Connectist: Istanbul University Journal of Communication Sciences

E-ISSN: 2636-8943

İSTANBUL UNIVERSITY PRESS

Araştırma Makalesi / Research Article

Sosyal Büyük Veri Ekseninde Kişisel Gizlilik Sorunsalı: Türkiye'de Eğitimli ve Kentli Sosyal Ağ Kullanıcılarının Gizlilik Sorunlarına Yaklaşımları

Personal Privacy Issue from Social Big Data Perspective: Educated and Urban Social Network Users' Privacy Approaches in Turkey

Ebru GÖKALİLER[1], Ezgi SAATCIOĞLU[2]

[1]Assoc. Prof. Dr., Yaşar University, Faculty of Communication, Department of Public Relations and Advertising, İzmir, Turkey
[2]PhD., İzmir, Turkey

ORCID: E.G. 0000-0002-4134-8447; E.S. 0000-0003-3108-0579

Sorumlu yazar/Corresponding author:
Ebru Gökaliler,
Yaşar Üniversitesi, İletişim Fakültesi, Halkla İlişkiler ve Reklamcılık Bölümü, İzmir, Türkiye
E-posta/E-mail: ebru.gokaliler@yasar.edu.tr

Geliş tarihi/Received: 26.12.2019
Revizyon talebi/Revision Requested: 23.05.2020
Son revizyon teslimi/Last revision received: 02.06.2020
Kabul tarihi/Accepted: 12.06.2020
Atıf/Citation: Gokaliler, E., & Saatcioglu, E. (2020). Sosyal büyük veri ekseninde kişisel gizlilik sorunsalı: Türkiye'de eğitimli ve kentli sosyal ağ kullanıcılarının gizlilik sorunlarına yaklaşımları. *Connectist: Istanbul University Journal of Communication Sciences, 58,* 133-167.
https://doi.org/10.26650/CONNECTIST2020-0085

ÖZ

Günlük yaşam üzerinde sosyal medyanın rolü ve etkisi her geçen gün artmaktadır. Bu durum beraberinde gizlilik kavramının anlam ve rol açısından değişimini de getirmektedir. Sosyal medyadaki içerikler aracılığıyla paylaşılan kişisel bilgiler, büyük veri havuzu içinde analiz edilerek pek çok farklı sektör tarafından kullanılmaktadır. Bu bağlamda bireylerin sosyal ağları kullanırken onayladıkları gizlilik politikaları hakkında bilgiye sahip olup olmadıkları da tartışılagelmektedir. Bu çalışmada bireylerin sosyal medyada gizliliğe bakış açılarının, büyük veri ve gizlilik konularının iletişim gizliliği yönetimi kuramı ekseninde değerlendirilmesi amaçlanmaktadır. Bu amaçla çalışmada nitel bir araştırma tasarımından ve derinlemesine görüşme tekniğinden yararlanılmıştır. Olasılıklı olmayan örneklem seçimi yöntemlerinden amaçlı örneklem yöntemiyle seçilen 18 sosyal medya kullanıcısıyla Kasım 2019-Aralık 2019 tarihleri arasında derinlemesine görüşme yapılmıştır. Veriler, Miles & Huberman (1994) modeli çerçevesinde değerlendirilmiştir. Araştırma sonucunda katılımcıların ağırlıklı olarak sosyal medyada özel yaşamlarının gizliliğine önem verdikleri ve kendilerine sunulan gizlilik ayarlarından yararlandıkları anlaşılmıştır. Öte yandan katılımcıların, sosyal medya platformlarının yayınladığı gizlilik politikalarını okumadıkları ve okusalar dahi platforma üye olmak istedikleri için onayladıkları anlaşılmıştır. Kişisel bilgilerini paylaşmaktan tedirgin olsalar bile birtakım önlemlerle paylaşmaya devam ettikleri görülmektedir. Bu bağlamda katılımcıların bir platformda bulunma, paylaşımlarla kendilerini ifade etme isteklerinin gizlilik endişelerini bastırdığı şeklinde belirtilebilmektedir.

Anahtar Kelimeler: Büyük veri, gizlilik, sosyal medya, sosyal medyada gizlilik sorunları, iletişim gizliliği yönetimi kuramı

ABSTRACT

The role and influence of social media on daily life is increasing day by day. It also brings about the change of the privacy concept in terms of meaning and role. The personal information that is being shared via social media content is analyzed in a big data pool and is used by various sectors. In this context, it is also discussed whether individuals have information about the privacy policies they approve while using social networks. In this study, it is aimed to evaluate individuals' perspectives on privacy in social media, big data and privacy issues from the perspective of communication privacy management theory. For this aim, a qualitative research design and an in-dept interview technique was used in the study. In-dept interviews were conducted between November 2019 and December 2019 with 18 social media users who were selected by purposive sampling, which is one of the non-probable sampling methods. The data was evaluated by the Miles & Huberman (1994) model. As a result, it was understood that the participants mostly paid attention to the privacy of their private lives on social media and benefited from the privacy settings offered to them. On the other hand, it was understood that the participants didn't read the privacy policies published by social media platforms and they approved those policies as they wanted to be members of those platforms. Even if they are worried about sharing their personal information, it seems that they continue to share. In this context, it can be interpreted as the participants' desire to be on a platfrom and to express themselves through sharing is suppressing their privacy concerns.

Keywords: Big data, privacy, social media, privacy issues on social media, communication privacy management theory

EXTENDED ABSTRACT

The term of big data was first used by Cox and Ellsworth (1997, p. 235) to define the issue of huge data sets' visualization. Big data means heterogeneous data that cannot be processed by using traditional database techniques (Gahi, Guennon, & Mouftah, 2016, p. 953). Social media and big data are interrelated since they are both sources and techniques. The relation between social media and big data reveals social big data. Social big data refers to the huge size of data collected from social media. The processing of social big data is carried out by various algorithms and methods (Bello-Orgaz, Jung, & Camacho, 2016, pp. 46). Social big data is an important source for understanding and evaluating human behavior. It is not wrong to say many different sectors benefit from social big data. But it also brings privacy invasion risks (boyd, & Crawford, 2012; Tufekci, 2014). Westin (1967) defines privacy as the individuals ability to decide when, how, and which personal information to share. It can also be defined as controlling the line between one's own self and others (Derlega, & Chaikin, 1977, p. 1). People have different understandings and perceptions of privacy which affect their behavior.

Big data can cause privacy issues in social media (Eroğlu, 2018, p. 133). When it comes to privacy in social media, it is possible to mention the Communication Privacy

Management Theory. Communication Privacy Management Theory was developed by Petronio (1991) to explain personal privacy in face-to-face communication. It mainly explains how people decide to reveal or not to reveal personal information. In the literature, it is stated that individuals tend to manage their privacy on digital platforms in a similar way as to face-to-face communication. Individuals think that the ownership of their content belongs to them and they want to control the content just by themselves (Child, & Petronio, 2011, pp. 23-25). Social media users draw their boundaries by using private or public accounts and deciding what to share on their accounts. Social media platforms save and archive all the stuff that has been shared by the users. All this data contribute to big data.

As social media becomes more important in everyday life people are generating more content about themselves on social media. At this point the privacy issues of social media become an important argument as it is an important contributer of big data. This study aims to understand social media users' privacy perceptions and their opinions about big data. Accordingly, 18 respondents were chosen by purposive sampling. The research has a qualitative research design. An in-dept interview was chosen as the research technique. The interview was unstructured. The data which was obtained by in-dept interviews was analyzed by descriptive analysis. Interviews were recorded and transcripted. Interview questions were derived from Sang's (2015) in-dept interview questions and also from the related literature. Those questions consisted of general questions about social media usage, privacy in social media, big data and privacy issues in the context of communication privacy management. The data was evaluated by the Miles and Huberman (1994) model.

As a result of the study, it is clear that people are using social media although they know there can be important privacy breaches. All the respondents manage their privacy in different ways as their perceptions are different too. The participants use social media for communication, socializing, and information seeking. Most of them are using private accounts to draw a line between acquaintances and strangers. So that they can feel safe. All of them are aware of tracking technologies of social media. The participants feel uncomfortable while sharing their information as they think malicious third parties can reach their information. They feel more secure when they share information with governmental institutions rather than private institutions.

GİRİŞ

Bilgiye erişim giderek daha da kolaylaşırken üretilen içeriklerle ve paylaşılan bilgilerle de veri havuzu genişlemektedir. Büyük veri ve küçük veri olarak ifade edilen veri analizleriyle bireyler hakkında sürekli yeni bilgilere ulaşılmakta; sağlık, pazarlama ve iletişim gibi pek çok alanda bu verilerden yararlanılmaktadır. Sosyal ağların günlük yaşamın bir parçası haline gelmesiyle sosyal büyük veri kavramı doğmuştur. Elde edilen veriler çeşitli yollarla işlenerek yine sosyal ağ kullanıcılarına yönelik kullanılmaktadır. Bu durum gizlilik sorunlarını beraberinde getirmektedir. Bireyler, kendileri hakkında bilgi paylaşırken bazı bilgileri gizlemeye çalışmaktadır. Bu süreç aynı zamanda enformasyonel, sosyal, psikolojik gizlilik olarak gruplandırılmakta iken gizlilik de, sosyal ilişkilerin sürdürülmesi açısından önem taşımaktadır.

Gizlilik yaklaşımına göre tutucu, faydacı, umursamaz olarak kategorileştirilen bireyler sosyal medyadan elde ettikleri kazanımlara karşın sakındıklarına göre bir denge oluşturarak paylaşımlarını kontrol altına almaktadırlar. Sosyal medyada gizlilik ilk günden itibaren tartışılagelmektedir. Yer bildirimleri, ev paylaşımları, kişisel bilgilerin paylaşımı gibi konular veri güvenliği açısından değerlendirilmektedir. Veri güvenliği tartışmaları sonucunda sosyal ağ platformları, gizlilik politikalarını ve kurallarını yayınlayarak potansiyel kullanıcılarının onayını almaktadır. Bununla birlikte bireyler, eğer bir platformun kullanıcısı olmak istiyorlar ise gizlilik politikalarını ve kuralları onaylamak zorunda kalmaktadırlar. Sosyal ağ platformlarındaki gizlilik sorunlarına bakıldığında ilk grupta bireylerin kendi paylaşımları bulunmaktadır. Bu noktada sosyal ağ kullanıcısının hangi bilgileri, içerikleri kimlerle paylaştığı söz konusudur. İkinci grupta ise bireyin paylaştığı içeriklerde yer alan diğer kişiler olmaktadır. Örneğin, bir sosyal ağ kullanıcısı arkadaşlarıyla bir fotoğraf paylaştığında fotoğrafta yer alan kişilerin gizlilikleri ihlal edilmiş midir? sorusu gündeme gelmektedir. Kişinin kendi kontrolü dışında gerçekleşen bu bilgi paylaşımı, rıza dışı da olabileceği ve içerik üzerinde hiçbir kontrolü de olmaması nedeniyle daha büyük bir gizlilik ihlali olarak değerlendirilmektedir. Bir diğer yandan kullanıcıların yer aldıkları platformlarla paylaştıkları bilgiler, bir başka gizlilik endişesi yaratmaktadır. Sosyal ağ kullanıcılarının platformlara kayıt olmak için kullandıkları bilgiler, fotoğraflar, ürettikleri içerikler veri tabanlarında saklanarak üçüncü taraflarla paylaşılabilmektedir. Bu durum platformlar tarafından da açıkça belirtilirken kimi zaman bireyler, tedirgin olsalar da platformları kullandıklarını ifade etmektedirler.

Türkiye'de sosyal medyada gizliliği ele alan çalışmalara bakıldığında sosyal medyanın gelişimi ile birlikte gizliliğin yeni bir ortama taşınmasının (Utma, 2018) Facebook özelinde sosyal medya ve büyük veri ilişkisinin etik boyutunun (Ergen, 2018) literatür çerçevesinde tartışıldığı görülmektedir. Türkiye'de sosyal ağ platformu kullanıcılarının gizlilik yaklaşımlarına yönelik çalışmalara bakıldığında ise özellikle üniversite (Öz, 2014; Zengin, Zengin, & Altunbaş, 2015; Eroğlu, 2018; Hekimoğlu, 2019) ve lise (Şimşek, 2019) çağındaki gençlere yönelik anket tekniğinden yararlanılan araştırmalar gerçekleştirildiği görülmektedir. Öz (2014) Facebook özelinde gerçekleştirdiği araştırma sonucunda; gençlerin sosyal medya kullanım düzeyleri arttıkça gizlilik sorunlarına yönelik farkındalıklarının da arttığını ve farkındalık düzeyi arttıkça Facebook'un sunduğu gizlilik ayarlarından daha katı bir biçimde yararlandıkları ortaya koymaktadır. Facebook'u daha az kullanan gençlerin ise gizlilik sorunlarına ilişkin farkındalıkları daha düşük olmaktadır. Zengin ve arkadaşları (2015) da Facebook özelinde bir anket çalışması gerçekleştirmiş olup araştırma katılımcısı olan üniversiteli gençlerin, bilgi paylaşmanın gizlilik riski taşıdığının farkında olduklarını ancak paylaşımlarının arkadaş listeleri ile sınırlı kalacağını düşündüklerini belirlemiştir. Bir diğer deyişle katılımcılar, platform ve kullanıcılar arasındaki gizlilik sorunlarına ve üçüncü tarafların olası ihlallerine yönelik farkındalık sahibi değildirler. Eroğlu (2018) tarafından gerçekleştirilen anket sonucunda ise üniversite öğrencilerinin sosyal medyada yeterli gizlilik önlemi almadıkları sonucu elde edilmektedir. Örneğin, öğrenciler bir platformda kullandıkları şifreyi diğer platformlarda da kullanmaktadırlar. Bir diğer anket çalışması ise Türkiye'deki sosyal ağ kullanıcılarının gizlilik ihlalleri hakkındaki görüşlerini ve farkındalıklarını değerlendirme amacıyla Aslanyürek (2016) tarafından gerçekleştirilmiştir. Araştırma; Facebook, Twitter ve Google Plus kullanıcılarıyla gerçekleştirilmiş olup araştırma sonucunda, katılımcıların gizlilik sorunlarına yönelik farkındalıklarının yüksek olduğu ancak platformları kullanmaktan vazgeçme eğilimlerinin düşük olduğu ortaya konmaktadır.

Hekimoğlu (2019) ise önceki çalışmalardan farklı olarak yüksek lisans tezi kapsamında Instagram özelinde bir anket çalışması gerçekleştirilmiştir. Araştırma sonucunda üniversiteli gençler, gizlilik ayarlarını kullandıkları sürece gizliliklerinin ihlal edilmeyeceğini, gözetlenmeyeceklerini düşünmektedirler. Bununla birlikte kişisel bilgilerinin reklam ve pazarlama amaçlarıyla şirketlerle paylaşılabileceğinin bilincindedirler. Evren ve örneklem seçiminde bir farklılaşmaya giden Şimşek (2019) ise Instagram özelinde lise öğrencilerine yönelik bir anket gerçekleştirmiştir. Araştırma sonuçlarına göre gençler, sosyal medyayı yararlı bulmakta ve gizliliklerine önem vermektedirler. Ancak gizlilik konusunda tam bir bilince sahip değildirler. Türkiye'de sosyal medyada gizliliği ele alan

çalışmaların ağırlıklı olarak gençlerin gizlilik yaklaşımlarına odaklandığı ve çoğunlukla Facebook özelinde, anket tekniğinden yararlanıldığı anlaşılmaktadır. Bununla birlikte farklı yaşlardan, eğitimli sosyal ağ kullanıcılarının büyük veri ekseninde sosyal medyada gizliliğe bakışlarını ele alan bir çalışma bulunmamaktadır.Bu çalışmada, sosyal ağ kullanıcılarının büyük veri ekseninde sosyal medyada gizlilik konusuna bakışlarını anlamak amaçlanmaktadır. Bu amaç doğrultusunda nitel bir araştırma tasarımından ve derinlemesine görüşme tekniğinden yararlanılmıştır. Böylelikle sosyal ağ kullanıcılarının gizliliğe bakışları, özel yaşamlarına ilişkin bilgi paylaşımları, ürettikleri içerikleri bilinçli olarak yönetip yönetmediklerine yönelik çok boyutlu ve detaylı bir biçimde değerlendirme gerçekleştirilebilecektir. Derinlemesine görüşmeler, olasılıklı olmayan örneklem seçimi yöntemlerinden amaçsal örneklem yöntemi ile belirlenen 18 katılımcı ile 15.11.2019-09.12.2019 tarihleri arasında yüz yüze gerçekleştirilmiştir. Çalışmada kullanılan araştırma tekniği ve belirlenen örneklem ile literatürdeki mevcut çalışmalardan farklılaşmak amaçlanmaktadır. Derinlemesine görüşmelerde katılımcılara yöneltilen sorular; sosyal medya kullanım alışkanlıkları, sosyal ağlardaki gizlilik kurallarına yönelik bakış açıları, gizlilik yaklaşımları, iletişim gizliliği yönetimi kuramı eksenindeki gizlilik yönetimi bulguları olarak gruplandırılarak tartışılmıştır. Çalışmada ilk olarak büyük veri kavramı açıklanarak büyük verinin doğal kaynağı olması bakımından sosyal medyada gizliliğe yer verilmektedir. İletişim gizliliği yönetimi kuramı ise bireylerin gizliliklerini nasıl yönettiklerini ele aldığı için bireylerin gizlilik ve büyük veriye bakışlarının anlaşılmasında önem taşımaktadır.

Büyük Veri ve Sosyal Medya

Günümüzde bilgiye erişim kolaylaşırken üretilen içerikler, veri havuzunu genişletmektedir. Büyük veri kavramı, ilk olarak 1997'de Cox ve Ellsworth'ün hazırladığı bir bildiride kullanılmıştır. NASA çalışanı araştırmacılar, bilimsel amaçlarla görselleştirme yapılmak istendiğinde ortaya çıkan çok büyük veri setlerinin işlenme zorluğunu "büyük veri sorunu" olarak adlandırmaktadırlar (Cox, & Ellsworth, 1997, p. 235; Aktan, 2018, p. 3). Büyük veri, geleneksel veritabanı tekniklerinden yararlanılarak işlenemeyen çok sayıdaki heterojen veriyi ifade etmektedir (Gahi, Guennon, & Mouftah, 2016, p. 953). Karışık ve dağınık haldeki büyük veri, ölçülecek daha az şey sunan küçük düzeydeki veriyle yapılabildiğinden çok daha farklı analizler sunmaktadır (Mayer-Schönberger, & Cukier, 2013, p. 13). Laney (2001) büyük verinin tanımlanmasında ve yönetiminde 3 unsurdan söz etmektedir. Bunlar; 3V olarak anılan veri hacmi, veri hızı, veri çeşitliliğidir. Veri hacmi, verinin boyutu olup verinin depolanmasını ilgilendirmektedir. Veri hızı,

büyük verinin çok hızlı üretilmesini vurgularken çeşitlilik, verinin standart bir formatta üretilmediğini fotoğraftan metne çeşitli formatlarda olduğunu ifade etmektedir. Yıllar içinde Laney'nin (2001) 3V'sine doğruluk ve değer eklenerek 5V oluşturulmuştur. Doğruluk, farklı kaynaklardan elde edilen verilerin karşılaştırılarak doğrulanmasıdır. Değer, büyük verinin işlenmesi sonucunda ortaya yarar sağlayan bir değerin çıkarılmasıdır (White, 2012, p. 211; Bello-Orgaz, Jung, & Camacho, 2016; Cyganek et al., 2016, pp. 498-499; Gahi et al., 2016, p. 953; Aktan, 2018, p. 4).

Literatürde büyük veri; sağlık (Belle et al., 2015), reklam ve pazarlama (Ashworth, & Free, 2006; Couldry, & Turow, 2014), sosyal medya (Mahrt, & Scharkow, 2013; Stieglitz, Mirbabaie, Ross, & Neuberger, 2018) açısından incelenmektedir. Literatürde büyük veri çalışmalarında sosyal medyadan yararlanan (Xu et al., 2016) çalışmalar olduğu gibi sosyal medya araştırmacıları da büyük veri kavramından yararlanmaktadır (Stieglitz et al., 2018). Bu bağlamda literatürde sosyal büyük veri (Guellil, & Boukhalfa, 2015; Sang, 2015; Bello-Orgaz et al., 2016), sosyal medya büyük verisi (Tufekci, 2014; Lynn et al., 2015) kavramları bulunmaktadır. Sosyal büyük veri, sosyal medyada toplanan devasa boyuttaki veriyi ifade ederken bu veriler, çeşitli algoritmalar ve yöntemlerle işlenmektedir (Bello-Orgaz et al., 2016, p. 46). Sosyal büyük verinin işlenmesi; verinin bulunması, toplanması, hazırlanması ve analiz edilmesi olmak üzere 4 aşamadan oluşmaktadır (Stieglitz et al., 2018, p. 158). Sosyal medyada veri madenciliği; fikir madenciliği ve duygu analiziyle gerçekleştirilebilirken (Guellil, & Boukhalfa, 2015, p. 134) sosyal ağ analizi, metin analizi gibi tekniklerden yararlanılmaktadır (Bello-Orgaz et al., 2016, p. 49). Sosyal medya madenciliği 3 alanda gerçekleştirilebilmektedir. Bunlardan ilkinde kullanıcıların verileri temel alınmaktadır. Böylelikle topluluklar değerlendirilmekte, kullanıcılar sınıflandırılmaktadır. İkinci alanda; kullanıcı ilişkileri temel alınarak bağlantılar, sosyal ilişkiler, ilişkinin güçlülüğü tahmin edilebilmektedir. Üçüncü alanda; kullanıcıların içerikleri temel alınarak öneriler oluşturulabilmekte, duygu analizi yapılabilmektedir (Tang, Chang, & Liu, 2014, pp. 23-26).

Sosyal medya büyük verisi, insan davranışının anlaşılarak değerlendirilmesinde önemli bir kaynaktır. Başta araştırmacılar ve pazarlama profesyonelleri olmak üzere pek çok farklı sektör, sosyal medya büyük verisinden yararlanmaktadır. Sosyal medya büyük verisinin istismara açık olması beraberinde riskler getirmekte (boyd, & Crawford, 2012; Tufekci, 2014); risklerin temelinde, sosyal medyadaki gizlilik sorunu yer almaktadır (Smith, Szongott, Henne, & von Voight, 2012).

İletişim Gizliliği Yönetimi Kuramı, Sosyal Medyada Gizlilik ve Büyük Veri İlişkisi

Sosyal medya platformlarının doğuşundan bu yana gizlilik, önemli bir tartışma konusu olagelmiştir (boyd, & Ellison, 2007, pp. 221-222). Farklı çıkarımlara olanak tanıyan sosyal medya büyük verisinin varlığı, beraberinde gizliliğin ihlalini de getirmektedir (Tang et al., 2014, p. 21; Eroğlu, 2018, p. 133). Gizlilik; bireyin kendisine ait bilgileri nerede, ne zaman, nasıl, hangi düzeyde paylaşacağını belirleme yeteneği olarak tanımlanmaktadır (Westin, 1967). Bir diğer tanımda gizlilik; bireylerin birbirleriyle kurdukları ilişkinin düzeyini yani sınırlarını kontrol etmelerini ifade etmektedir (Derlega, & Chaikin, 1977, p.1). Bireyler; kişisel gizliliğin bir gereği olarak sosyal yaşamda sınırlar oluşturmakta, sürdürmekte ve düzenlemektedir (Zimmer, Kumar, Vitak, Liao, & Kritikos, 2018, p. 3). Gizliliğin başarılı bir biçimde yönetilmesi sosyal ilişkilerin sürdürülmesi açısından önem taşımaktadır (Nippert-Eng, 2010). Bireylerin, kişisel bilgilerinin paylaşımı üzerinde kontrol sahibi olmaları ise gizlilik hakkı olarak tanımlanmaktadır (Nissenbaum, 2009, p. 127).

Sandra Petronio'nun ortaya koyduğu İletişim Gizliliği Yönetimi Kuramı; bireylerin, kişisel bilgilerini nasıl yönettiklerini ele almaktadır. İletişim Gizliliği Yönetimi Kuramı, kişisel gizliliğin nasıl etkili bir biçimde sağlandığını, hangi durumlarda aşıldığını anlamaya dayanmaktadır (Petronio, 2002, p. 2). Bu durum aynı zamanda iletişimin sınırlarını belirlemekte olup Petronio (1991) tarafından iletişim sınırı yönetimi olarak da isimlendirilmektedir. Bireylerin sahip oldukları sınırlar, kişisel bilgiler üzerinde koruyucu görevi görmektedir. Hangi bilginin, ne zaman, kiminle paylaşılacağına karar veren kişisel bilginin sahibi olmaktadır (Griffins, 2011, p. 168). Bireyler, kişiler arası iletişim çerçevesinde kişisel bilgilerini diğerleriyle paylaşabilmektedirler. Bu paylaşım, aralarındaki ilişkiyi ve iletişimi güçlendirici nitelik taşımaktadır. Bununla birlikte kişisel bilgilerin paylaşılması sonucunda bilginin ortak sahibi haline gelen bireylerin sahip oldukları bilgiyi, üçüncü kişilerle paylaşması sınırları ihlal ederek olumsuz sonuçlar doğurabilmektedir (Griffin, 2011, p. 168). Kişisel gizlilik sınırlarının korunması bireyin gizliliğinin korunmasıdır (Child, & Petronio, 2011, p. 23). Bireyler, kişisel bilgilerini açıklamadıkları zaman kişisel bir sınır; açıkladıklarında ise kolektif bir sınır oluşturmaktadırlar. Kolektif sınırda bilgi, ilişkiye yani bilginin ilk sahibi ve paylaştığı kişiye ait olmaktadır (Petronio, 2002; Jin, 2013, p. 815). Bilginin ortak sahipliği arttıkça sınırlar incelmektedir (Sang, 2015, p. 24). Bireyler, kendilerine özgü gizlilik kuralları geliştirmektedir. Bu kuralların geliştirilmesinde kültür, cinsiyet, motivasyon, bağlam ve risk-fayda oranı süreci etkileyen temel faktörlerdir. Kültür; gizliliğe verilen değere ilişkin kültürel beklentileri ifade etmektedir. Cinsiyet,

gizlilik yönetiminde dişi ve erkek olmaya dayalı normları, motivasyon; bireyin isteklerini, ihtiyaçlarını ifade etmektedir. Dördüncü faktör olan bağlam, bireyin içinde bulunduğu koşulların etkisini ifade etmektedir. Son olarak gizlilik üzerinde her zaman risk-fayda faktörü bulunmaktadır. Risk-fayda faktörü; bireyin hangi faydayı ne kadar elde edeceğine bağlı olarak gizlilik sınırlarını ne kadar gevşeteceğini ifade etmektedir (Petronio, 2002; Waters, & Ackerman, 2011, p. 104).

Literatürde İletişim Gizliliği Yönetimi Kuramı'nın kişiler arası iletişim (Petronio, 1991; Durnham, 2008), sağlık (Petronio, & Kovach, 1997) gibi alanlarda değerlendirilmektedir. İletişimin dijitale taşınmasıyla bireylerin, sosyal medyada özellikle sosyal ağ platformlarında yaptıkları paylaşımlar, İletişim Gizliliği Yönetimi Kuramı çerçevesinde değerlendirilebilmektedir (Metzger, 2007; Child, & Petronio, 2011; Waters, & Ackerman, 2011; Cavusoglu et al., 2013; Jin, 2013; Chennamaneni, & Taneja, 2015; Sang, 2015; Zimmer et al., 2018). İletişim gizliliği dijital ortamda da yüz yüze iletişime benzer biçimde yürütülmektedir (Metzger, 2007, p. 354). Bireyler, sosyal medyada paylaştıkları içeriklerde kişisel bilgilerinin sahipliğinin kendilerine ait olduğunu düşünmekte ve paylaştıkları bilgilerin üzerinde kontrol sahibi olmak istemektedirler (Child, & Petronio, 2011, pp. 23-25).

Bireyler, sosyal medyayı gündelik yaşamlarının bir parçası haline getirerek günlük aktivitelerini diğer kullanıcılarla paylaşmakta; arkadaşlık, sohbet gibi çevrimdışı ortamda gerçekleştirdikleri etkinlikleri sosyal medyada da gerçekleştirmektedirler. Ayrıca yer bildirimleri, fotoğraflar aracılığıyla gündelik yaşamdaki etkinliklerini sosyal medyada paylaşarak sosyal medya hesaplarını, yaşamlarının bir yansıması haline getirmektedirler. Bu bağlamda sosyal medya kullanıcıları, profillerinde sürekli olarak kendileri hakkındaki bilgileri paylaşmaktadırlar (Joinson, Houghton, Vasalou, & Marder, 2011; Nguyen, Bin, & Campbell, 2012; Tosun, 2012; Utma, 2018). Drennan, Mort ve Previte (2006, pp. 9-11) sosyal medyada üç tür gizlilik yaklaşımı olduğunu belirtmekte olup bu yaklaşımları; gizlilik farkındalığı, gizlilik şüpheciliği, gizlilik etkinliği olarak sıralamaktadır. Gizlilik farkındalığı; bireylerin, sosyal medyada kişisel bilgilerini paylaşmalarının taşıdığı risklere dair bilgilerini, hassasiyetlerini ifade etmektedir. Gizlilik şüpheciliği; bireylerin, paylaştıkları bilgilerin kurumlar tarafından kullanılmasına yönelik endişelerini ifade etmektedir. Gizlilik etkinliği; bireylerin, gizlilikle ilişkili davranışlarını ifade etmektedir. Burgoon (1982, pp. 210-232) gizliliğin boyutlarını; enformasyonel gizlilik, sosyal gizlilik, psikolojik gizlilik ve fiziksel gizlilik olarak sıralamaktadır. Enformasyonel gizlilik, bireyin kendisine ait olan bilgileri yani kişisel

bilgilerini işleme ve iletme kontrolünü elinde bulundurmasıdır. Sosyal gizlilik; bireyin, diğerleriyle yakınlığını kontrol etmesidir. Psikolojik gizlilik; bireyin, bilişsel ve duygusal girdileri ve çıktıları üzerinde sahip olduğu kontroldür. Fiziksel gizlilik; bireyin, kişisel alanına istenmeyen erişimleri kontrol edebilmesini ve kişisel alanındaki özgürlüğünü ifade etmektedir (Dienlin, & Trepte, 2014, p. 286). Her bireyin sahip olduğu değerlere ve algılara dayanan kendisine özgü bir gizlilik anlayışı ve endişeleri bulunmaktadır (Joinson, & Paine, 2007, p. 244). Bireyler; gizlilik yaklaşımlarına göre tutucular, faydacılar, umursamazlar olmak üzere üç şekilde ele alınmaktadır. Tutucuların ödün vermeyi kabul etmedikleri bir gizlilik anlayışları bulunmaktadır. Hangi amaçla olursa olsun kişisel verilerin depolanmasına ve kullanılmasına karşı çıkmaktadırlar. Faydacılar, ılımlı bir gizlilik anlayışına sahip olup belirli koşullarda, verilerin toplanmasının ve kullanılmasının yararlı olacağını ifade etmektedirler. Gizliliğe yönelik riskler için kurumlar tarafından önlemler alınması gerektiğini savunarak alınan önlemlere göre karar vermektedirler. Umursamazlar, gizliliğe yönelik hiçbir endişe taşımamaktadırlar (Westin, 2003, p.445). Bireyler, gizlilik tutumlarına ve yaklaşımlarına uygun olan davranışları sergilemektedirler (Dienlin, & Trepte, 2014, p. 285). Van Dijk (2016, pp. 175-180) gizliliğe yönelik tehditleri; veri madenciliği ve sınıflandırma, takip teknolojileri, fiziksel takip olarak sıralamaktadır. Büyük veriye, veri madenciliği yapılarak belirli bir kişi veya grubun davranış haritası, bilgileri çıkarılabilmektedir. Sosyal medya kullanıcılarının hangi cihazlarla hangi konumdan hangi internet sayfalarını inceledikleri, kullandıkları sosyal medya platformlarında gerçekleştirdikleri sayfa ziyaretleri, kullanım alışkanlıkları takip teknolojileriyle izlenebilmektedir. Fiziksel takip, kamera gibi dijital cihazlarla toplanan biyometrik verilerle gerçekleştirilen takibi ifade etmektedir. Böylelikle güvenlik kameraları gibi araçlarla ne zaman, nerede bulunduğunuz belirlenebilmektedir

Debatin, Lovejoy, Horn ve Hughes (2009, p. 88) sosyal medyada gizliliği Facebook üzerinden ele alarak Facebook Buzdağı Modeli'ni oluşturmuştur. Shozi ve Mtsweni (2017, p. 3) Facebook Buzdağı Modeli'ni, Sosyal Medya Buzdağı Modeli olarak ele almaktadır. Buzdağının görünen yüzü, sosyal medya kullanıcılarının gördükleridir. Görünen yüzde kullanıcıların birbirleriyle etkileşimleri, eğlence vb. bulunmaktadır. Buzdağının görünmeyen yüzündeyse büyük veriyi oluşturan kişisel bilgiler, veri madenciliğiyle hedefli reklam ve pazarlama faaliyetleri için kullanılmaktadır. Sosyal medyada gizlilik söz konusu olduğunda hem bireyler arasında hem de birey ve kurum arasında gizlilik ilişkileri oluşmaktadır. Sosyal gizlilik olarak tanımlanan bireyler arasındaki gizlilik; kişinin kimliği, itibarıyla ilişkilidir. Sosyal gizliliğin ihlali, kişinin bilgilerine,

paylaşımlarına istemediği kişilerin erişimini veya bireyin hakkında kendi kontrolü dışında bilgiler paylaşılmasını ifade etmektedir. Birey ve kurum arasındaki gizlilik; kurumsal gizlilik olup verilerin yönetimi, korunması, kullanımı, paylaşımını ifade etmektedir (Raynes-Goldie, 2012, p. 81). Sosyal medya platformları tarafından toplanan büyük veri işlenip analiz edilerek reklam hedefleme, ürün-hizmet önerilerinin tüketicilere iletilmesi gibi amaçlarla kullanılmaktadır (De Prato, & Simon, 2015).

Kurumsal gizliliğin ihlali temelde, gözetimin bir boyutu olan ticari veya bir diğer deyişle kurumsal gözetime işaret etmektedir. Gözetim kavramı; bir güç sahibinin veya güç sahibi olan bir kesimin, otoritesi altında bulunan diğer unsurlara yönelik takibini ifade etmektedir (Whiting, & Williams, 2013, p. 367). Gözetimin içselleştirildiği ve toplumun da rıza göstererek bu sürece dahil olduğu toplumlar, gözetim toplumu olarak adlandırılmaktadır (Çoban, 2014, p. 3). Dijital olanakların ve sosyal medyanın tanımış olduğu takip, kayıt ve depolama işlemleriyle oluşturulan veri tabanlarıyla doğan büyük veri, geleneksel anlamdaki fiziksel odaklı gözetime yeni bir boyut kazandırmaktadır (Lyon, 2001, pp. 114-115). Ticari gözetim, pazar araştırmaları ve tüketici davranışlarına yönelik araştırmalarla uzun yıllardır gerçekleştirilse de asıl yükselişini dijitalleşmeyle yaşamaktadır. Ticari amaçlarla toplanmış olan büyük veriye, veri madenciliği yapılarak tüketici profilleri oluşturulabilmektedir. Böylelikle davranış kalıpları belirlenebilmekte, gelecekteki davranışlara yönelik tahminlerde bulunulabilmektedir (Pridmore, & Zwick, 2011, p. 271). Ticari gözetim, birey ve kurum arasındaki gizliliğin ihlali anlamına gelebilmektedir. Fuchs (2011) Facebook'u ele aldığı çalışmasında platformun gizlilik politikasında; kullanıcıların kişisel bilgilerinin izinsiz olarak paylaşılmayacağı bilgisi yer alsa da kullanıcıların, verileri üzerinden sürekli olarak hedefli reklamcılığa maruz kaldıklarını ve sosyal medyada gizliliğin bir meta halini aldığını ifade etmektedir. Bu bağlamda sosyal medya kullanıcılarının bilgileri ve davranış biçimleri reklamverenlere satılmaktadır.

Sosyal medyada ticari gözetimin yanı sıra devlet gözetimi de tartışılagelmektedir. Devlet gözetimi de kurumsal gizliliğin ihlali anlamına gelen bir diğer gözetim olmaktadır. Sosyal medya verisi değerlendirilerek davranış ve kişilik profillemesi gerçekleştirilebilmekte ve tüketim alışkanlıklarından politik görüşlere birçok çıkarımda bulunulabilmektedir. Bu bağlamda sosyal ağ kullanıcılarının, gönüllü olarak paylaşmakta oldukları bilgilerinden ve içeriklerinden yararlanılarak kamu oyu yoklamaları da yapılabilmekte; kullanıcılar, politik görüşlerine göre sınıflandırılabilmekdir (Mitrou, Kandias, Stavrou, & Gritzalis, 2014). Mitrou ve arkadaşları (2014) bu durumu, sosyal

ağ kullanıcılarının gözetime katkı sağladıkları anlamına gelen katılımcı panoptisizm olarak değerlendirmektedirler. Panoptikon kavramı, Jeremy Bentham tarafından tasarlanmış olan hapishane mimarisinin ismi olmaktadır. Bu hapishane mimarisinde; tüm mahkumların gözetlenebildiği merkezi bir gözetleme noktası bulunurken mahkumlar, ne zaman gözetlendiklerinden emin olamamaktadırlar (Foucault, 1995, pp. 200-201). Markaların yaptığı gibi devletler de sosyal medya izlemesi yapabilmektedirler. Amerika Birleşik Devletleri'nde güvenlik güçlerinin sosyal medya platformlarında tehdit taraması ve şiddet eğilimlerini ölçümlediği yazılımlar bulunduğu bilinmektedir. Bu durum bir yandan suçluların bulunması için yarar sağlarken diğer yandan sosyal medyada gizliliğin ihlali, demokrasi açısından sorunlara da işaret edebilmektedir. Bu bağlamda sosyal medyada gizliliğin yasalarla korunma altına alınması önem taşımaktadır (Scott, 2017).

Smith ve arkadaşları (2012, pp.2) sosyal medyada gizlilik sorunlarını iki grupta ele almaktadır. Bunlardan ilki kişinin bilgilerini herkese açık bir biçimde paylaşmasıdır. İkincisiyse daha büyük gizlilik riski oluşturan diğer sosyal medya kullanıcılarının paylaştıkları içeriklerdir. Çünkü bireyler başkalarının içeriklerinde kontrol sahibi olamamaktadır. Örneğin sosyal medya kullanıcısı hangi fotoğrafı paylaşacağını kendisi belirlerken başkaları tarafından paylaşılan fotoğraf üzerinde bir denetim sağlayamamaktadır. Özellikle ikinci grup, büyük verinin kontrolsüz kaynağı olarak değerlendirilmektedir.

Sosyal medya kullanıcılarının gizlilik endişeleri söz konusu olduğunda en yüksek endişe, üçüncü taraflardan yanadır. Kullanıcılar, bilgilerinin kendilerinden habersiz bir biçimde kullanılmasından ve istemedikleri kişilerin bilgilerine erişmesinden endişe duymaktadırlar (Öz, 2014, p. 6248; Onifade, Olomu, Ajao, Atoyebi, & Ilevbare, 2018, p. 44). Bu bağlamda sosyal medyadaki gizlilik yönetimi stratejilerinden biri; profil erişimini yalnızca yetki verilen kullanıcılarla sınırlandırmaktır. Sosyal ağ platformu kullanıcılarının, profil erişimi çerçevesinde gerçekleştirdikleri gizlilik yönetimlerini inceleyen bir araştırmada; gizlilikleri ihlal edilen katılımcıların %82'sinin ihlal nedeniyle profillerinin gizlilik ayarlarını değiştirdiği belirlenmiştir. Ek olarak katılımcıların %42'si çevrelerindeki kullanıcıların gizliliklerinin ihlal edilmesine ilişkin olumsuz deneyimlerini duyduklarında gizlilik ayarlarını değiştirmektedir. Bu bağlamda sosyal medya kullanıcıları, kendi yaşadıkları ihlallerle karşılaştırıldığında çevrelerinde olan ihlallerden daha az etkilenmektedir (Debatin et al., 2009, p. 83).

Sosyal medya kullanıcıları, gizliliklerinin ihlal edilmesinden çekiniyorlarsa daha az bilgi açıklama eğilimdedirler (Cavusoglu, Phan, & Cavusoglu, 2013, p. 14). Öte yandan sosyal ağ platformlarının kullanıcıları, sosyal medyada gizliliğin ve veri güvenliğinin düşük düzeyde olduğunu bilmelerine rağmen sosyal ağlarda gönüllü bir biçimde paylaşım yapmayı sürdürmektedirler (Acquisti, & Gross, 2006, p. 1). İletişim gizliliğinin yönetiminde risk-fayda faktörü önemli bir rol oynarken bu durum sosyal medyada da kolaylıkla görülebilmektedir. Bireylerin amaçladıklarına ne kadar ulaştıkları yani ne kadar fayda sağladıkları, kişisel bilgilerini paylaşmaları üzerinde etkili olmaktadır (Chennamaneni, & Taneja, 2015, p. 7). Örneğin, çevrimiçi alışveriş yapmak isteyen bir kişinin alışverişi gerçekleştirebilmek için kredi kartı numarasını, kimlik bilgilerini paylaşması gerekmektedir. Bu bağlamda kurumsal düzeyde gizlilik; ilgili kurumların gizlilik politikaları ve aldıkları önlemler önem taşımaktadır (Pan, & Zinkhan, 2006, p. 337). Çevrimiçi alışveriş faaliyetleri söz konusu olduğunda birer tüketici konumuna geçen sosyal medya kullanıcıları; kişisel bilgilerini paylaşmaktan çekindiklerini ve gizlilik sınırları ihlal edildiğinde rahatsız olduklarını belirtmektedirler. Örneğin, e-posta ve telefon numaraları üzerinden çok fazla istenmeyen mesaj almaktadırlar (Metzger, 2007, p. 354). Kurumsal gizliliği ele alan bir diğer araştırmaya göre ise üniversite çağındaki gençler, kişisel bilgilerini ticari kurumlardansa resmi kurumlarla daha rahat bir biçimde paylaşmakta ve bilgilerinin, haberdar oldukları amaçlar doğrultusunda kullanılmasında sorun görmemektedirler. Ancak pazarlama faaliyetleri çerçevesinde kişisel bilgilerinin paylaşılmasından rahatsızlık duymaktadırlar (Eroğlu, 2018, p. 151).

Sosyal medya kullanıcılarının bilgi paylaşımları üzerindeki etkenleri irdeleyen bir diğer araştırmada gizlilik davranışının en önemli etkeninin, bilgi paylaşımına yönelik algılanan risk olduğu ortaya konmaktadır. Platformda yer alan gizlilik ayarlarının kullanılabilirliğinin bilgi paylaşımı üzerindeki etkisi daha düşük düzeydedir. Kişilerin gizliliğe verdikleri önem, bilgi paylaşımını en düşük düzeyde etkilemektedir (Garg, Benton, & Camp, 2014). Bu bağlamda sosyal medya kullanıcılarının, gizlilik ihlaline yönelik yüksek risk algılamaları bilgi paylaşımlarını azaltmaktadır. Öte yandan, gizliliğe verdikleri önemin en düşük düzeyde etki sahibi olması gizliliklerini yönetirken risk-fayda etkeninin öne çıktığını göstermektedir.

We are Social tarafından hazırlanan rapora göre Ocak 2019'da Türkiye'de en çok kullanıcıya sahip platformlar olan Facebook, Instagram, Twitter, Linkedin ve Snapchat ("Digital in 2019…," 2019) veri gizliliği ilkelerini kullanıcılarla paylaşarak hangi verileri topladıkları, ne amaçla kullandıkları, kullanıcıların platformdan ayrılmaları halinde

verilerin silinmesi hakkında bilgi vermektedir ("Snapchat Gizlilik Politikası," 2019; "LinkedIn Gizlilik Politikası," 2019; "Twitter Privacy Policy," 2019; "Veri İlkesi," 2019). Sosyal ağ platformlarının kullanıcılarının platformlara ait gizlilik politikalarını okuma eğilimleri düşük olmakla birlikte ilgili platformlarda bulunan gizlilik ayarlarının farkında olup bu ayarlardan yararlanmaktadırlar (Tuunainen, Pitkanen, & Hov, 2009, p. 14). Ayrıca kullanıcılar, yeni gizlilik ayarları eklendikçe bu ayarları da kullanmaya başlamakta ve böylece kendilerini daha rahat hissedebilmektedirler (Cavusoglu, Phan, & Cavusoglu, 2013, p. 14). Sosyal medya kullanıcılarının gizlilik önlemleri almaları, gizlilik yönetimlerinde belirli sınırlar oluşturduklarını göstermektedir (Metzger, 2007).

AMAÇ VE YÖNTEM

Sosyal medyanın günlük yaşam pratikleri içindeki yeri giderek güçlenmekte olup sosyal medya ve günlük yaşam arasında oluşan ilişki nedeniyle sosyal medyada paylaşılan kişisel veriler de artmaktadır. Sosyal medya büyük verisi; kullanıcı, ilişki ve içerik ekseninde farklı alanlardaki veri madenciliği çalışmaları için kullanılmaktadır. Bu bağlamda büyük veri çerçevesinde sosyal medyada gizlilik, önemli bir tartışma konusu olagelmektedir. İletişim gizliliği yönetimi kuramı ekseninde değerlendirildiğinde kullanıcılar, yüz yüze iletişimde olduğu gibi sosyal medyada da yaşamlarına ilişkin bilgileri ne kadar paylaşacaklarını belirleyerek bilinçli olarak yönetmektedirler. İlgili yaklaşımdan yola çıkılan bu çalışmanın amacını; Türkiye'de eğitimli ve kentli sosyal medya kullanıcıları özelinde, sosyal ağ platformu kullanıcılarının büyük veri ekseninde sosyal medyada gizliliğe bakışlarını anlamak oluşturmaktadır. Araştırma kapsamında sosyal medya kullanıcılarının gizlilik anlayışı, sosyal medyadaki gizliliğe yaklaşımları üzerinden büyük veri olgusuna yönelik görüşleri nitel bir araştırma tasarımıyla derinlemesine görüşme tekniğinden yararlanılarak incelenmiştir. Çalışmanın amacı doğrultusunda araştırma soruları belirlenmiştir:

1. Katılımcıların sosyal ağlardaki gizlilik kurallarına bakış açısı nedir?
2. Katılımcıların sosyal ağlarda veri paylaşımına yönelik görüşleri nedir?
3. Katılımcılar hangi tür gizlilik yaklaşımına sahiptirler?
4. Katılımcılar İletişim Gizliliği Yönetimi ekseninde kendilerini nerede değerlendirmektedirler?

Araştırmanın evrenini Türkiye'deki eğitilimli ve kentli sosyal medya kullanıcıları oluşturmaktadır. Araştırma kapsamında olasılıklı olmayan örneklem seçimi yöntemlerinden olan amaçlı örneklem kullanmıştır. Amaçlı örneklem, odaklanılmış

gruba yönelerek örneklemi daraltmak ve doğru kitleye ulaşmak için tercih edilmektedir (Kemper, & Stringfield, 2003, p. 279). Araştırma; amaçlı örneklem yöntemiyle saptanmış sosyal medya kullanıcılarıyla derinlemesine görüşme tekniği kullanılarak gerçekleştirilmiştir. Derinlemesine görüşme, araştırılan konunun tüm boyutlarını ele alan genellikle açık uçlu soruların yer aldığı ve detaylı cevaplarla yüz yüze görüşülerek gerçekleştirilen veri toplama tekniğidir (Tekin, 2006, p. 101). Sosyal medya kullanım sıklıkları, içerik üretimleri, profillerinin gizlilik tercihleri dikkate alınarak en fazla çeşitlilik olması amaçlanmıştır. Bu süreçte farklı demografik özelliklerin de olması göz önünde bulundurulmuştur. Çalışmanın giriş bölümünde de değinildiği üzere literatürde, sosyal medyada gizlilik sorunsalının özellikle üniversite çağındaki gençlere odaklanılarak değerlendirildiği görülmektedir. Bu çalışmada farklılaşma adına farklı yaş gruplarından eğitimli bireylerle görüşmeler gerçekleştirmek amaçlanmıştır. Lisans ve lisans üstü eğitim düzeyindeki kentli sosyal medya kullanıcılarıyla gerçekleştirilecek görüşmelerle sosyal medyada gizlilik üzerine görüşleri anlaşılabilecektir. Derinlemesine görüşmelerde açık uçlu sorulardan yararlanılmış olup derinlemesine bilgi alınması amacıyla yapılandırılmamış görüşme formu kullanılmıştır..

Araştırma kapsamındaki sorular Sang'in (2015) çalışmasındaki derinlemesine görüşme soruları ve literatür taramasından elde edilen ifadelerden oluşmuştur. Görüşme formu; demografik sorular, sosyal medya kullanım alışkanlıklarıyla ilgili genel sorular, sosyal medya kullanımında gizlilik soruları, bireylerin gizlilik yaklaşımlarına yönelik sorular, İletişim Gizliliği Yönetimi kuramı ekseninde büyük veri ve gizlilik sürecini ifade eden sorular olarak gruplanmıştır. Görüşme formunda 20 soru bulunmaktadır. Sorular, uzman bir akademisyenle birlikte tartışılarak revize edilmiştir. Pilot görüşme, 4 katılımcıyla gerçekleştirilerek dikkat çeken anlam ve ifade karışıklıkları düzenlenmiştir. Araştırma, 15.11.2019-09.12.2019 arasında 18 katılımcıyla gerçekleştirilmiştir. Görüşmeler, 60-75 dakika arasında sürmüştür. Görüşme, katılımcının izniyle ses kaydına alınarak sonrasında deşifre edilmiştir. Katılımcıların ifadeleri olduğu gibi aktarılmıştır. Görüşme metinleri ortak değerlendirilerek metinler arasında ortak dil olması sağlanmıştır. Veriler, Miles ve Huberman (1994) tarafından geliştirilen Miles & Huberman modeli çerçevesinde değerlendirilmiştir. Miles & Huberman modeli; nitel analize yönelik bir modeldir. Model; veri azaltma, veri sunumu, sonuç çıkarma olmak üzere 3 bileşenden oluşmaktadır. Bileşenlerle birlikte aynı anda yürütülebilen kodlama, not alma ve öneri geliştirme olmak üzere 3 işlem de bulunmaktadır.Bir diğer deyişle analiz süresince tüm bileşenler ve işlemler aynı anda ve tekrarlı bir biçimde gerçekleştirilebilmektedir.

BULGULAR

Katılımcıların Demografik Özellikleri

Derinlemesine görüşme gerçekleştirilen ve amaçsal olarak belirlenen toplam 18 katılımcının sosyo-demografik özellikleri incelendiğinde; toplam 8 kadın, 10 erkek katılımcı bulunmaktadır. Katılımcıların yaş aralığı 19-44 arasında değişirken katılımcıların yaş ortalaması 29,83'tür. Eğitim düzeyleri dağılımına göre 7 katılımcı lisansüstü eğitim düzeyinde, 11 katılımcı lisans eğitim düzeyindedir. Tüm katılımcılar, sosyal medyayı günde bir defadan fazla kullanmaktadır (Tablo 1).

Sosyal Medya Kullanım Alışkanlıklarına Yönelik Bulgular

Araştırma katılımcılarına sosyal medya kullanım alışkanlıklarını anlamaya yönelik olarak "İlk sosyal medya hesabınızı ne zaman açtınız?", "Hangi tür sosyal ağları tercih edersiniz–işle ilgili, arkadaşlarla sosyalleşme, haber alma vb.?" "Hangi sosyal medya ağını tercih edersiniz?" "Sosyal ağlarda genellikle kiminle iletişim kurarsınız?" "Sosyal ağ sayfanızda her gün ne tür içerikler paylaşırsınız?" soruları yöneltilmiştir. 12 katılımcı (K1, K2, K4, K7, K9, K10, K12, K13, K14, K15, K16, K18) ilk sosyal medya hesaplarının Facebook'ta olduğunu belirtirken katılımcıların %88,8'i Facebook hesaplarını 2003-2009 arasında açmıştır. Bir katılımcı (K3) Netlog, bir katılımcı (K8) Hi5, 3 katılımcı (K5, K6, K17) Yonja yanıtını vermiştir. Bir katılımcı (K11), açtığı ilk sosyal medya hesabının Twitter olduğunu sonrasında Facebook hesabı açtığını belirtmektedir.

Sosyal medya; sosyalleşme, iletişim, haber edinme gibi pek çok olanak sunmaktadır. Ayrıca kullanıcılar, sosyal medyadaki varlıkları, ürettikleri veya üretmedikleri içerikler hakkında pek çok bilgi sunmaktadırlar (Joinson et al., 2011; Nguyen et al., 2012; Tosun, 2012; Utma, 2018). Katılımcılar çoğunlukla haber alma, arkadaşlarıyla iletişim kurma amacıyla sosyal ağları kullanmaktadır. Katılımcıların en çok tercih ettikleri sosyal ağlar; Facebook, Twitter, Instagram'dır. Katılımcıların kullandıkları mecraların, kullanım amaçları doğrultusunda farklılık gösterdiği anlaşılmakta olup aşağıda katılımcıların yanıtlarından örneklere yer verilmektedir.

> K1: Bilgi amaçlı, haber almak için tercih ediyorum. Modern insanın ilk işi 5-6 yıl önce gazete okumaktı. Yerini şimdi Twitter aldı (Erkek, 44, Lisans).

K3: Doğrudan haber almak, gazete gibi kullanıyorum. Sadece Twitter kullanıyorum (Erkek, 27, Lisansüstü).

K4: Sosyal ağları tercih ediyorum. Hem arkadaşlarımdan haber almak hem de gündemden geri kalmamak, haber almak için kullanıyorum. En çok kullandığım Facebook. Arkadaş ve aile üyeleriyle Facebook'ta iletişim kuruyorum aynı zamanda haber de takip ediyorum. Yurtdışındaki arkadaşlarımla Facebook görüntülü arama yapıyorum (Erkek, 36, Lisansüstü).

K5: Haber almak için kullanıyorum. En çok Twitter kullanıyorum. Facebook'ta içerik paylaşıyorum, Instagram'da arkadaşlarımla iletişim kuruyorum (Erkek, 25, Lisansüstü).

K6: Arkadaşlarla sosyalleşmek, dünyadan haber almak için kullanıyorum. En çok Instagram'da paylaşım yapıyorum ama en çok Twitter'ı okuyorum. Arkadaşlarımla iletişim kuruyorum (Kadın, 26, Lisansüstü).

K12: Daha çok arkadaşlarla sosyalleşme ve yakınlarımdan haber almak için sosyal ağları tercih ederim. En çok Whatsapp ve Instagram hesaplarımı aktif olarak kullanırım. Bunun dışında takip ettiğim fenomenler, ünlüler aracılığıyla istemesem bile markalarla iletişim kurmuş olduğumu düşünüyorum (Kadın, 26, Lisans).

Katılımcıların sosyal medyada yaptıkları paylaşımlar farklılık göstermektedir. K1, K2, K5, K6, K8 özel yaşamlarını sosyal medyada paylaşmamayı tercih ederken (genel katılımcılar arasında %27,7 oranda) K7, K12 için sosyal medya yaşamlarının bir yansıması (genel katılımcılar arasında %11,2) olmaktadır. Ayrıca K4, K9, K10, K11 sık paylaşım yapmadıklarını ancak zaman zaman yaşamlarındaki gelişmeleri paylaştıklarını, aileleri ve arkadaşlarıyla fotoğraf paylaşımı yaptıklarını (genel katılımcılar arasında %22,2) belirtmektedir. Kullanıcılar günlük yaşantılarını, kişisel bilgilerini paylaşmasalar dahi beğendikleri içerikleri paylaşmaları onlar hakkında bir takım bilgiler sunmaktadır. Aşağıda özel yaşamın paylaşımına ilişkin iki farklı katılımcı türüne örnek verilmektedir.

K1: Paylaşımı daha az yapıyorum. Ama paylaşırsam kendi durumumu paylaşmayı tercih ederim. Kendi durumumdan kastım beğendiğim postu repost ediyorum. Gündemle ilgili bilgi paylaşıyorum o gün özel bir günse post paylaşıyorum ama kendi özel hayatımı hiçbir şekilde paylaşmıyorum (Erkek, 44, Lisans).

K7: Benim tüm sosyal hayatım orada. Hemen hemen her şeyim orada, insanlar istiyor ben de paylaşıyorum (Kadın, 30, Lisansüstü).

K2, K4, K6, K9, K13 önceden planlamadan beğendikleri içerikleri, kitapları, şarkıları, yerleri (%27,7 oranında) paylaşmaktadırlar. Kullanıcıların neleri paylaştıkları da gizlilik sınırlarını ortaya koymakta olup gizlilik önemleri arasında yer almaktadır.

K2: İçerik paylaşımım kısıtlı, güncel ve bilimle ilgili şeyler paylaşmayı tercih ederim (Erkek, 25, Lisansüstü).

K4: Çok beğendiğim kitabı paylaşıyorum. Başkaları da okusun diye paylaşırım. Bir de kendime anı oluşturmak istediğim anları paylaşırım. Örneğin tatilde bir yeri beğendiysem onu paylaşırım (Erkek, 36, Lisansüstü).

K6: Paylaşmıyorum ama beğeniyorum. Ciddi meseleler paylaşmıyorum bazen kitap, şarkı paylaşıyorum (Kadın, 26, Lisansüstü).

K9: Aslında tamamen o anki moduma bağlı yani paylaşımlarım spontane ilerliyor diyebilirim. Açıkçası bugün ne paylaşsam diye düşünmüyorum, her şey içimden geldiği gibi. Ama sanırım en çok benim için özel günlerden fotoğraflar paylaşıyorum (Kadın, 19, Lisans).

K13: Gündemde yer alan konuları, özel bir günse onu belirten paylaşımlar yapmayı tercih ediyorum (Erkek, 20, Lisans).

Sosyal Ağlardaki Gizlilik Kurallarına Yönelik Bakış Açılarına İlişkin Bulgular

Araştırma katılımcılarına sosyal ağlardaki gizlilik kurallarına bakış açılarını anlamaya yönelik olarak "Gizliliği nasıl tanımlarsınız?," "Sosyal ağların gizlilik kurallarını hiç okudunuz mu?," "Gizlilik kurallarının ne kadarını anladınız?," "Sosyal ağlardaki gizlilik ayarlarını kullandınız mı?," "Sosyal ağların sizin davranışlarınızı izlemesi konusunda ne düşünüyorsunuz?," "Sosyal ağların sizin hakkınızda sizden veri/bilgi topladığını bildiğinizde bu sizi etkiliyor mu? Nasıl etkiliyor? (Daha az bilgi paylaşımı, sosyal ağdan çıkma vb.)," "Sizin için gizliliğin genel olarak ne demek olduğunu açıklayabilir misiniz?" ve "Sosyal ağlarda gizlilik sizin için nedir?" soruları yöneltilmiştir.

Tüm katılımcılar, gizliliği farklı sözcüklerle ifade etseler de tanımlamaları, literatürde yer alan gizlilik tanımlarıyla örtüşmektedir. Westin (1967) gizliliği; bireyin kendisine dair bilgileri nasıl paylaşacağını belirlemesi Derlega ve Chaikin (1977, p. 1) bireyler arasındaki ilişkinin sınırlarının kontrolü olarak ifade etmektedir. Katılımcılarla yapılan görüşme sonucunda bir gizlilik tanımı ortaya çıkmıştır. Bu tanıma göre gizlilik; bireylerin kendi özelinde olan, yaşamıyla ilgili kendi istediği kadarını paylaşma gücü olarak ifade edilebilir. K8, K12, K14 tarafından gizliliği özetleyen tanımlamalar aşağıda yer almaktadır.

> K8: İzin verdiğim kadarının bilinmesi (Kadın, 26, Lisans).

> K12: Benim insanlarla paylaşmadığım her şey, kişinin kendisinde kalanlar (Kadın, 26, Lisans).

> K14: Kişisel bilgilerimi dış dünyayla sınırlı olarak paylaşma veya paylaşmama (Kadın, 38, Lisans).

Araştırmada katılımcıların %55,5'inin (K1, K2, K6, K7, K8, K10, K11, K13, K14, K16) gizlilik kurallarını okumadığı saptanmıştır. Bu durumu; kuralları okusalar dahi bir şey değişmeyeceğini, platformu kullanabilmek için şartları kabul etmek zorunda olduklarıyla açıklamaktadırlar. %11,2 oranında ise bazen okuduklarını ancak çok uzun olduğu için çoğunlukla okumadıklarını ifade etmektedirler. Katılımcıların %5,5'i ise okuduğunu ancak platformu kullanabilmek için izin vermek zorunda olduğunu ifade etmektedir.

> K7: Hiç okumadım. Zaten mikrofona, kameraya, her şeye izin veriyoruz (Kadın, 30, Lisansüstü).

> K9: Bazen okuyorum, okunması gerektiğini düşünüyorum fakat çoğunlukla okumuyorum çünkü çok uzun, zaman alıcı gibi geliyor. Bize ait verilerin ticari amaçlarla firmalarla paylaşılabileceğini anladım (Kadın, 19, Lisans).

> K12: Hiçbir zaman tam olarak okumadım. Çünkü gizlilik ayarlarımı en yüksekte tutsam bile verilerimin bir şekilde sosyal ağları yöneten kurumlar tarafından ulaşılabilir olacağına inanıyorum. Ama bu durum beni yine de Instagram veya diğer sosyal ağları kullanmaktan alıkoymuyor. Profilimi "yalnızca arkadaşlarım" seçeneğinde ayarlayarak en azından diğer tanımadığım kullanıcılara karşı kişisel bilgilerimi koruma altına alarak kendimi rahatlatıyorum. Facebook gizlilik ayarları

> Instagram'a göre daha karmaşık, sürekli yenileniyor. Bu yüzden Facebook'umdaki gizlilik ayarlarımı daha zor anlayabiliyorum, daha zor kontrol edebiliyorum (Kadın, 26, Lisans).

> K17: Telefonumda nelere ulaşabileceği konusunda kayıt olurken okudum. Telefonumdaki her şeye ulaşabileceğini anladım. Zorunluluktan izin verdim (Kadın, 27, Lisans).

Katılımcıların sosyal ağ platformları tarafından sunulan gizlilik ayarlarını kullandıkları görülmektedir. Bu bağlamda katılımcılar sosyal medya platformalarını kullanmak için gizlilik kurallarını kabul etme dışında bir seçenekleri olduklarını düşünmemektedirler. Ancak kendilerine göre gizliliklerini ve mahremiyetlerini korumak için sosyal medya hesaplarındaki gizlilik ayarlarını aktifleştirmekte ve bu alanda bir hassasiyet göstermektedirler. Katılımcıların %33,3'ü (K4, K7, K9, K14, K15, K17) profillerini sadece tanıdıklarına açık olarak kullanırken %11,2'si (K5, K12) kişi listelerindekilerle paylaştıkları içeriklere dair sınırlandırmada bulunduklarını belirtmektedir. Katılımcıların %11,2'si de (K2, K11) profillerinde kişisel bilgilerini de bulundurmamaktadırlar. Bu bağlamda sosyal medya kullanıcıları kendilerine ait güvenlik ayarları unsurları ile gizliliklerini korurken kendilerini daha güvende hissetmektedirler.

> K4: Ben sadece paylaşımlarımı arkadaşlarıma açık yapıyorum (Erkek, 36, Lisansüstü).

> K5: Instagram story'de close friends özelliğini kullanıyorum (Erkek, 25, Lisansüstü).

> K2: Tüm doğumgünü, okul, aile bilgisi gibi kişisel bilgileri sildim, başta vardı. Tüm ayarların üzerine Facebook'un reklamlarını kapatan güvenlik eklentileri kullanıyorum (Erkek, 25, Lisansüstü).

> K9: Facebook ve Instagram kullanıyorum. İkisinde de gizlilik ayarlarını aktif olarak kullanıyorum. Bunun benim için oldukça önemli olduğunu söyleyebilirim çünkü bana, özel yaşamıma ait fotoğraf veya herhangi bir bilgiyi tanımadığım kişilerin görmesi veya paylaşması fikrini hoş karşılamıyorum (Kadın, 19, Lisans).

Sosyal gizlilik, kişinin kimliğiyle ilgiliyken kurumsal gizlilik, kurum-birey arasındaki veri gizliliğidir (Raynes-Goldie, 2012, p. 81). Katılımcılar, özellikle kurumların sosyal medya üzerinden hareketlerini ve paylaşımlarını değerlendirirerek kişiselleştirilmiş

mesajlar iletmesi, markalardan gelen iletişim mesajlarına maruz kalınması gibi durumlardan rahatsızlık duyduklarını ifade etmişlerdir. Katılımcılar için gizlilik, sadece siber saldırı vb alanlarda değil kurumlardan gelen reklam içerikli iletişim mesajlarından da korunmak anlamına gelmektedir. K11, sosyal medya algoritmalarının benzer içerik önerme özelliğini vurgulamakta K13, verilerinin kullanılmasına şüpheyle yaklaşmaktadır. K15, reklam hedefleme açısındansa sosyal gizlilik açısından tedirgin olmaktadır. Katılımcılar, bilgilerini paylaşmaktan rahatsızlık duyarak bilgilerinin kötü niyetli üçüncü kişilerin eline geçebileceğini düşünmektedir.

> K11: Beğensem de beğendiğimi belli etmemek için beğendiye basmıyorum. Ben onu beğenince hep o tarz şeyler çıkaracağı için beğenmiyorum etkileşime girmiyorum (Kadın, 39, Lisans).

> K13: Etkiliyor. Kişisel bilgilerimin kullanılması ihtimali tedirgin ediyor. Elimden geldiğince bilgilerimi paylaşmamaya özen gösteriyorum (Erkek, 20, Lisans).

> K15: Toplanan veri veya bilgi tüketim alışkanlıkları vb durumlar alakalıysa sorun etmiyorum. Ama kişisel olarak benimle ilgili veri toplanacaksa bundan rahatsız olurum. O aşamada bilgi paylaşmam (Erkek, 32, Lisans).

Literatürde, sosyal medyada gizlilik kişinin kendi içeriklerinde yer alan bilgiler ve diğerlerinin içeriklerinde yer alan bilgiler olarak iki boyutta ele alınabilmektedir (Smith et al., 2012, p. 2). Katılımcılara sosyal ağlarda gizlilik kavramını nasıl tanımladıkları sorulmuş olup gizlilik kavramının dijitale taşınmış haliyle değerlendirdikleri anlaşılmaktadır. K1, K10, K13'ün yanıtlarında olduğu gibi kişinin kendisinin yönettiği bir süreç olarak ele alınabildiği gibi K3'ün yanıtında görüldüğü üzere gizlilik sınırının yalnızca kişinin kendisinin elinde olmadığı da düşünülmektedir. Bu bağlamda gizlilik sınırı farklı yönlerde değerlendirilse de katılımcıların %61,1'i gizliliği sosyal medya kullanıcılarının kendisi tarafından yönetilen bir süreç olarak değerlendirmektedir. %38,9'u ise gizlilik sınırının kendi idarelerinde olmadığını, sosyal medya platformlarının bilgi paylaşımına olanak tanıyan bir yapıda olduğunu belirtmektedir. Bu bağlamda dijital dünyada bilgiyi kişisel bilgiyi kullanıcı tarafından gizli tutabileceğini düşünen anlamlı bir katılımcı olduğu saptanmıştır.

> K1: İz bırakmamak demek. Kişisel bilgilerim, ailemin resimleri, telefonum benim için gizliliktir (Erkek, 44, Lisans).

K10: Sosyal medya bir şeyleri göstermekle ilgili. Hangi bölümü göstermek, ne kadar göstermek istiyorsun onunla ilgilidir (Kadın, 40, Lisansüstü).

K13: Kullandığın sosyal ağı tamamen kendi tercihine göre şekillendirmek. İsteğe bağlı olarak gizli hesap kullanmak gibi (Erkek, 20, Lisans).

K3: Gizlilik katmanlı bir durum. Örneğin biriyle yemeğe gidiyorum o paylaşmasa da ben paylaşınca o kişinin benim yanımda olduğu biliniyor. Bir paylaşımda kişinin yanındakini etiketleme sorunu da var. Ben paylaşmıyorum ama etiketleniyorum, etiketi kabul etmiyorum ama bu veriler o ağda kalıyor. Kimin nerede olduğu bilgisine sahip oluyor (Erkek, 27, Lisansüstü).

Gizlilik Yaklaşımlarına İlişkin Bulgular

Araştırma katılımcılarının gizlilik yaklaşımlarını belirlemek üzere "Kişisel verilerinizde, paylaşımlarınızda gizliliğe önem veriyor musunuz? Gizliliğinizin ihlal edilmesinden çekiniyor musunuz? Nasıl önlem alıyorsunuz alıyorsunuz?," "Siz kendinizi nasıl ifade edersiniz? (Tutucu, Faydacı, Umursamaz)," "Sosyal ağ platformlarındaki gizlilik politikalarındaki değişimler, eklenen yeni gizlilik ayarları kendinizi daha rahat hissetmenizi sağlıyor mu?," "Bilgilerinizi paylaşmaktan rahatsız olduğunuz, olmadığınız kurumlar hangileridir?" soruları yöneltilmiştir.

Literatürde kullanıcıların gizliliklerinin ihlal edilmesinden çekindikleri için daha az bilgi açıkladıkları bilgisi bulunmaktadır (Cavusoglu et al., 2013, p. 14). Tüm katılımcılar, kişisel bilgileri söz konusunda olduğunda paylaşımlarına yönelik otokontrol uygulamakta; paylaşımlarında nelerin yer aldığına dikkat ederek özellikle konum içeren paylaşımlar yapmamaktadırlar. Aşağıda K9, K12, K14, K15'in yanıtları örnek olarak verilmektedir.

K9: Tabii ki gizliliğe önem veriyorum, zaten olması gereken bu! Mesela paylaşımlarımı sadece benim izin verdiğim kişilerin görebileceği şekilde ayarlıyorum. Öncesinde ne paylaşacağıma, paylaşımımın hangi bilgileri içerdiğine çok dikkat ediyorum. Kesinlikle çekiniyorum. Bazı önlemler alıyorum. Herhangi bir bilgi verirken dikkatli olmak hatta bazen bilgi vermekten uzak durmak gibi (Kadın, 19, Lisans).

K12: Evet çekiniyorum. Bu yüzden eskiye göre daha az paylaşım yapmaya, gizlilik ayarlarını daha sık kontrol etmeye çalışıyorum (Kadın, 26, Lisans).

K14: Çok büyük çekincelerim yok. Buna yönelik çok önemli verilerim yok. Yine de anladığım kadarıyla profillerimi, bilgilerimi gizli tutuyorum (Kadın, 38, Lisans).

K15: Çok kişisel bilgi, yorum, bulunduğum konum, işimin detayları, yeri gibi paylaşımlardan kaçınmaya özen gösteriyorum (Erkek, 32, Lisans).

Gizlilik yaklaşımları kişisel geçmiş ve kişilik özelliklerine göre farklılaşmaktadır. Yapılan araştırma sonuçlarına göre katılımcıların %55,5'i (K1, K4, K5, K12, K13, K14, K15, K16, K17, K18) kendisini faydacı olarak tanımlamaktadır. Bununla birlikte kendisini tutucu olarak tanımlayan katılımcı oranı %11,2 (K9, K11)'dir. Bununla birlikte K2, K3, K6, K8 düşünce bakımından tutucu olsalar da davranışları söz konusu olduğunda faydacı ve umursamaz olarak nitelenebileceklerini çünkü gizlilik sorunlarına rağmen sosyal medya kullanmaya devam ettiklerini belirtmektedir. Bu bağlamda kişilik özellikleri, verdikleri kararlar, sosyal medya kullanım amaçları, bilgi paylaşma motivasyonları gibi değişkenler bireylerin gizlilik yaklaşımlarında kendilerini ifade ettikleri unsurlar olarak belirtilmektedir.

K7: Faydacıyla umursamaz arasındayım. Tam ikisi arasında bir yer varsa orada duruyorum. Akıllı telefonlar ve sosyal medyayla birlikte bilgilerin açığa çıkması anlamında pek çok şeyi kabul ediyoruz. Kaçınılmaz bir şey. İstediğimiz kadar kaçalım içindeyiz, tutuculuk bana kaçınılmaz olanı geciktirmek veya çatışmak gibi geliyor. Kötü olduğu kadar iyi yanları da var, tatile giderken güzel yerleri önceden keşfedip oralara gitmek daha önce sosyal medyada paylaşılan o deneyimlerden yararlanmak iyi oluyor gri bir alan aslında (Kadın, 30, Lisansüstü).

K5: Faydacı olabilir. Getirilerini kullanmayı seviyorum. Bazı uygulamalar var, eve gidince hatırlat gibi bana yarar sağlayan o faydaları kullanmak hoşuma gidiyor bunun için konumu açıyorum, etkinliği söylüyorum birçok bilgiyi veriyorum ama aynı zamanda günümü kolaylaştırıyor (Erkek, 25, Lisansüstü).

K9: Kendime en yakın seçeneğin "tutucu" olduğunu düşünüyorum. Çünkü; hangi koşullar karşısında olursa olsun kişisel verilerin depolanmasının, kullanılmasının asla yararlı olmayacağı taraftarıyım. Bu konularda endişe taşıdığımı söyleyebilirim (Kadın, 19, Lisans).

Katılımcıların sosyal ağ platformlarının gizlilik politikalarındaki ve ayarlarındaki değişikliklere yaklaşımları farklılık göstermektedir. Değişen güvenlik ayarları ve gizlilik

politikalarına olumlu bakılsa da hiçbir güncellemenin tam anlamıyla bir gizlilik sağlamayacağını düşünen katılımcılar da yer almaktadır. K1, K9, K13, K15 yeni gizlilik ayarlarının kendilerini daha güvende hissetmelerini sağladığını belirtmektedir. K12 ise her güncelleme ile ayarlarını kontrol etmek zorunda hissederken hiçbir güncellemenin tam gizlilik sağlayamayacağını düşünmektedir. K6, K7, K8, için gizlilik kurallarının ve ayarlarının anlamı bulunmamakta çünkü bu ayarların tam bir gizlilik sağlayamayacağını düşünmektedirler. Bu bağlamda katılımcıların %22,2'si sosyal medya platformlarındaki gizlilik ayarı güncellemelerinin kendilerini güvende hissettirdiğini belirterek olumlu olarak değerlendirirken; %87,8'i güncelleme olsa da olmasa da sosyal medya platformlarında gizlilik ayarlarının tam anlamıyla gizlilik sağlamadığı görüşündedir. Bu bağlamda bireylerin her ne kadar anlamlı bir çoğunlukla (%87,8) gizlilik ayarlarına güvenmeseler de yine de sosyal medya platformlarında varolmaya devam ettikleri ancak paylaşımlarını kendi gizlilik ayarlarına göre bireysel koruma ile sağladıkları saptanmıştır.

> K8: Bu postla verilerimi koruyorum diye bir ara kullanıcılar post girerek gerçekten böylece verilerinin korunduğunu zannetmişlerdi. Ne yaparsan yap koruyamayacağını bilmeyen bir kitle var aslında (Kadın, 26, Lisans).

> K6: Hiçbir etkisi yok öncesini bilmediğim için yeni güncellemeler beni etkilemiyor. Yazıyor ama ne demek olduğunu okusam da bilemiyorum. Bu beni rahatsız ediyor (Kadın, 26, Lisansüstü).

> K9: Kendimi daha rahat hissettiğimi söyleyebilirim. Özellikle gizlilik ayarlarının daha anlaşılır, açık ve kullanışlı olması, kullanıcılara ayarlar bölümünde daha fazla kontrol imkanı verilmesi beni memnun etti (Kadın, 19, Lisans).

İletişim Gizliliği Yönetimi Kuramı Ekseninde Bulgular

Araştırma katılımcılarına İletişim Gizliliği Yönetimi ekseninde "Kişisel bilgilerinizin ne kadarını sosyal ağlarda açıklıyorsunuz? (demografik özellikler, beğeniler, içinde bulunulan duruma bağlı paylaşım, bazı riskleri göze alarak fayda elde etmek amacıyla paylaşım gibi)," "Sizce dijital ortamdaki ve yüz yüze iletişimdeki gizlilik benzer mi? Sosyal medyada paylaşılan içeriklerde kişisel bilgilerin sahipliğinin size ait olduğunu düşünüyor musunuz? (Sosyal medya profillerinizin gizli veya herkese açık olması, platformdaki paylaşımlarınızı kimin göreceğini belirleyebilmeniz gibi)," "Gizliliğe önem verseniz de

bilgilerinizin ilgili platformların sunucularında depolanarak ortadan kaybolmayışı hakkında ne düşünüyorsunuz?" soruları yöneltilmiştir.

Katılımcılar, cinsiyet gibi demografik özelliklerini genellikle zorunlu hallerde paylaşmakta özellikle vurgulama gereği duymamaktadır. Yaptıkları paylaşımlarda müzik, kitap, film, dizi paylaşımlarına ağırlıklı olarak yer verilirken isteklerini, ihtiyaçlarını belirten paylaşımlar yapmayı çoğunlukla tercih etmemektedirler. K17'nin ifadesi, isteklerin paylaşmasına yönelik bir örnek olmaktadır.

> K17: Çalışırken keşke X yerinde olsam diye paylaşım yapıyorum o an mutsuzsam nerede mutlu olacağımla ilgili paylaşım yapıyorum (Kadın, 27, Lisans).

Gizlilik kurallarının etkenleri arasında koşullar ve risk-fayda etkeni bulunmaktadır (Petronio, 2002; Waters, & Ackerman, 2011, p. 104). Literatürde yer alan bilgilere göre çevrimiçi alışveriş yapan kullanıcılar, bilgilerini paylaşmakta ancak sınırlarının ihlal edileceğini düşünerek bu durumdan rahatsız olmaktadırlar (Metzger, 2007, p. 354). Katılımcıların %38,8'i için içinde bulunulan durumun, gündemin paylaşımları üzerinde bir etkisi olmazken katılımcıların %67,2 içinde bulundukları duruma, gündeme göre paylaşım yapmaktadır. Risk-fayda bakımından K1, K7, K10 çevrimiçi alışverişte kimlik bilgilerinin paylaşılması zorunluluğu gibi durumlarda bilgilerini paylaşmaktadır. Resmi kurumlar açısından bakıldığında kişisel bilgilerin hali hazırda devlet kurumlarında bulunması K12, K13, K15, K16, K17, K18 için rahatlatıcı olsa da K10'un da belirttiği gibi çevrimiçi bilgi paylaşımı sonucunda bilgilerinin üçüncü kişilerin eline geçebilmesi olasılığı nedeniyle çekinceyle yaklaşılmaktadır. Katılımcıların %38,8'i (K2, K3, K6, K8, K10, K11, K14) zorunda olmadıkları sürece bilgilerini paylaşmak istememekte bu bağlamda fayda sağlamak için riskleri göze almamaktadır. K9 ve K18 ise sadece tanıdıkları, bildikleri kurumlarla bilgi paylaşabileceklerini vurgulamaktadırlar. K4 ve K5 ise bilgi paylaşımına faydacı olarak yaklaşmakta ve bilgi paylaşmaktan rahatsız olmamaktadır. K7, beğenilme isteğiyle motive olarak yapılan paylaşımların, riskin göze alındığı şeklinde yorumlanabileceğini belirtmektedir.

> K1: Karşılığında nasıl bir fayda sağlarsam sağlayım gizliliğimi ortadan kaldırmak istemem. Adı üstünde kişisel bilgilerim olduğu için bu bilgilerimin başkasının eline geçmesi durumunda maddi veya manevi zarar görmek istemem (Erkek, 44, Lisans).

> K7:…Neden insan tek başına güzel bir fotoğrafını koyar? Birçok beğeni alıyor ve tekrarlanan davranış haline geliyor aslında (Kadın, 30, Lisansüstü).

Katılımcıların, sosyal medya platformlarında ürettikleri içerikleri sadece yakın arkadaşlarla paylaşma, kişisel bilgileri paylaşmama, sadece mevcut içeriği paylaşma vb kendi gizlilik tercihleri ile paylaşarak yüz yüze iletişimde olduğu gibi paylaşmak istedikleri konuları sınırlandırdıkları saptanmıştır. Dijital ortamdaki ve yüz yüze iletişimdeki gizliliğin benzer olduğunu ifade eden K9 ve K14 bu bağlamda yüz yüze iletişimde sınır çizdikleri gibi dijitalde de çizebildiklerini belirtmektedir. Buna göre bireyler yüz yüze olarak kiminle iletişim kuracaklarını, neler paylaşacaklarını belirledikleri gibi dijitalde de belirlemektedir. Yüz yüze iletişimle benzer olmadığını söyleyen K1, K4, K10, K12, K13, K18 dijitalde bireylerin kendilerini bambaşka bir biçimde tanıtabileceklerini; rol yapmalarının, yalan söylemelerinin daha kolay olması nedeniyle gizliliğin daha rahat sağlanabileceğini düşünmektedirler. Bu bağlamda katılımcıların%72,2'si , dijital ortamdaki ve yüz yüze iletişimdeki gizliliğin farklı olduğunu düşünmektedir.

> K9: Dijital ortamdaki gizlilikle yüz yüze iletişimdeki gizliliğin benzer olduğunu, sosyal medyada paylaştıklarımın sahipliğinin benim olduğunu düşünüyorum. Tıpkı yüz yüze iletişimde kiminle konuşup konuşmayacağıma veya ne kadar süre karşımdaki kişiyle iletişim kuracağıma karar verebiliyorsam bu hakkımı sosyal medyada da kullanıyorum. İstemediğim biriyle nasıl görüşmüyorsam aynı şekilde bu insanların sosyal medya profillerimi, paylaşımlarımı görmelerini de istemem (Kadın, 19, Lisans).

> K14: Benzer olduğunu düşünüyorum. Yüz yüze iletişimde de her zaman her şeyimizi paylaşmıyoruz veya karşı tarafın bilmesini istediğimiz kadar bilgi paylaşıyoruz. Bana ait olduğunu düşündüğüm özel bilgi veya içerik paylaşımlarını sosyal medyada yapmıyorum (Kadın, 38, Lisans).

> K13: Benzer değil. İnsanlar sosyal medyada kendilerini başka biri gibi tanıtabiliyorlar (Erkek, 20, Lisans).

TARTIŞMA VE SONUÇ

Sosyal medyanın gündelik yaşamda önemli bir yer edindiği yer bilinmektedir. Kullanıcıların ürettikleri içerikler açısından gizlilik, sosyal medyaya dair önemli bir

tartışma konusudur. Farklı alanlarda ve amaçlarla sosyal medya büyük verisinden yararlanılarak pek çok analiz yapılabilmektedir. Kullanıcıların sosyal medyada gizliliklerini yönetme biçimleri, gizliliğe ve büyük veriye bakışlarıyla ilişkilendirilmektedir. Bu çalışmada sosyal medya kullanıcılarının büyük veri ekseninde sosyal medyada gizliliğe bakışlarını anlamak amaçlanmaktadır. Bu amaçla 15.11.2019-09.12.2019 arasında 18 katılımcıyla derinlemesine görüşme tekniğiyle araştırma gerçekleştirilmiştir.

Araştırma sonucunda katılımcıların özellikle sosyal ağları kullandıkları ve temel amaçlarının iletişim ve haber alma olduğu saptanmıştır. Katılımcılar sosyal medyada özel yaşamları için bir sınır çekmek için çaba gösterseler de bazı katılımcıların sosyal medyada özel yaşamlarını açıkça paylaşmaktan çekinmediği görülmektedir. Bununla birlikte katılımcıların sosyal medyadaki güvenlik ayarlarına ya da rutin olarak güncelenen güvenlik ve gizlilik ayarlarına güvenmedikleri kendi gizlilik ayarlarını kendilerinin oluşturmak için bazı yollara başvurdukları saptanmıştır. Bu yollar arasında yaşadığı şehir, cinsiyet, çalıştığı kurum gibi kişisel bilgileri paylaşmamak, kendi içerik üretmeden varolan içerikleri paylaşmak yer almaktadır. Bir diğer yandan çoğunlukla sadece tanıdıklarına, arkadaşlarına açık hesaplar kullanarak da gizlilik sorunsalına bireysel çözümlerin üretildiği saptanmıştır. Bu durum da sosyal medya kullanıcısı katılımcıların paylaşımlarını güven hissiyle yapmalarına yardımcı olmaktadır. Paylaşımlarına sınırlar koyan katılımcılar okudukları kitapları, beğendikleri şarkıları paylaşma eğilimdedirler. Literatürde görüldüğü üzere gizlilik yönetimi açısından sosyal medya profillerine erişimin sınırlandırılması gizliliğin yönetilmesi açısından önemli bir öğedir (Debatin et al., 2009). Araştırmadan elde edilen bir diğer bulguya göre katılımcıların %55,5'i katıldıkları platformların gizlilik politikalarını okumamaktadır. Bu durumu; çok uzun olması, okusalar da platforma üye olmak için her şekilde kabul etmek zorunda oldukları, okusalar da anlamayacakları gibi nedenlerle açıklamaktadırlar. Literatüre bakıldığında kullanıcıların gizlilik politikalarını okuma eğilimlerinin düşük olduğu (Tuunainen et al., 2009) ancak paylaşım yapmaya devam ettikleri (Acquisti, & Gross, 2006) bilgisi bulunmaktadır. Bu doğrultuda araştırma bulgularının literatürle tutarlı olduğu anlaşılmaktadır.

Katılımcılar, sosyal ağ platformlarının gizlilik politikalarındaki ve ayarlarındaki değişikliklere birbirlerinden farklı yaklaşımlar göstermektedir. Katılımcıların %61,1'i gizliliğin sosyal medya platformlarında kullanıcı tarafından yönetilebilecek bir süreç olarak değerlendirmektedir. Bu bağlamda kullanıcılar, sosyal medya platformlarının sunduğu gizliliğe kendileri müdahale ederek kişisel gizlilik ayarlarını düzenlemektedir. Bu görüşe sahip olan katılımcıların, kendilerini gizliliklerinin düzenleyicisi ve yöneticisi

olarak gördükleri anlaşılmaktadır. Katılımcı görüşlerinden elde edilen ortak gizlilik tanımına göre gizlilik, bireyin kendi izin verdiği kadarının bilinmesiyken sosyal medyada ve dijital dünyada da katılımcıların bilgiyi gizli tutabileceğine yönelik inancı olduğu görüşüne varılmıştır. Literatürde de benzer bulgular yer almakta olup gizlilik yönetimi çerçevesinde bireylerin kendi sınırlarını çizebildiği ve çizilen sınırların, kişisel bilgilerin koruyucusu olarak yüz yüze iletişimdeki ve dijital iletişimdeki gizliliğin, benzer süreçler olduğu ifade edilmektedir (Griffins, 2011; Metzger, 2007; Child, & Petronio, 2011).

Katılımcıların %38,9'u ise yüz yüze iletişimdeki gizlilik ile dijitaldeki gizliliğin farklı olduğunu ifade etmektedir. İlgili katılımcılara göre yüz yüze iletişimden farklı olarak dijital dünyada farklı davranma eğilimi ve imkanı gibi sebeplerle daha kolay gizlilik sağlanabileceği de belirtilmiştir. Katılımcılar sosyal medyada rol yapmanın daha kolay olması nedeniyle daha kolay gizlilik sağlayabileceğini belirtmektedir. Ancak bu durum, gizliliğin bireyler arasındaki boyutu olan sosyal gizliliğin daha kolay olabileceğini göstermektedir. Anlaşıldığı üzere hem yüz yüze iletişimdeki ve dijitaldeki gizliliğin benzer olduğunu hem de farklı olduğunu ifade edilen katılımcılar gizlilik yönetimi söz konusu olduğunda kullanıcıları etkin olarak görmektedir. Bir diğer yandan katılımcıların mümkün olduğunca az bilgi paylaşarak sosyal medyada yer almaları dikkat çekici bulgulardan birisidir. Kullanıcılar her ne kadar gizliliklerini yönetseler de platformlarda bulunan bilgilerinin 3. tarafların eline geçerek kötü amaçlarla kullanılmasından tedirgin olduklarını belirtmektedirler. Gizliliklerinin ihlal edilmesinden çekinen kullanıcılar, daha az bilgi açıkladıklarını, daha az içerik ürettiklerini belirtmektedirler. Bu durum literatürde yer alan gizliliklerinin ihlal edilmesinden çekinen sosyal medya kullanıcılarının daha az bilgi açıklama eğilimde oldukları (Cavusoglu et al., 2013) bilgisi ile tutarlıdır. Takip teknolojilerinin ve reklam hedefleme faaliyetlerinin farkında olan kullanıcılar bu bağlamda sosyal medya büyük verisinin de farkındadır. Özellikle markalardan gelen mesajlarda ve iletişim çalışmalarından sıklıkla karşılarına çıkması sosyal medyada hareketlerinin takip edildiği hissi oluşturmakta ve bu mesajlara yönelik olumsuz duygular oluşmasına sebep olmaktadır.

Ayrıca gizlilik yaklaşımlarına göre katılımcıların %55,5'i kendilerini faydacı olarak betimlemişlerdir. Araştırmadan elde edilen diğer bulgularla birlikte değerlendirildiğinde katılımcıları gizliliklerine önem vererek gizliliklerini yönetmek istemektedirler. Verilerinin paylaşılmasından rahatsız olmaktadırlar. Bununla birlikte araştırma katılımcılarının, sosyal medya platformlarından belli bir fayda sağladıkları bu nedenle de platformlarda varlıklarını sürdürme yolunda eğilim gösterdikleri saptanmıştır. Bu bulgular, literatürde

yer alan bilgilerle de tutarlılık göstermektedir. Buna göre bireylerin, sosyal ağlarda gönüllü olarak yer aldıkları ifade edilmekte (Acquisti, & Gross, 2006, p.1) bireylerin amaçlarına ne kadar ulaştıkları, sağladıkları fayda (Chennamaneni, & Taneja, 2015, p. 7) ve bu durumun ne kadar risk yarattığı (Garg, Benton, & Camp, 2014) bu süreçte önem taşımaktadır. Bu anlamda bireylerin sosyal medyadaki varlıkları, paylaşımları, gizliliklerini nasıl yönettikleri algılanan fayda ve algılanan risk önem taşımaktadır.

Sonuç olarak araştırma katılımcılarının; gizlilik politikalarını okumadan mecburen onayladıkları, paylaşım yaparken tedirgin oldukları ancak gizlilik ayarlarını kullanarak veya otokontrol uygulayarak önlemler aldıkları, diğer kullanıcıların erişiminin yanı sıra depolanan verilerine üçüncü tarafların erişerek kötüye kullanmalarından tedirgin oldukları görülmektedir. Bu bağlamda sosyal medya kullanıcıları, sosyal büyük verinin farkında olup bundan tedirgin olsalar da sosyal medya platformlarını kullanmak istedikleri için birer kullanıcı olarak alabileceklerini düşündükleri önlemleri almaları dışında ellerinden bir şey gelmeyeceğini belirtmektedirler.

Bu çalışmanın alana, bireylerin sosyal medya büyük verisi ekseninde sosyal medyada gizliliğe bakışlarının anlaşılması açısından temel düzeyde katkı sağlayacağı düşünülmektedir. Gelecek çalışmalarda katmanlı olarak odak grup ve anket tekniklerinden yararlanılarak farklı veriler elde edilebileceği düşünülmektedir. Ayrıca gerek araştırma katılımcılarından elde edilen bilgiler gerek literatürde yer alan bilgiler ışığında bireylerin algılanan fayda ve algılanan risk ekseninde sosyal medyada gizlilik yönetimlerinin ve büyük veriye yaklaşımlarının araştırılması önerilmektedir. Böylelikle sosyal medya kullanıcılarının büyük veriye yaklaşımları üzerinde daha fazla bilgi sahibi olunabileceği öngörülmektedir. Araştırma katılımcılarının da belirttiği üzere sosyal medyada bireyler, kendilerini olduklarından farklı kişiler olarak tanıtabilmektedirler. Bu durum beraberinde gizlilik riskleri de taşıyabilmektedirler. Gerçek kişiler adına açılan sahte hesaplar, anonim hesaplar da sosyal medyada gizlilik ekseninde incelenebilecek konular olarak önerilmektedir.

Hakem Değerlendirmesi: Dış bağımsız.
Çıkar Çatışması: Yazarlar çıkar çatışması bildirmemiştir.
Finansal Destek: Yazarlar bu çalışma için finansal destek almadığını beyan etmiştir.

Peer-review: Externally peer-reviewed.
Conflict of Interest: The authors has no conflict of interest to declare.
Grant Support: The authors declared that this study has received no financial support.

KAYNAKLAR

Aktan, E. (2018). Büyük veri: Uygulama alanları, analitiği ve güvenlik boyutu. *Bilgi Yönetimi Dergisi, 1*(1), 1-22.

Ashworth, L., & Free, C. (2006). Marketing dataveillance and digital privacy: Using theories of justice to understand consumers' online privacy concerns. *Journal of Business Ethics*, *67*, 107-123.

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

Aquisti, A., & Gross, R. (2006). Imagined communities: Awareness, information sharing, and privacy on the Facebook. *Privacy Enhancing Technologies Workshop Pre-proceedings* (pp. 1-16).

Belle, A., Thiagarajan, R., Soroushmehr, S. M. R., Navidi, F., Beard, A. D., & Najarian, K. (2015). Big data analytics in healthcare. *Biomed Research International*, 1-16. https://doi.org/10.1155/2015/370194

Bello-Orgaz, G., Jung, J. J., & Camacho, D. (2016). Social big data: Recent achievements and challenges. *Information Fusion, 28*, 45-59.

boyd, d. m., & Ellison, N.B. (2007). Social network sites: Definition, history, and scholarship. *Journal of Computer-Mediated Communication*, *13*(1), 210-230. https://doi.org/10.1111/j.1083-6101.2007.00393.x

boyd, D., & Crawford, K. (2014). Critical questions for big data. *Information, Communication & Society, 15*(5), 662-679.

Burgoon, J.K. (1982). Privacy and communication. In M. Burgoon (Ed.), *Communication Yearbook 6* (pp. 206-249). CA, USA: Sage.

Cavusoglu, H., Phan, T., & Cavusoglu, H. (2013). Privacy controls and content sharing patterns of social network users: A natural experiment. *ICIS 2013 Proceedings*.

Chennamaneni, A., & Taneja, A. (2015). Communication privacy management and self-disclosure on social media – A case of Facebook. *Proceedings of the 21st Americas Conference on Information Systems* (pp. 1-11).

Child, J.T., & Petronio, S. (2011). Unpacking the paradoxes of privacy in CMC relationships: The challenges of blogging and relational communication on the internet. In K. B. Wright, & L. M. Webb (Eds.), *Computer-Mediated Communication in Personal Relationships* (pp. 21-40) NY, USA: Peter Lang.

Couldry, N., & Turow, J. (2014). Advertising, big data and the clearance of the public realm: Marketers' new approaches to the content subsid. *International Journal of Communication, 8,* 1710-1726.

Cox, M., & Ellsworth, D. (1997). Application-controlled demand paging for out-of-core visualization. *Proceedings of the 8th Conference on Visualization'97*, Phoenix, USA, (pp. 235-244).

Cyganek, B., Graña, M., Krawczyk, B., Kasprzak, A., Porwik, P., Walkowiak, K., & Woźniak, M. (2016). A survey of big data issues in electronic health record analysis. *Applied Artificial Intelligence*, *30*(6), 497-520.

Çoban, B. (2014). Göz ve İktidar: "Vitrinlere Değil Gökyüzüne Bak!" *LAÜ Sosyal Bilimler Dergisi*, *5*(1), 1-15.

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

De Prato, G. & Simon, J.P. (2015). The next wave: "big data"? *Digiworld Economic Journal, 97*(1), 15-39.

Dienlin, T., & Trepte, S. (2014). Is the privacy paradox a relic of the past? an in-depth analysis of privacy attitudes and privacy behaviors. *European Journal of Social Psychology, 45*(3), 285-297. https://doi.org/10.1002/ejsp.2049

Digital in 2019. (2019). *We are Social*. Retrieved from https://wearesocial.com/global-digital-report-2019

Durham, W.T. (2008). The rules-based process of revealing/concealing the family planning decisions of voluntarily child-free couples: A communication privacy management perspective,*Communication Studies, 59*(2), 132-147. https://doi.org/10.1080/10510970802062451

Drennan, J., Mort, G.S., & Previte, J. (2006). Privacy, risk perception, and expert online behaviour: An exploratory study of household end users. *Journal of Organizational and End User Computing, 18*(1), 1-22.

Ergen, Y. (2018). Büyük veri, sosyal medya ve etik: Facebook örneğinde bir değerlendirme. *Yeni Düşünceler*, *10*, 53-64.

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.

Foucault, M. (1995). *Discipline and Punish: The Birth of the Prison*. USA: Penguin Books.

Fuchs, C. (2011). An alternative view of privacy on Facebook. *Information*, *2*, 140-165.

Gahi, Y., Guennoun, M., & Mouftah, H.T. (2016). Big data analytics: Security and privacy challenges. *2016 IEEE Symposium on Computers and Communication (ISCC)*, Messina, Italy (pp. 952-957).

Garg, V., Benton, K., & Camp, L.J. (2014). The privacy paradox: a Facebook case study. *2014 TPRC conference.*

Griffin, E. (2011). *A first look at communication theory*. New York, USA: The McGraw-Hill.

Guellil, I., & Boukhalfa, K. (2015). Social big data mining: A survey focused on opinion mining and sentiments analysis. *12th International Symposium on Programming and Systems*, ISPS 2015 (pp. 132–141). https://doi.org/10.1109/ISPS.2015.7244976.

Hekimoğlu, H. (2019). *Sosyal Ağlarda Mahremiyetin Dönüşümü: Instagram Örneği* (MA Thesis, Erciyes University, Institute of Social Sciences).

Jin, S.-A.A. (2013). Peeling back the multiple layers of Twitter's private disclosure onion: The roles of virtual identity discrepancy and personality traits in communication privacy management on Twitter. *New Media & Society*, *15*(6), 813-833. https://doi.org/10.1177/1461444812471814

Joinson, A.N., & Paine, C.B. (2007). Self-disclosure, privacy and the internet. In A. N. Joinson, K. Y. A. McKenna, T. Postmes, & U. Reips (Eds.), *The Oxford Handbook of Internet Psychology* (pp. 237-252). UK: Oxford University Press.

Joinson, A.N., Houghton, D. J., Vasalou, A., & Marder, B.L. (2011). Digital crowding: Privacy, self-disclosure and technology. In S. Trepte, & L. Reinecke (Eds.), *Privacy Online. Perspectives on Privacy and Self-Disclosure in the Social Web* (pp. 31-44). New York, USA: Springer.

Kemper, E. A., & Stringfield, S. (2003). Mixed methods sampling strategies in social science research. In A. Tashakkori, C. Teddlie, & C. B. Teddlie (Eds.), *Handbook of Mixed Methods in Social & Behavioral Research* (pp. 273-296) USA: Sage Publications.

Laney, D. (2001). 3D data management: Controlling data volume, velocity and variety. *META Group Research Note*, *6*.

LinkedIn Gizlilik Politikası. (2019). *Linkedin*. Retrieved from https://www.linkedin.com/legal/privacy-policy#share

Lynn, T., Healy, P., Kilroy, S., Hunt, G., van der Werff, L., Venkatagiri, S., & Morrison, J. (2015). Towards a general research framework for social media research using big data. *2015 IEEE International Professional Communication Conference (IPCC)* (pp. 1-8). https://doi.org/10.1109/ipcc.2015.7235843

Lyon, D. (2001). *Surveillance Society: Monitoring Everday Life.* UK: McGraw-Hill Education.

Mahrt, M., & Scharkow, M. (2013). The value of big data in digital media research. *Journal of Broadcasting & Electronic Media, 57*(1), 20-33. https://doi.org/10.1080/08838151.2012.761700

Mayer-Schönberger, V., & Cukier, K.(2013). *Big Data: A Revolution That Will Transform How We Live, Work, And Think*. USA: Houghton Mifflin Harcourt.

Metzger, M. J. (2007). Communication privacy management in electronic commerce. *Journal of Computer Mediated Communication, 12*(2), 335-361. https://doi.org/10.1111/j.1083-6101.2007.00328.x

Miles, M. B., & Huberman, A. M. (1994). *Qualitative Data Analysis: An Expanded Sourcebook*. California, USA: SAGE.

Mitrou, L., Kandias, M., Stavrou, V., & Gritzalis, D. (2014). Social media profiling: a panopticon or omniopticon tool? *Proceedings of the 6th Conference of the Surveillance Studies Network*.

Nguyen, M., Bin, Y.S., & Campbell, A.(2012). Comparing online and offline selfdisclosure: A systematic review, *Cyberpsychology, Behavior and Social Networking, 15*(2), 103-111.

Nippert-Eng, C. (2010). *Islands of Privacy*. Chicago, IL :University of Chicago Press.

Nissenbaum, H. (2009). *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. California, USA: Stanford University Press.

Onifade, O., Olomu, M., Ajao, B.F., Atoyebi, M., & Ilevbare, O. (2018). Social media users perception on privacy issues in a Nigerian university. *Journal of Digital Innovations & Contemporary Research in Science, Engineering & Technology, 6*(2), 35-46.

Öz, M. (2014). Sosyal medya kullanımı ve mahremiyet algısı: Facebook kullanıcılarının mahremiyet endişeleri ve farkındalıkları. *Journal of Yasar University, 9*(35), 6099-6260.

Pan, Y., & Zinkhan, G.M. (2006). Exploring the impact of online privacy disclosures on consumer trust. *Journal of Retailing*, *82*(4), 331-338. https://doi.org/10.1016/j.jretai.2006.08.006

Petronio, S. (1991). Communication boundary management: A theoretical model of managing disclosure of private information between marital couples. *Communication Theory*, *1*, 311-335.

Petronio, S., & Kovach, S.(1997). Managing privacy boundaries: Health providers' perceptions of resident care in scottish nursing homes. *Journal of Applied Communication Research, 25*(2),115-131. https://doi.org/10.1080/00909889709365470

Petronio, S. (2002). *Boundaries of Privacy.* USA: SUNY Press.

Pridmore, J., & Zwick, D. (2011). Editorial: Marketing and the rise of commercial consumer surveillance. *Surveillance & Society*, *8*(3), 269-277.

Raynes-Goldie, K. S. (2012). *Privacy in the Age of Facebook: Disclosure, Architecture, Consequences* (Doctoral dissertation, Curtin University Faculty of Humanities Department of Internet Studies). Retrived from https://pdfs.semanticscholar.org/466a/3ae1c8c43cdb583089cba198db04b01a4527.pdf

Sang, L. (2015). *Social Big Data and Privacy Awareness* (MA Thesis, Uppsala University Department of Informatics and Media Information Systems). Retrieved from https://www.diva-portal.org/smash/get/diva2:783517/FULLTEXT01.pdf

Scott, J. D. (2017). Social media and government surveillance: The case fot better privacy protections for our newest public space. *Journal of Business & Technology Law, 12*(2), 151-164.

Shozi, N.A., & Mtsweni, J. (2017). Big data privacy in social media sites. *IST Africa Conference Proceedings* (pp. 1-9).

Smith, M., Szongott, C., Henne, B., & von Voigt, G. (2012). Big data privacy issues in public social media. *6th IEEE International Conference on Digital Ecosystems & Technologies* (pp. 1-6). https://doi.org/10.1109/dest.2012.6227909

Snapchat Gizlilik Politikası. (2019). *Snapchat*. Retrieved from https://www.snap.com/tr-TR/privacy/privacy-policy

Stieglitz, S., Mirbabaie, M., Ross, B., & Neuberger, C. (2018). Social Media analytics–Challenges in topic discovery, data collection, and data preparation. *International Journal of Information Management*, *39*, 156-168.

Şimşek, T. (2019). Sosyal medyada mahremiyetin ifşası "Instagram örneği." *Sosyolojik Düşün, 4*(1), 10-24.

Tang, J., Chang, Y., & Liu, H. (2014). Mining social media with social theories: A survey. *SIGKDD Explor. Newsl., 15*(2), 20–29.

Tekin, H.H. (2006). Nitel araştırma yönteminin bir veri toplama tekniği olarak derinlemesine görüşme. *İstanbul Üniversitesi Sosyoloji Dergisi, 3*(13), 101-116.

Tosun, L. (2012). Motives for Facebook use and expressing "true self" on the internet. *Computers in Human Behavior*, *28*(4), 1510-1517.

Tufekci, Z. (2014). Big questions for social media big data: Representativeness, validity and other methodological pitfalls. *Proceedings of the 8th AAAI Conference on Weblogs and Social Media* (pp. 505-514).

Tuunainen, V.K., Pitkanen, O., & Hovi, M. (2009). Users' awareness of privacy on online social networking sites – Case Facebook. *22nd Bled eConference Enablement: Facilitating an Open, Effective and Representative eSociety*, June 14-17, Bled, Slovenia.

Twitter Privacy Policy. (2019). *Twitter*. Retrieved from https://twitter.com/en/privacy#update

Utma, S. (2018). Mahremiyet olgusu ve sosyal medyada mahremiyetin serüveni. *Uluslararası Sosyal Araştırmalar Dergisi, 11*(59), 1193-1204.

Van Dijk, J. (2016). *Ağ Toplumu.* İstanbul, Turkey: Kafka-Epsilon Yayıncılık.

Veri İlkesi. (2019). *Facebook*. Retrieved from https://tr-tr.facebook.com/privacy/explanation

Waters, S., & Ackerman, J. (2011). Exploring privacy management on Facebook: Motivations and perceived consequences of voluntary disclosure. *Journal of Computer-Mediated Communication, 17*(1), 101–115. https://doi.org/10.1111/j.1083-6101.2011.01559.x

Westin, A. (1967). *Privacy and Freedom*. New York, USA: Atheneum.

Westin, A. F. (2003). Social and political dimensions of privacy. *Journal of Social Issues, 59*(2), 431-453.

White, M. (2012). Digital workplaces: Vision and reality. *Business Information Review*, *29*(4), 205-214.

Whiting, A., & Williams, D. (2013). Why people use social media: A uses and gratifications approach. *Qualitative Market Research: an International Journal, 16*(4), 362-369.

Xu, Z., Liu, Y., Yen, N., Mei, L., Luo, X., Wei, X., & Hu, C. (2016). Crowdsourcing based description of urban emergency events using social media big data. *IEEE Transactions on Cloud Computing*, (pp. 1–1). https://doi.org/10.1109/tcc.2016.2517638

Zengin, M., Zengin, G., Altunbaş, H. (2015). Sosyal medya ve değişen mahremiyet "Facebook mahremiyeti." *Gümüşhane Üniversitesi İletişim Fakültesi Elektronik Dergisi, 3*(2), 112-136.

Zimmer, M., Kumar, P., Vitak, J., Liao, Y., & Kritikos, K. (2018). 'There's nothing really they can do with this information': unpacking how users manage privacy boundaries for personal fitness information. *Information, Communication & Society*, https://doi.org/10.1080/1369118X.2018.1543442

TABLOLAR VE ŞEKİLLER

Tablo 1: Katılımcılarla İlgili Bilgiler

	Cinsiyet	Yaş	Eğitim	Kullanım sıklığı
K1	Erkek	44	Lisans	Günde 1'den fazla
K2	Erkek	25	Lisansüstü	Günde 1'den fazla
K3	Erkek	27	Lisansüstü	Günde 1'den fazla
K4	Erkek	36	Lisansüstü	Günde 1'den fazla
K5	Erkek	25	Lisansüstü	Günde 1'den fazla
K6	Kadın	26	Lisansüstü	Günde 1'den fazla
K7	Kadın	30	Lisansüstü	Günde 1'den fazla
K8	Kadın	26	Lisans	Günde 1'den fazla
K9	Kadın	19	Lisans	Günde 1'den fazla
K10	Kadın	40	Lisansüstü	Günde 1'den fazla
K11	Kadın	39	Lisans	Günde 1'den fazla
K12	Kadın	26	Lisans	Günde 1'den fazla
K13	Erkek	20	Lisans	Günde 1'den fazla
K14	Kadın	38	Lisans	Günde 1'den fazla
K15	Erkek	32	Lisans	Günde 1'den fazla
K16	Kadın	26	Lisans	Günde 1'den fazla
K17	Kadın	27	Lisans	Günde 1'den fazla
K18	Erkek	31	Lisans	Günde 1'den fazla