systems,* 27(4), 163–200.

Lyon, D. (2018). *The culture of surveillance: Watching as a way of life*. Polity.

Maddux, J. E., & Rogers, R. W. (1983). Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. *Journal of Experimental Social Psychology,* 19(5), 469 479.

Nemati, H., Wall, J. D., & Chow, A. (2014). Privacy coping and information-sharing behaviors in social media: A comparison of Chinese and U.S. users. *Journal of Global Information Technology Management,* 17(4), 228–249.

Omand, D., Bartlett, J., & Miller, C. (2012). Introducing social media intelligence (SOCMINT). *Intelligence and National Security,* 27(6), 801–823. https://doi.org/10.1080/02684527.2012.716965

Penney, J. (2017). Internet surveillance, regulation, and chilling effects online: A comparative case study. *Internet Policy Review,* 6(2), 1–22. https://doi.org/10.14763/2017.2.708

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *Journal of Psychology,* 91(1), 93–114.

Rogers, R. W., & Prentice-Dunn, S. (1997). Protection motivation theory. In D. S. Gochman (Ed.), *Handbook of health behavior research 1: Personal and social determinants* (pp. 113–132). Springer.

Schneier, B. (2015). Data and Goliath: The hidden battles to collect your data and control your world. W.W. Norton & Company.

Shillair, R. (2020). *Protection motivation theory. In The international encyclopedia of media psychology* (pp. 1 3). Wiley.

Stoycheff, E. (2016). Under surveillance: Examining Facebook's spiral of silence effects in the wake of NSA internet monitoring. *Journal of Mass Communication and Society,* 19(2), 202–219. https://doi.org/10.1080/15205436.2015.1100832

Tajfel, H., & Turner, J. C. (1979). An integrative theory of intergroup conflict. In W. G. Austin & S. Worchel (Eds.), *The social psychology of intergroup relations* (pp. 33–47). Brooks/Cole.

Toprak, A., Yıldırım, A., Aygül, E., Binark, M., Börekçi, S., & Çomu, T. (2014). *Toplumsal paylaşım ağı: Facebook, görülüyorum öyleyse varım*. Kalkedon Yayınları.

Trottier, D. (2017). *Social media as surveillance: Rethinking visibility in a converging world*. Routledge.

Tsai, J., Egelman, S., Cranor, L., & Acquisti, A. (2011). The effect of online privacy information on purchasing behavior: An experimental study. *Information Systems Research,* 22(2), 254–268. https://doi.org/10.1287/isre.1090.0260

Yıldız, A., Kaya, S., Altunkaynak, B., & Güngörer, B. (2022). Covid-19'dan korunma davranışlarını etkileyen faktörleri değerlendirme ölçeği: Türkçeye uyarlama çalışması. *Hacettepe Sağlık İdaresi Dergisi,* 25(4), 861–882.

Zhang, Z., & Zhang, X. (2024). Why not use facial recognition payment? From the perspective of the extended protection motivation theory. *Journal of Retailing and Consumer Services,* 81, 1–9.

Zhang, Y. J., Chen, J. Q., & Wen, K.-W. (2002). Characteristics of internet users and their privacy concerns: A comparative study between China and the United States. *Journal of Internet Commerce,* 1(2), 1–16.

Weimann, G. (2014). *New terrorism and new media*. Wilson Center. https://www.wilsoncenter.org/publication/new-terrorism-and-new-media