

SOSYAL MEDYADAKİ GÖRSEL VERİLERİN GDPR VE KVKK KAPSAMINDA ANALİZİ

ANALYSIS OF VISUAL DATA ON SOCIAL MEDIA WITHIN THE SCOPE OF GDPR AND KVKK

Utku AYDIN

Gazi Üniversitesi, Bilişim Enstitüsü, Adli Bilişim Ana Bilim Dalı,
uutkuaydin123@gmail.com

Ankara / Türkiye

ORCID: 0009-0007-6808-2478

Prof. Dr. Hasan Hüseyin SAYAN

Gazi Üniversitesi, Teknoloji Fakültesi, Elektrik - Elektronik Mühendisliği Bölümü,
hsayan@gazi.edu.tr

Ankara / Türkiye

ORCID: 0000-0002-0692-172X

ÖZET

Bu çalışma, sosyal medya platformlarında görsel kişisel verilerin işlenmesi süreçlerine ilişkin kullanıcı farkındalığını, hukuki bilgi düzeylerini ve koruyucu davranış eğilimlerini nicel bir yaklaşımla analiz etmeyi amaçlamaktadır. Dijitalleşme süreçlerinin ivme kazanmasıyla birlikte, bireylerin paylaştığı görsel veri hacmindeki artış, kişisel verilerin korunmasını kritik bir veri güvenliği ve hak meselesi haline getirmiştir. Araştırmada veri toplama aracı olarak 24 maddelik Likert tipi bir ölçek kullanılmış ve 240 katılımcıdan elde edilen veriler üzerinde Açıklayıcı Faktör Analizi (AFA) gerçekleştirilmiştir. Analiz sonuçları, ölçeğin üç boyutlu bir yapı sergilediğini doğrulamıştır. Araştırma bulguları; katılımcıların görsel kişisel verilerin korunmasına yönelik farkındalık düzeylerinin yüksek olduğunu, ancak 6698 sayılı KVKK kapsamındaki hukuki düzenlemelere ve sosyal medya platformlarının veri politikalarına duyulan güvenin görece düşük seyrettiğini ortaya koymaktadır. Sonuç olarak, veri koruma ekosisteminde yalnızca bireysel farkındalığın artırılmasının yeterli olmadığı; KVKK mevzuatının uygulama etkinliğinin güçlendirilmesi ve platformların daha şeffaf politikalar geliştirmesi gerektiği değerlendirilmektedir.

Anahtar kelimeler: Görsel Kişisel Veriler, Veri Koruma Farkındalığı, Sosyal Medya Gizliliği, KVKK (Kişisel Verilerin Korunması Kanunu), Koruyucu Davranışlar, Veri Güvenliği

ABSTRACT

This study aims to analyze user awareness, legal knowledge levels, and protective behavior tendencies regarding the processing of visual personal data on social media platforms using a quantitative approach.

With the acceleration of digitalization processes, the surge in the volume of visual data shared by individuals has transformed the protection of personal data into a critical issue of data security and rights. A 24-item Likert-type scale was utilized as the data collection instrument, and Exploratory Factor Analysis (EFA) was performed on the data obtained from 240 participants. The analysis results confirmed that the scale exhibits a three-dimensional structure. Research findings indicate that while participants' awareness levels regarding the protection of visual personal data are high, trust in legal regulations under the Law No. 6698 on the Protection of Personal Data (KVKK) and the data policies of social media platforms remains relatively low. Consequently, it is evaluated that enhancing individual awareness alone is insufficient within the data protection ecosystem; the enforcement effectiveness of KVKK legislation must be strengthened, and platforms should develop more transparent policies.

Keywords: Visual Personal Data, Data Protection Awareness, Social Media Privacy, KVKK (Personal Data Protection Law), Protective Behaviors, Data Security

1.GİRİŞ

Günümüzde teknolojinin hızlı gelişimi ve dijitalleşme süreci, iletişim teknolojilerinde önemli dönüşümlere yol açmış; bireylerin bilgiye erişim, iletişim kurma ve içerik üretme biçimlerini köklü şekilde değiştirmiştir. İnternet tabanlı uygulamaların yaygınlaşmasıyla birlikte geleneksel iletişim modelleri yerini, kullanıcıların aktif katılımına dayanan ve etkileşim imkânı sunan sosyal medya platformlarına bırakmıştır. Bu bağlamda sosyal medya, bireylerin yalnızca içerik tüketicisi değil aynı zamanda içerik üreticisi hâline geldiği çok yönlü bir iletişim ortamı olarak öne çıkmaktadır (Kaplan & Haenlein, 2010; Fuchs, 2017).

Sosyal medya platformlarının yaygınlaşması, bireylerin günlük yaşamlarının önemli bir bölümünü dijital ortamlarda sürdürmesine neden olmuş ve bu durum kişisel veri üretimini önemli ölçüde artırmıştır. Özellikle fotoğraf, video ve canlı yayın gibi görsel içeriklerin yoğun biçimde paylaşılması, görsel kişisel verilerin daha merkezi bir konuma gelmesine yol açmıştır. Görsel kişisel veriler, bireyin kimliğini doğrudan veya dolaylı olarak belirlenebilir kılabilmesi nedeniyle hassas veri niteliği taşıyabilmektedir (Gündüz & Das, 2022).

Kişisel verilerin korunması, bireyin temel hak ve özgürlüklerinin dijital ortamda güvence altına alınmasını ifade etmektedir. Bu kapsamda kişisel veri kavramı, yalnızca kimliği açıkça belirleyen bilgilerle sınırlı olmayıp, bireyi belirlenebilir kılan tüm veri türlerini kapsamaktadır (Yüksek, 2023). Türkiye’de bu alanı düzenleyen 6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK), kişisel veriyi “kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi” olarak tanımlamakta ve veri işleme faaliyetlerini belirli kurallara bağlamaktadır.

Bununla birlikte sosyal medya platformlarının veri işleme yapıları, algoritmik sistemler ve üçüncü taraf uygulamalar aracılığıyla giderek daha karmaşık bir hâl almakta; bu durum bireylerin verileri üzerindeki kontrolünü zorlaştırarak gizlilik ve güvenlik risklerini artırmaktadır (Marwick & Boyd, 2014). Özellikle görsel içeriklerin hızlı yayılması ve kalıcılığı, mahremiyet ihlallerinin etkisini artırmakta ve bu ihlallerin giderilmesini güçleştirmektedir. Ayrıca literatürde kullanıcıların veri gizliliğine önem verdiklerini ifade etmelerine rağmen çeşitli faydalar karşılığında kişisel verilerini paylaşmaya devam ettiklerini ortaya koyan “mahremiyet paradoksu” kavramı dikkat çekmektedir (Wu vd., 2019). Bu durum, farkındalık ile davranışlar arasında bir uyumsuzluk olabileceğine işaret etmektedir.

Bu çalışma, sosyal medya ortamlarında görsel kişisel verilerin işlenmesine ilişkin kullanıcı farkındalığını, hukuki bilgi düzeyini, koruyucu davranış eğilimlerini ve mevzuat ile platformlara yönelik güven algısını incelemeyi amaçlamaktadır. Literatürde bu konuya ilişkin çalışmaların sınırlı olması nedeniyle araştırmanın, görsel kişisel verilerin korunmasına yönelik farkındalığın çok boyutlu yapısını ortaya koyarak literatüre katkı sunması beklenmektedir.

Bu doğrultuda çalışma, kullanıcıların farkındalık düzeyleri ile mevcut hukuki düzenlemelere ve platformlara duydukları güven arasındaki ilişkiyi analiz etmeyi ve elde edilen bulgular çerçevesinde veri koruma mevzuatının geliştirilmesine yönelik değerlendirmeler sunmayı hedeflemektedir.

2. LİTERATÜR

2.1. Sosyal Medya Kavramı

İnsanlık tarihi boyunca iletişim biçimleri, teknolojik gelişmelere paralel olarak sürekli değişim göstermiştir. Yüz yüze iletişimden yazılı kültüre, oradan kitle iletişim araçlarına uzanan bu süreç, dijital teknolojilerin gelişmesiyle birlikte yeni bir boyut kazanmıştır. Özellikle internetin yaygınlaşması, iletişimi zaman ve mekân sınırlarından büyük ölçüde bağımsız hâle getirmiş ve çok yönlü bir yapıya dönüştürmüştür. Bu bağlamda iletişim süreçlerinin toplumsal yapıyı şekillendiren önemli unsurlar arasında yer aldığı ifade edilmektedir (Castells, 2010).

Sanayileşme süreciyle birlikte ortaya çıkan geleneksel medya araçları (radyo, televizyon ve basılı medya), merkezi yapılar aracılığıyla geniş kitlelere tek yönlü iletişim sağlamıştır (Kara, 2013). Ancak dijitalleşmeyle birlikte bu yapı dönüşmüş; sosyal medya, kullanıcıların hem içerik üreticisi hem de tüketicisi olduğu etkileşimli bir iletişim ortamı sunmuştur (Fuchs, 2017). Bu dönüşüm, iletişimi tek yönlü bir yapıdan çıkararak çok yönlü ve katılımcı bir hâle getirmiştir (Ceylan, 2020).

Sosyal medya, literatürde kullanıcı merkezli bir iletişim ortamı olarak tanımlanmakta; bireylerin zaman ve mekân sınırlaması olmaksızın içerik üretmesine, paylaşmasına ve etkileşim kurmasına olanak sağlamaktadır (Kaplan & Haenlein, 2010). Bu platformların erişilebilirliği, sosyal medyanın küresel ölçekte yaygınlaşmasına katkı sağlamış; kullanıcıların farklı coğrafyalarda iletişim kurabilmesini mümkün kılmıştır (Bayer & Özek, 2021). Bununla birlikte sosyal medya kullanımının artması, bireylerin sosyal ilişkilerini ve iletişim biçimlerini dönüştürmüş; sosyal ağların genişlemesine ve etkileşim dinamiklerinin değişmesine neden olmuştur (Hall & Liu, 2022). Ancak sosyal medyanın yaygınlaşması, bilgi kirliliği, mahremiyet ihlalleri ve bilişim suçları gibi çeşitli riskleri de beraberinde getirmektedir (Bahar, 2018). Özellikle dijital ortamlarda paylaşılan verilerin kalıcılığı, kişisel verilerin korunması açısından önemli sorun alanları oluşturmaktadır (Korkmaz, 2021). Bu nedenle sosyal medya, yalnızca bir iletişim aracı değil, aynı zamanda kişisel verilerin korunması bağlamında da değerlendirilmesi gereken önemli bir çalışma alanı olarak öne çıkmaktadır.

2.2. Sosyal Ağlar ve Diğer Sosyal Medya Türleri

İnsan, doğası gereği sosyal bir varlık olup iletişim ihtiyacını farklı yapılar aracılığıyla karşılamaktadır. Bu bağlamda sosyal ağlar, başlangıçta yüz yüze ilişkiler temelinde şekillenmiş; internet ve dijital teknolojilerin gelişmesiyle birlikte çevrim içi ortamlara taşınmıştır. Sosyal ağlar, bireylerin dijital ortamlar üzerinden bağlantı kurabildiği, etkileşimde bulunabildiği ve içerik paylaşabildiği yapılar olarak tanımlanmaktadır. Özellikle Web 2.0 teknolojilerinin gelişmesiyle birlikte kullanıcıların içerik üreticisi hâline gelmesi, sosyal ağların temel özelliklerinden biri olmuştur (Boyd & Ellison, 2007).

Sosyal ağlar, farklı sosyo-demografik gruplardan geniş bir kullanıcı kitlesine sahiptir. Bu nedenle kullanıcılar, ilgi, bilgi paylaşımı ve etkileşim biçimlerine göre çeşitli kategoriler altında incelenmektedir (Hagel, 1997; Akkurt, 2019). Platformlar içerik türlerine göre de farklılaşmakta; bazıları sosyal ilişkileri ön plana çıkarırken, bazıları görsel ve işitsel içerik paylaşımına odaklanmaktadır (Topbaş & Gazi, 2016).

Sosyal ağlar günümüzde küresel ölçekte milyarlarca kullanıcıya ulaşmış ve dijital iletişimin merkezinde yer almıştır. Mobil cihazların yaygınlaşmasıyla birlikte kullanım oranları artmış; bireylerin dijital ortamlarda geçirdiği süre ve ürettikleri veri miktarı önemli ölçüde yükselmiştir (Kemp, 2018; Kemp, 2021; Çömlekçi & Başol, 2019; DataReportal, 2022). Bu durum, kişisel verilerin korunmasına yönelik hukuki düzenlemelerin önemini artırmaktadır.

Sosyal ağların yaygın kullanımı, veri güvenliği ve mahremiyet açısından çeşitli riskler doğurmaktadır. Paylaşılan içeriklerin geniş kitlelere ulaşabilmesi ve kalıcı olması, gizlilik ihlallerini artırmaktadır (Choi & Choi, 2007). Web 2.0 ile birlikte kullanıcıların aktif içerik üreticisi hâline gelmesi, veri üretimini hızlandırmış ve kontrolü zorlaştırmıştır (O'Reilly, 2005). Ayrıca mobil uygulamalar aracılığıyla konum, iletişim ve kişi listesi gibi verilerin toplanması ve üçüncü taraflarla paylaşılması, veri güvenliği risklerini daha da artırmaktadır (Kim, Oh & Kim, 2015; Zhu vd., 2014). Bu nedenle sosyal ağlar, teknik, hukuki ve etik boyutlarıyla birlikte değerlendirilmelidir (Bozdağ Tulum & Kaya, 2023).

2.2.1. Wikiler ve Bloglar

Bloglar, başlangıçta bireylerin kişisel deneyimlerini paylaştığı dijital günlükler olarak ortaya çıkmış, zamanla bilgi paylaşımı ve etkileşim aracı hâline gelmiştir (Paličko, 2023). Wiki sistemleri ise kullanıcıların ortaklaşa içerik üretmesine ve mevcut içerikleri düzenlemesine imkân tanıyan iş birliğine dayalı platformlardır (Savran Çelik & Aydın, 2021).

2.2.2. Sanal Gerçeklik Platformları

Sanal gerçeklik (VR), artırılmış gerçeklik (AR) ve karma gerçeklik (MR) teknolojileri, kullanıcıya etkileşimli dijital deneyimler sunmaktadır (Steuer, 1992; Arıkan, 2023). Bu teknolojiler eğitim, sağlık ve eğlence gibi birçok alanda kullanılmakta; ancak kullanıcıların davranışsal ve biyometrik verilerini toplaması nedeniyle yeni veri güvenliği risklerini de beraberinde getirmektedir (Mantelero, 2016; Giaretta, 2024).

2.2.3. Elektronik Posta Grupları ve Forumlar

Elektronik posta grupları ve forumlar, kullanıcıların bilgi paylaşımı ve iletişim kurmasını sağlayan dijital platformlardır. Bu sistemler aracılığıyla metin, belge ve görsel içerik paylaşılabilir; ancak kişisel veri güvenliği açısından çeşitli riskler de ortaya çıkmaktadır (Akkaya, 2020; Kocabay, 2007).

2.3. Kişisel Veri Kavramı

2.3.1. Kişisel Veri Tanımı ve Kapsamı

Kişisel veri, belirli veya belirlenebilir bir gerçek kişiye ilişkin, o kişiyi doğrudan ya da dolaylı olarak tanımlamaya elverişli her türlü bilgi olarak tanımlanmaktadır (Yüksek, 2023). Bu tanım, yalnızca kimliği açıkça belirleyen verilerle sınırlı olmayıp, diğer verilerle birlikte kullanıldığında kişiyi belirlenebilir hâle getiren tüm unsurları kapsamaktadır. Hukuki düzenlemelerde kişisel verilerin kapsamı sınırlı bir liste ile belirlenmemiş, teknolojik gelişmelere uyum sağlayabilecek şekilde geniş ve esnek tutulmuştur. Nitekim günümüzde giyilebilir sağlık cihazları aracılığıyla toplanan kalp atış hızı, kan basıncı ve uyku düzeni gibi hassas sağlık verileri, kişisel veri tanımının kapsamını genişleten ve korunması gereken kritik unsurlar haline gelmiştir (Özçağdavul, 2024). Bu yaklaşım, yeni veri türlerinin de koruma kapsamına alınmasını amaçlamaktadır. Nitekim 6698 sayılı KVKK'nın 3. maddesinde yer alan "her türlü bilgi" ifadesi, bu geniş yaklaşımı açıkça ortaya koymaktadır. Bu tür kapsayıcı düzenlemeler, kişilik haklarının etkin korunması açısından önem taşımaktadır (Henkoğlu, 2018).

2.3.2. Kişisel Veri ve Kişilik Hakkı İlişkisi

Kişisel veri kavramı, kişilik hakkının dijital ortamlara yansıyan bir boyutu olarak değerlendirilmektedir. Kişilik hakkı, bireyin varlığıyla birlikte doğan ve hukuk düzeni tarafından korunan temel haklardan biridir (Gözler, 2002). Dijitalleşmeyle birlikte bu hak, çevrim içi ortamlarda da korunması gereken bir nitelik kazanmıştır. Sosyal medya ve dijital platformlarda bırakılan veriler, kişilik hakkının dijital uzantısını oluşturmakta ve bireyin mahremiyetiyle doğrudan bağlantılı hâle gelmektedir (Güngör, 2019).

Hukuken kiři kavramı gerek ve tuzel kiřiler olarak ayrılmakla birlikte, kiřisel veri kavramı yalnızca gerek kiřilere iliřkin verileri kapsamaktadır (Gozler, 2002; Rado, 2016). KVKK'da da benimsenen bu yaklařım dođrultusunda, veri sahiplerine tanınan haklar yalnızca gerek kiřiler için geerlidir. Ozellikle sosyal medya platformlarında paylařılan gořsel ierikler, kiřilik hakkının dijital ortamda gořunur hale gelmesine neden olurken, aynı zamanda verilerin kontrolsuz yayılması riskini de artırmaktadır.

2.3.3. Kiřisel Verilerin Turleri ve Hassas Veri Kavramı

Kiřisel veriler, hassas (ozel nitelikli) ve hassas olmayan veriler olarak sınıflandırılmaktadır. Hassas veriler, bireyin mahremiyetine daha fazla mudahale potansiyeli tařıyan ve bu nedenle daha sıkı koruma gerektiren veri turleridir. KVKK'nın 6. maddesine goře; ırk, etnik kořen, siyasi gořuř, dini inan, sađlık bilgileri, cinsel hayat, biyometrik ve genetik veriler ozel nitelikli kiřisel veriler arasında yer almakta ve bu verilerin iřlenmesi daha sıkı Őartlara bađlanmaktadır (Arınmiř Uzun, 2020, s. 210).

2.3.4. Veri Gizliliđi ve Sosyal Ađlar

Veri gizliliđi, bireylerin kiřisel verileri uzerinde kontrol sahibi olmasını ifade etmektedir. Ancak sosyal medya platformlarında veri akıřının karmařık yapısı, bu kontrolun sađlanmasını guleřtirmektedir (Metheney, 2017; Marwick & Boyd, 2014). Paylařılan ieriklerin farklı ortamlara aktarılması, gizlilik ihlali riskini artırmaktadır. Bu bađlamda "mahremiyet paradoksu" kavramı, bireylerin gizliliđe önem vermelerine rađmen eřitli faydalar karřılıđında verilerini paylařmaya devam ettiklerini ortaya koymaktadır (Wu vd., 2019).

2.3.5. Bilgi Guvenliđi, Riskler ve Farkındalık

Kiřisel verilerin korunmasında önemli sorunlardan biri, kullanıcıların bilgi guvenliđi farkındalıđının yetersiz olmasıdır. Bireyler ođu zaman kullandıkları sistemlerin guvenliđini deđerlendirememekte ve bu durum veri guvenliđi risklerini artırmaktadır. Ayrıca bilgi guvenliđi risklerinin olulmesindeki zorluk, bu risklerin etkin Őekilde yonetilmesini engellemektedir (Anderson & Moore, 2006). Bireysel duzeyde alınan guvensiz kararlar, yalnızca bireyi deđil daha geniř kullanıcı kitlelerini de etkileyebileceđinden, bilgi guvenliđi aynı zamanda toplumsal bir sorun olarak deđerlendirilmektedir.

Kiřisel verilerin kontrolsuz biimde yayılması, bireyleri hem istenmeyen pazarlama faaliyetlerine maruz bırakmakta hem de dolandırıcılık riskini artırmaktadır. Kotu niyetli kiřiler, elde ettikleri veriler sayesinde kendilerini resmi kurum temsilcisi gibi tanıtarak hatta buna bile gerek duymadan herhangi bir Őekilde kullanıcılarda guven sađlayabilmekte ve mađduriyetlere yol aabilmektedir. Bu olguya rađmen bireylerin ođu, uzun ve karmařık aydınlatma metinlerini incelemeyen verilerini paylařmaya devam etmektedir. Bu hususta kiřilerin bireysel farkındalıđını arttırması onlemler için önemli bir katkıda bulunsa da Kiřisel Verileri Koruma Kurulu tarafından yurutulen bilgilendirme faaliyetleri önemli bir noktada durmaktadır. Bunlara ek olarak toplumsal farkındalıđın artırılması için bu alıřmaların daha geniř kitlelere ulařacak Őekilde geliřtirilmesi gerekmektedir (Ozađdavul & Sayan, 2023).

2.3.6. Hukuki Duzenlemeler ve KVKK'nın Onemi

evrimii sosyal ađların yaygınlařmasıyla birlikte veri gizliliđi, giderek daha önemli bir hukuki sorun hiline gelmiřtir. Bu alanda yapılan alıřmalar, sosyal medya platformlarının eřitli turlerde kiřisel verilerin sızmasına neden olabildiđini ve kullanıcıların gizlilik ayarlarını etkin Őekilde yonetmekte zorlandıđını ortaya koymaktadır (Liu vd., 2011).

Turkiye'de kiřisel verilerin korunmasına yonelik en temel duzenleme olan 6698 sayılı KVKK'nın yururluđe girmesiyle birlikte, kiřisel veriler yasal guvence altına alınmiřtir. Kanun, veri sorumlularına eřitli yuكلuьluьkler getirirken, veri sahiplerine de belirli haklar tanımiřtir.

Kişisel verilerin korunmasına ilişkin düzenlemeler yalnızca ulusal düzeyde değil, uluslararası alanda da gelişim göstermiştir. OECD'nin 1980 tarihli rehber ilkeleri, Avrupa Konseyi'nin 108 No'lu Sözleşmesi ve Avrupa Birliği'nin veri koruma düzenlemeleri bu alandaki temel metinler arasında yer almaktadır.

GDPR, yalnızca Avrupa Birliği sınırları içerisinde geçerli olan bir mevzuat olmaktan çıkarak küresel ölçekte etki doğuran bir yönetmelik hâline gelmiştir. Nitekim AB üyesi ülke vatandaşlarına hizmet sunan, ancak merkezleri Birlik dışında bulunan ve AB menşei olmayan şirketler dahi GDPR kapsamına girebilmektedir. Bu sebeple, Avrupa Birliği ile ticari veya hizmet ilişkisi bulunan birlik dışı şirketler de veri işleme faaliyetlerini GDPR hükümlerine uygun şekilde yürütmeye çalışmaktadır. Aksi hâlde, söz konusu şirketler Birlik içerisindeki faaliyetlerinin engellenmesi gibi ağır yaptırımlarla karşı karşıya kalabilmektedir. (Voigt & Von dem Bussche, 2017)

Bu bağlamda KVKK, Türkiye'de veri koruma alanında önemli bir hukuki altyapı oluşturmuş ve bireylerin temel haklarının korunmasına katkı sağlamıştır. Ancak KVKK – GDPR karşılaştırması yapacak olursak Türkiye'nin KVKK'yı daha etkin biçimde uygulayabilmesi için GDPR kapsamında geliştirilen kavram ve ilkelerin detaylı biçimde analiz edilmesi gerekmektedir. Özellikle hesap verebilirlik ilkesinin veri koruma uygulamalarının temel unsurlarından biri olarak ele alınması ve bu ilkenin Türk veri koruma sistemine entegre edilmesi önem taşımaktadır. Nitekim yapılan araştırmalar, kullanıcıların kişisel bilgileri üzerinde kontrol sahibi olmaları durumunda uygulamalara güvenme ve bu uygulamalarla etkileşime geçme olasılıklarının daha yüksek olduğunu göstermektedir (Özçağdavul & Sayan, 2025). Bu yaklaşım, hem hukuki belirsizliklerin giderilmesine katkı sağlayacak hem de paydaşlar arasında güvenin tesis edilmesine yardımcı olacaktır (Geden & Bensghir, 2019).

2.3.7. Görsel Kişisel Veriler

Kişisel veri kavramı kapsamında, bireyin kimliğini doğrudan veya dolaylı olarak belirlenebilir kılan tüm bilgiler yer almaktadır. Bu bağlamda görsel içerikler de kişisel veri niteliği taşımaktadır.

Görsel kişisel veriler; bireylerin fotoğrafları, videoları, canlı yayın kayıtları ve benzeri içerikleri kapsamaktadır. Bu veriler, bireyin fiziksel özellikleri, bulunduğu ortam ve sosyal ilişkileri hakkında önemli çıkarımlar yapılmasına imkân tanımaktadır. Bu nedenle görsel veriler, bireyin kimliğinin belirlenmesinde güçlü araçlar olarak değerlendirilmektedir.

Özellikle sosyal medya platformlarında paylaşılan görsellerin kontrolsüz şekilde yayılabilmesi, ciddi mahremiyet ihlallerine yol açabilmektedir. Görsel içeriklerin hızlı yayılımı ve geri döndürülmesinin zor olması, bu veri türünü daha hassas hâle getirmektedir (Gündüz & Das, 2022).

Ayrıca görsel verilerin biyometrik veri olarak kullanılabilmesi, bu verilerin korunmasını daha kritik bir konu hâline getirmektedir. Yüz tanıma teknolojileri gibi gelişmeler, görsel verilerin kimlik doğrulama aracı olarak kullanılmasına olanak tanımaktadır. Bu durum, veri güvenliği risklerini artırmaktadır (European Data Protection Board, 2019).

Sonuç olarak görsel kişisel veriler, dijitalleşmenin etkisiyle birlikte kişisel veri kategorileri içerisinde daha merkezi ve hassas bir konuma ulaşmıştır. Bu nedenle bu verilerin korunmasına yönelik hukuki ve teknik önlemlerin geliştirilmesi büyük önem taşımaktadır.

3. METODOLOJİ

3.1. Ölçme Aracı ve Geçerlik Süreci

Bu çalışmada, sosyal medyada görsel kişisel verilerin işlenmesine ilişkin kullanıcı farkındalığı ve tutumlarını incelemek amacıyla nicel araştırma yöntemi benimsenmiştir. Veri toplama aracı olarak, literatürden yararlanılarak oluşturulan 25 maddelik Likert tipi yapılandırılmış anket kullanılmıştır.

Ölçeğin yapısal geçerliğini test etmek amacıyla açımlayıcı faktör analizi uygulanmıştır. KMO değerinin 0.82 bulunması ve Bartlett testinin anlamlı çıkması, veri setinin analize uygun olduğunu göstermiştir. Yapılan analiz sonucunda üç faktörlü bir yapı elde edilmiştir. Düşük yük değerine sahip bir madde (S2) çıkarılarak analiz 24 madde üzerinden tamamlanmıştır.

Elde edilen faktörler; Görsel Veri Farkındalığı ve Koruma Yönelimi ,Mevzuat ve Platform Güvenilirliği Algısı , Hukuki Bilgi ve Bireysel Farkındalık , Cronbach Alpha değerleri 0.73–0.83 aralığında bulunmuş ve ölçeğin güvenilir olduğu değerlendirilmiştir.

3.2. Evren ve Örneklem

Araştırmanın evrenini Türkiye’de sosyal medya kullanan bireyler oluşturmaktadır. Örneklem, kolayda örnekleme yöntemiyle seçilen 240 katılımcıdan oluşmaktadır. Katılımcıların önemli bir kısmının hukuk alanına yakın meslek gruplarından olması, veri koruma farkındalığının değerlendirilmesine katkı sağlamakla birlikte, bulguların genellenmesinde dikkatli olunmasını gerektirmektedir.

3.3. Veri Toplama Süreci

Veriler Google Forms aracılığıyla çevrim içi ortamda toplanmıştır. Katılım gönüllülük esasına dayalı olup, veriler anonim olarak elde edilmiştir. Katılımcılara araştırmanın amacı hakkında bilgilendirme yapılmış ve açık rıza alınmıştır.

3.4. Veri Analizi

Veriler öncelikle betimleyici istatistikler (ortalama, standart sapma) ile analiz edilmiştir. Ardından açımlayıcı faktör analizi uygulanmış ve faktör yapısı belirlenmiştir. Son aşamada faktör puanları oluşturularak boyutlar arası ilişkiler incelenmiştir.

3.5. Etik İlkeler

Araştırma, bilimsel etik kurallara ve veri koruma ilkelerine uygun şekilde yürütülmüştür. Katılımcılardan kimlik bilgisi alınmamış, veriler yalnızca akademik amaçlarla kullanılmıştır.

4. BULGULAR VE YORUM

4.1. Bulgular

Elde edilen bulgular, katılımcıların görsel kişisel verilerin korunmasına ilişkin yüksek düzeyde farkındalığa sahip olduğunu göstermektedir. Özellikle veri paylaşımının riskli olduğu ve kullanıcıların daha dikkatli olması gerektiği yönündeki ifadeler yüksek katılım sağlanmıştır.

Buna karşılık, sosyal medya platformlarının veri politikalarına ve mevcut hukuki düzenlemelerin yeterliliğine yönelik güven düzeyinin daha düşük olduğu görülmektedir.

Faktör analizi sonucunda elde edilen üç boyut incelendiğinde; Farkındalık düzeyi yüksek, Hukuki bilgi orta düzeyde, Sistem ve mevzuata güven düşük bulunmuştur.

Ayrıca farkındalık ile bireysel bilinç arasında pozitif ilişki tespit edilirken, bu durumun kurumsal güven ile aynı yönde gelişmediği görülmüştür.

4.2. Tartışma ve Sonuç

Bulgular, kullanıcıların veri koruma konusunda bilinçli olmasına rağmen mevcut sistemlere sınırlı düzeyde güvendiğini göstermektedir. Bu durum, veri koruma alanında yalnızca farkındalık değil, aynı zamanda şeffaflık ve uygulama etkinliğinin de önemli olduğunu düşündürmektedir.

Elde edilen çok boyutlu yapı, kullanıcı algısının tek yönlü olmadığını ve bireysel farkındalık ile kurumsal güvenin ayrı değerlendirilmesi gerektiğini ortaya koymaktadır.

Çalışma, kullanıcıların görsel kişisel verilerin korunmasına yönelik yüksek farkındalık taşıdığını ancak mevcut mevzuat ve platform uygulamalarını yeterli görmediğini göstermektedir.

Bu doğrultuda, veri koruma alanında; mevzuatın güçlendirilmesi, uygulama mekanizmalarının geliştirilmesi, kullanıcı dostu ve şeffaf politikaların oluşturulması gerektiği değerlendirilmektedir. Gelecek çalışmalar için farklı örneklem gruplarıyla karşılaştırmalı analizlerin yapılması önerilebilir.

KAYNAKLAR

- Akkaya, A. (2020). Elektronik posta gruplarında veri güvenliği. *Bilişim Hukuku Dergisi*, 5(2), 45–62.
- Akkurt, M. (2019). Sosyal ağ kullanıcılarının davranışsal analizi. *İletişim Çalışmaları Dergisi*, 7(1), 88–102.
- Anderson, R., & Moore, T. (2006). The economics of information security. *Science*, 314(5799), 610–613.
- Arıkan, R. (2023). Artırılmış ve sanal gerçeklik teknolojilerinin gelişimi. *Dijital Teknolojiler Dergisi*, 4(1), 55–70.
- Arınmış Uzun, S. (2020). Kişisel verilerin korunması hukuku. Seçkin Yayıncılık.
- Bahar, E. (2018). Sosyal medyada bilgi kirliliği ve güvenlik sorunları. *Yeni Medya Araştırmaları*, 3(2), 33–48.
- Bayer, J., & Özek, H. (2021). Digital communication and global interaction. *Journal of Media Studies*, 9(4), 122–138.
- Boyd, D. M., & Ellison, N. B. (2007). Social network sites: Definition, history, and scholarship. *Journal of Computer-Mediated Communication*, 13(1), 210–230.
- Bozdağ Tulum, E., & Kaya, A. (2023). Sosyal ağlarda veri güvenliği. Beta Yayınları.
- Castells, M. (2010). *The rise of the network society*. Wiley-Blackwell.
- Ceylan, S. (2020). Sosyal medya ve iletişim dönüşümü. *İletişim Kuram ve Araştırma Dergisi*, 51, 75–90.
- Chatterjee, S., & Kar, A. K. (2018). Smart city data protection and integration model. *Government Information Quarterly*, 35(4), 577–586.
- Choi, J. H., & Choi, J. H. (2007). User privacy in online environments. *Information Systems Journal*, 17(2), 123–145.
- Çömlekçi, M. F., & Başol, O. (2019). Türkiye’de sosyal medya kullanımı. *Akdeniz İletişim Dergisi*, 31, 124–139.
- DataReportal. (2022). *Digital 2022: Turkey*. <https://datareportal.com>
- Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, 13(3), 319–340.
- European Data Protection Board. (2019). *Guidelines on facial recognition*.
- Fuchs, C. (2017). *Social media: A critical introduction* (2nd ed.). Sage.
- Geden, G., & Bensghir, T. K. (2019). Personal data protection in smart cities: Comparative analysis of GDPR and Turkish law. *Journal of Urban Technology*, 26(3), 203–226.
- Giaretta, E. (2024). Data protection in virtual environments. *Technology Law Review*, 15(2), 201–220.
- Gözler, K. (2002). *Hukuka giriş*. Ekin Yayınları.
- Gündüz, M., & Das, R. (2022). Visual privacy risks in social media. *Cybersecurity Journal*, 8(3), 67–81.
- Güngör, M. (2019). Dijital çağda kişilik hakları. On İki Levha Yayıncılık.
- Hagel, J. (1997). *Net gain: Expanding markets through virtual communities*. Harvard Business School Press.
- Hall, J. A., & Liu, D. (2022). Social media use and social relationships. *Computers in Human Behavior*, 130, 107–115.
- Henkoğlu, T. (2018). Kişisel verilerin korunması ve hukuki boyutu. Yetkin Yayınları.
- Kaplan, A. M., & Haenlein, M. (2010). Users of the world, unite! The challenges and opportunities of social media. *Business Horizons*, 53(1), 59–68.
- Kara, T. (2013). Kitle iletişim araçlarının gelişimi. Beta Yayınları.
- Kemp, S. (2018). *Digital 2018 global overview report*.
- Kemp, S. (2021). *Digital 2021 global overview report*.

- Kim, J., Oh, J., & Kim, S. (2015). Mobile data privacy issues. *Information Systems Review*, 17(4), 45–60.
- Kocabay, Ş. (2007). İnternet forumları ve kullanıcı davranışları. *Yeni Medya Çalışmaları*, 2(1), 44–58.
- Korkmaz, A. (2021). Dijital ortamda veri güvenliği. Nobel Yayınları.
- Liu, Y., et al. (2011). Privacy leakage in social networks. *IEEE Security & Privacy*, 9(3), 20–27.
- Mantelero, A. (2016). Personal data in VR environments. *Computer Law & Security Review*, 32(3), 399–410.
- Marwick, A. E., & Boyd, D. (2014). Networked privacy: How teenagers negotiate context in social media. *New Media & Society*, 16(7), 1051–1067.
- Metheney, C. (2017). *Federal cloud computing*. Syngress.
- O'Reilly, T. (2005). *What is Web 2.0?*
- Özçağdavul, M. (2024). General Data Protection Regulation compliance and privacy protection in wearable health devices: Challenges and solutions. *Artuklu Health*, 10, 29–37. <https://doi.org/10.58252/artukluhealth.1566573>
- Özçağdavul, M., & Sayan, H. H. (2023). Akıllı şehirler ve Kişisel Verileri Koruma Kanunu uyumu. *TYB Akademi*, 37, 86–100.
- Özçağdavul, M., & Sayan, H. H. (2025). Developing a new technology acceptance model for smart city applications in compliance with GDPR. *Intelligent Buildings International*, 1–11.
- Paličko, D. (2023). Blogging culture and development. *Media Studies Review*, 11(2), 55–70.
- Rado, T. (2016). Tüzel kişilik kavramı. Yetkin Yayınları.
- Savran Çelik, S., & Aydın, B. (2021). Wiki sistemleri ve işleyişi. *Bilişim Teknolojileri Dergisi*, 14(2), 90–105.
- Steuer, J. (1992). Defining virtual reality. *Journal of Communication*, 42(4), 73–93.
- Topbaş, H., & Gazi, M. (2016). Sosyal medya türleri. *İletişim Araştırmaları*, 14(1), 25–40.
- Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology. *MIS Quarterly*, 27(3), 425–478.
- Voigt, P., & Von dem Bussche, A. (2017). *The EU GDPR: A practical guide*. Springer.
- Wu, Y., Zhang, C., & Liu, H. (2019). The privacy paradox in social media: A systematic review. *IEEE Access*, 7, 180837–180850. <https://doi.org/10.1109/ACCESS.2019.2959037>
- Yüksek, S. (2023). *Kişisel verilerin korunması hukuku*. Seçkin Yayıncılık.
- Zhu, H., et al. (2014). Privacy risks in mobile applications. *IEEE Transactions on Mobile Computing*, 13(6), 1234–1247.