T.C.
İSTANBUL TİCARET ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ
MEDYA VE İLETİŞİM ÇALIŞMALARI ANABİLİM DALI
MEDYA VE İLETİŞİM ÇALIŞMALARI YÜKSEK LİSANS PROGRAMI

DİJİTAL ÇAĞDA GÖZETİM VE SOSYAL MEDYA MAHREMİYETİ: KAZAKİSTAN ÖRNEĞİ

Yüksek Lisans Tezi

Ruslan BEGEN

İSTANBUL, 2025

T.C.
İSTANBUL TİCARET ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ
MEDYA VE İLETİŞİM ÇALIŞMALARI ANABİLİM DALI
MEDYA VE İLETİŞİM ÇALIŞMALARI YÜKSEK LİSANS PROGRAMI

DİJİTAL ÇAĞDA GÖZETİM VE SOSYAL MEDYA MAHREMİYETİ: KAZAKİSTAN ÖRNEĞİ

Yüksek Lisans Tezi

Ruslan BEGEN

Y23TMIL001

Danışman: Prof. Dr. Abdulhamit AVŞAR

İSTANBUL, 2025

ETİK BEYAN SAYFASI

Hazırlamış olduğum bu tez, YÖK ile İstanbul Ticaret Üniversitesi Lisansüstü Yönetmeliklerine uygun şekilde hazırlanmıştır. Çalışmam sırasında bilimsel etik kurallarına tam olarak uyduğumu; faydalandığım tüm kaynakları eksiksiz şekilde belirttiğimi ve herhangi bir kaynaktan ayrıntılı alıntı yapmadığımı beyan ederim. Tezde yer alan görüşler tamamen şahsıma ait olup, İstanbul Ticaret Üniversitesi'nin resmi görüşünü temsil etmemektedir.

Ruslan BEGEN

ÖZET

Gözetim olgusu, toplumsal denetim mekanizmalarının tarihsel gelişimi çerisinde uzun bir geçmişe sahip olup, modern devlet aygıtlarının gelişimiyle birlikte kurumsallaşmış bir yapıya kavuşmuştur. Bu çalışma, gözetimin tarihsel gelişim çizgisini takip ederek, özellikle dijitalleşme ile birlikte gözetim pratiklerinin biçimsel ve işlevsel olarak nasıl dönüşüme uğradığını incelemektedir. Çalışmada, postmodern toplum yapısı çerçevesinde dijital gözetimin sıradanlaşan, içselleştirilen ve bireylerin gündelik yaşam pratiklerine nüfuz eden bir yapıya evrildiği ortaya konulmaktadır. Bu çerçevede, dijital dönemin temel dinamiklerinden biri olan yeni medya teknolojileri, özellikle de sosyal medya platformları, bireylerin mahremiyet anlayışlarını şekillendiren temel unsurlar arasında değerlendirilmektedir. Sosyal medyanın bireyin öznel alanı ile kamusal alan arasındaki sınırları belirsizleştirdiği, bireylerin mahrem bilgilerini rıza göstererek gönüllü biçimde paylaşma eğilimini artırdığı tespit edilmiştir. Bu bağlamda çalışma, sosyal medyanın bireysel mahremiyetin sınırlarını nasıl yeniden tanımladığına dair eleştirel bir değerlendirme sunmaktadır. Ayrıca tez kapsamında, Kazakistan Cumhuriyeti'nde dijital gözetimin kurumsal boyutunu temsil eden "eGov" elektronik hükümet portalı detaylı bir biçimde ele alınmıştır. Bundan 19 yıl önce Kazakistan'da başlatılan (2006) eGov.kz – E-devlet Portalı, kamu hizmetlerinin kullanılabilirliğini sağlamak için ücretsiz bir elektronik dijital imza (e-İmza) kullanılarak vatandaşlara çevrimiçi formatta hizmet vermektedir. e-Hükümet (eGov) uygulamalarının genel işleyişine, kullanıcı etkileşimine, kamu hizmetlerine erişimi kolaylaştırıcı etkilerine ve platformun başarısına ilişkin veriler değerlendirilmiştir. Kazakistan örneği üzerinden dijital devletleşme süreci analiz edilerek, dijital gözetim ile kamu hizmetlerinin dijitalleşmesi arasındaki ilişki kuramsal ve uygulamalı düzeyde tartışılmıştır. Bu tez, dijital gözetim olgusunu hem bireysel mahremiyet bağlamında hem de devlet-birey ilişkileri düzleminde analiz ederek, dijitalleşen dünyada gözetimin görünmezleşen ama etkisi artan doğasına ışık tutmayı hedeflemektedir.

Anahtar Kelimeler: Dijital Çağ, Gözetim, Panoptikon, Sosyal Medya, Mahremiyet

ABSTRACT

The concept of surveillance, which has historically functioned as a mechanism of social regulation, has progressively institutionalized in parallel with the emergence of modern state apparatuses. This study traces the historical trajectory of surveillance and investigates how its practices have been transformed – both formally and functionally – within the context of digitalization. The findings reveal that, in the postmodern social context, digital surveillance has become normalized, internalized, and embedded into individuals' everyday behaviors and routines. In this context, new media technologies – especially social media platforms – are analyzed as key instruments reshaping individual perceptions of privacy. Social media is shown to blur the boundaries between the private and public spheres, increasingly encouraging individuals to voluntarily share personal and intimate information. The study offers a critical assessment of how social media redefines the limits of personal privacy and influences voluntary exposure in digital spaces. Furthermore, the research provides a detailed examination of Kazakhstan's "eGov" electronic government portal, which represents the institutional dimension of digital surveillance in the country. Launched in 2006, the eGov.kz portal has provided citizens with online access to public services using a free electronic digital signature (e-signature), designed to enhance service accessibility. The functioning of e-government services, user interaction, improvements in access to public services, and the overall effectiveness of the platform are explored. By analyzing the Kazakhstani experience, the study establishes a theoretical and practical link between digital surveillance and the digitalization of public administration. This study aims to shed light on the increasingly invisible yet pervasive nature of surveillance in the digital age by analyzing it through the dual lens of personal privacy and state–individual relations in the context of emerging communication technologies and digital governance systems.

Keywords: Digital Age, Surveillance, Panopticon, Social Media, Privacy.

ÖNSÖZ

Günümüzde dijital teknolojilerin hayatın her alanına nüfuz etmesiyle birlikte bireylerin mahremiyet algısı ve sınırları önemli ölçüde değişime uğramaktadır. Özellikle sosyal medya platformlarının yaygın kullanımı, bireylerin kendilerini ifade etme biçimlerini dönüştürürken beraberinde kişisel verilerin ve özel hayatın görünürlüğünü artırmakta; bu durum, dijital gözetim olgusunu daha da derinleştirmektedir. Dijital çağda gözetimin bireysel mahremiyet üzerindeki etkilerini anlamak, bu sürecin toplumsal sonuçlarını irdelemek, hem akademik hem de toplumsal açıdan önem taşımaktadır.

Bu yüksek lisans tezi, Kazakistan'da yükseköğretim mezun ve öğrencilerin (lisans, yüksek lisans ve doktora) sosyal medya platformlarında gözetim altında olup olmadıklarını ve özel yaşamlarına dair paylaşımlar yaparken mahremiyetlerine ilişkin bir kaygı taşıyıp taşımadıklarını incelemeyi amaçlamaktadır. Mahremiyetin dijital ortamlarda nasıl şekillendiğini anlamak, bireylerin bu yeni düzene nasıl uyum sağladıklarını ortaya koymak bu çalışmanın temel hedefleri arasındadır.

Tez süreci boyunca bilgi ve yönlendirmeleriyle bana her aşamada yol gösteren, desteğini esirgemeyen kıymetli tez danışmanım Prof. Dr. Abdulhamit AVŞAR'a, jüri üyeleri değerli hocalarım Doç. Dr. Berk ÇAYCI ve Doç. Dr. Kenan DUMAN ile çalışmalarım sırasında desteğini esirgemeyen Doç. Dr. Nihal Kocabay ŞENER'e en içten teşekkürlerimi sunarım. Ayrıca bu süreçte beni her zaman destekleyen aileme, eşime, değerli arkadaşlarıma ve görüşme sürecine katkıda bulunan katılımcılara da şükranlarımı sunarım.

Bu çalışmanın, dijital mahremiyet ve gözetim konularında yapılacak olan akademik araştırmalara katkı sağlamasını ve bu alandaki farkındalığın artmasına vesile olmasını diliyorum.

İstanbul - 2025

Ruslan BEGEN

İÇİNDEKİLER

Sayfa No.

ETİK BEYAN SAYFASI ii
ÖZET iii
ABSTRACT iv
ÖNSÖZ v
İÇİNDEKİLER vi
TABLOLAR LİSTESİ viii
ŞEKİLLER LİSTESİ ix
KISALTMALAR x
GİRİŞ 1

BİRİNCİ BÖLÜM

1. GÖZETİM KAVRAMI, GÖZETİM TOPLUMU VE GÖZETİM MODELLERİ

1.1. Gözetim Kavramı 3
1.1.1. Gözetim Toplumu 6
1.2. Gözetim Modelleri 10
1.2.1. Panoptikon 10
1.2.1.1 Süper-panoptikon 13
1.2.2. Sinoptikon 14
1.2.3. Omniptikon / Ban-optikon 15

İKİNCİ BÖLÜM

2. SOSYAL MEDYA VE MAHREMİYET YÖNELİMLERİ

2.1. Sosyal Medya Kavramına Genel Bakış 17
2.2. Sosyal Ağlar 18
2.3. Tarihsel Düzlemde Mahremiyet Kavramı 30
2.4. Geleneksel Mahremiyetin Dönüşümü ve Gönüllü İfşa: Yeni Medyada Gözetim, Denetim ve Yeni Mahremiyet 34
2.5. Sosyal Ağların Mahremiyet Algısı Üzerindeki Rolü 36
2.6. Dijital Mahremiyet ve Benlik Gösterisi 37
2.7. Sosyal Medyada İhlal Tartışmaları 40
2.8. Sosyal Ağlarda Alınması Gereken Güvenlik Tedbirleri 43

ÜÇÜNCÜ BÖLÜM

3. KAZAKİSTAN ÖRNEĞİ ÜZERİNE BİR ARAŞTIRMA

3.1. Sosyal Medyada Gözetim Çalışmaları Çerçevesinde Mahremiyet Algısı 44
3.2. Kazakistan'da Yükseköğretim Mezun ve Eğitim Gören Bireylerinin Sosyal Medya Kullanımında Mahremiyet ve Gözetim Algılarına Yönelik Araştırma 45
3.2.1. Araştırmanın Problemi 45
3.2.2. Araştırmanın Amacı ve Önemi 53
3.2.3. Varsayımlar ve Sınırlılıklar 54
3.2.4. Araştırma Yöntemi 54
3.2.5. Veri Toplama Süreci ve Araştırmanın Örneklem Seçimi 56
3.2.6. Verilerin Analizi 57
3.2.7. Araştırmanın Soruları 57
3.3. Bulguların Yorumlanması 58
3.3.1. Katılımcı Özellikleri 58
3.3.2. Katılımcıların Sosyal Medya Alışkanlıkları 63
3.3.3. Katılımcıların Sosyal Medya İçerikleri 70
3.3.4. Katılımcılardan Mahremiyet Algıları 75
3.3.5. Katılımcıların Kişisel Veri Sınıflamaları 80
3.3.6. Katılımcıların Kişisel Verilerinin Paylaşımı ve Kişisel Mahremiyet 81
3.3.7. Mahremiyet İhlali ve Gözetim 87
3.3.8. İnternet Ortamında Kişisel Verilerin Güvenliği 90
3.3.9. Sosyal Medya: Gözetimin Yeniden İnşa Edildiği Bir Zemin 95
3.3.10. Onay Süreci ve Kişisel Verilere Erişim 99
3.4. Gözetim ve Mahremiyete İlişkin Analiz Sonuçlarının Değerlendirilmesi 102
SONUÇ VE ÖNERİLER 107
KAYNAKÇA 111
EKLER 122

TABLOLAR LİSTESİ

Sayfa No.

Tablo 1. Kazakistan Cumhuriyeti E-Devleti'nin 2005-2020 Yılları Arasındaki Başarıları *(Birleşmiş Milletler Dünya Sıralaması)* 48

Tablo 2. Katılımcıların Özellikleri 58

Tablo 3. Katılımcıların Günlük İnternet Kullanım Süreleri ve Kullandıkları Sosyal Medya Araçları 64

Tablo 4. Katılımcıların Sosyal Medya Kullanım Amaçları 66

ŞEKİLLER LİSTESİ

Sayfa No.

Şekil 1. Jeremy Bentham'ın Hapishane Modeli 10

Şekil 2. Bir Dakikada İnternette Neler Oluyor? .....……... 19

Şekil 3. Egov.kz'in Uluslararası Sıralaması 49

Şekil 4. Ekonomi Sektörlerinin Dijitalleşmesi 51

Şekil 5. Dijital Devlete Geçiş 51

Şekil 6. Katılımcıların Yaş Grubu 61

Şekil 7. Katılımcıların Cinsiyeti 61

Şekil 8. Katılımcıların Medeni Durumu 62

Şekil 9. Katılımcıların Eğitim Durumu 62

Şekil 10. Katılımcıların Çalıştığı Sektörler 63

Şekil 11. Günlük Sosyal Medya Kullanımı Saat Ortalaması 63

Şekil 12. Katılımcıların Sosyal Medya Kullanım Amaçları 69

Şekil 13. Katılımcıların Cevaplarına Göre Sosyal Medya Hesaplarında İçeriklerin Değerlendirilmesi 70

Şekil 14. Katılımcıların Sosyal Medya Hesaplarında "Beğen" ve "Paylaş" Yaptıkları İçerikler 71

Şekil 15. Katılımcıların Cevaplarına Göre Kişisel Verilerin Değerlendirilmesi 80

Şekil 16. Katılımcıların Kişisel Verilerinin Paylaşımında Kişisel Mahremiyeti İhlal Edip Etmediğine Dair Görüşleri 81

Şekil 17. Katılımcıların Cevaplarına Göre Sosyal Medyada Gözetim 88

Şekil 18. Katılımcıların İnternette Bilgilerinin Güvende Olup Olmadığına Dair Görüşleri 90

Şekil 19. Katılımcıların Mobil Uygulamaların Erişim İzni İsteklerini İnceleyip İncelemediğine Dair Görüşleri 100

KISALTMALAR

ABD : Amerika Birleşik Devletleri

a.g.e. : adı geçen eser

Akt. : Aktaran

BİT : Bilgi ve İletişim Teknolojileri

BM : Birleşmii Milletler

BS : Bilgi Sistemi

C. : Cilt

Çev. : Çeviren

Der. : Derleyen

DVT : Devlet Veri Tabanı

Ed. : Editör

eGov.kz : Kazakistan Cumhuriyeti'nin Elektronik Devlet Portalı

Haz. : Hazırlayan

KOBİ : Küçük ve Orta Boyutlu İşletmeler

s. : sayfa

S. : Sayı

TDK : Türk Dil Kurumu

vb. : ve benzeri

www : World Wide Web

YÖK : Yükseköğretim Kurulu

GİRİŞ

Günümüzde gözetim olgusu toplumsal ve gündelik örgütlenmenin en önemli kavramlarından biri haline gelmiştir. "Gözetim olgusu teknolojik gelişmeler ile beraber olağan bir nitelik kazanmaya başlamıştır. Bu nedenle şimdi tüm topluluklar gözetim toplumlarıdır" (Bauman ve Lyon, 2013: s. 7).

Bireylerin gündelik hayattaki pek çok etkinlikleri çeşitli yöntemlerle izlenmekte ve kayıt altına alınmaktadır. Kredi kartları, akıllı telefonlar, mağazaların müşterilere sunduğu özel kartlar, sosyal ağlarda ve internetteki tüm paylaşımlar veri olarak kaydedilmektedir. Havalimanları, konutlar, kamusal alanlar ve iş yerleri gibi farklı mekânlarda yer alan güvenlik kameraları aracılığıyla bireyler sürekli olarak izlenmekte ve denetlenmektedir (Rizanaj, 2020: s. 73). Bu sebeple, gözetim olgusu son dönemlerde sosyal bilimler alanında en fazla üzerinde durulan ve incelenen konulardan biri hâline gelmiştir. Rizanaj'a (2020: s. 74) göre, teknolojinin hızla gelişmesi, yaşamı kolaylaştırmakla birlikte, bireylerin çeşitli alanlardaki verilerinin kayıt altına alınmasını mümkün kılarak gözetim süreçlerinin yaygınlaşmasına neden olmaktadır.

Dijital çağın ortaya çıkardığı yeni ekonomik yapı, artık devletin de bu dönüşüme eş zamanlı ve uyumlu politikalarla yanıt vermesini zorunlu kılmaktadır.

Bugün dijital dönüşüm süreci ile dijital iletişim teknolojileri yaşamın her sahasını etkilemiştir. Bireyler, bulundukları her ortamda dijital araçlar aracılığıyla izlenmekte ve denetlenmektedir. Denetim mekanizmasının, gücü ve otoriteyi elinde bulunduran küçük bir kesimin geniş toplulukları kontrol altında tutmasına olanak tanıyan panoptik gözetim yapısı, günümüzde yeni iletişim teknolojilerinin etkisiyle önemli bir dönüşüm geçirmiştir (Kavut, 2023: s. 22–23).

Bilgi devrinde, ülkenin kalkınma ve büyüme stratejisi olarak faydalanabileceği en önemli imkanlardan biri e-Devlet'tir. Topluluğun her kesimi tarafından kullanacak bir e-Devlet biçiminin geliştirilmesi, bu anlamda rasyonel bir yol olacaktır (Kuran, 2005: s. 6).

Bu doğrultuda çalışmanın ilk bölümünde, gözetim olgusu, gözetim toplumu kuramı ve farklı gözetim modelleri detaylı biçimde ele alınmıştır. İkinci bölümde ise sosyal medya ile mahremiyet kavramları incelenmiş; sosyal ağların kullanım amaçları ve bu platformların mahremiyet algısının oluşumuna olan etkileri değerlendirilmiştir. Ayrıca,

kapsamlı bir inceleme alanı olan mahremiyetin türleri üzerinde durulmuş ve geleneksel gözetim toplumundan dijital çağın yeni gözetim anlayışına geçiş süreci irdelenmiştir.

Çalışmanın üçüncü bölümünde, Kazakistan Cumhuriyeti'nin Elektronik Devlet Portalı (eGov.kz) analiz edilerek kapsamlı bir değerlendirme yapılmıştır. Bu çerçevede, portal bünyesinde yürütülen projeler ile en çok talep gören hizmetler özellikle vurgulanmıştır. Bölümün araştırma kısmında ise; kartopu örnekleme yöntemi ve yarı yapılandırılmış mülakat tekniği aracılığıyla, sosyal medya platformlarında gözetim ve mahremiyet algılarına ilişkin bulgular ortaya konmuştur. Araştırma, Kazakistan'da lisans, yüksek lisans ve doktora düzeylerinde öğrenim gören ya da bu düzeylerde mezun olup mesleki hayatına atılmış bireylerin, sosyal medya kullanımları sırasında gözetlendiklerine dair farkındalıkları ile özel yaşamlarına dair paylaşımlarda bulunurken mahremiyet konusunda endişe taşıyıp taşımadıklarını incelemektedir. Yarı yapılandırılmış mülakatlardan elde edilen veriler, belirli bir sistematik çerçevede değerlendirilmiş ve analiz edilmiştir.

BİRİNCİ BÖLÜM

1. GÖZETİM KAVRAMI, GÖZETİM TOPLUMU VE GÖZETİM MODELLERİ

1.1. Gözetim Kavramı

Gözetim olgusu, gerçekte yeni ortaya çıkan bir kavram değildir. İnsanlar, geçmişten günümüze kadar davranışlarının izlenmesi, denetlenmesi veya yönlendirilmesi amacıyla sürekli olarak gözetim altında tutulmuşlardır (Lyon, 1994a: s. 22).

Dolgun'un (2005: s. 25) belirttiği üzere, sosyal bilimlerde gözetim olgusu genellikle modern örgütler ve ulus-devletlerle ilişkilendirilse de; tarihin ilk dönemlerinden beri gerek kabile yapıları gerekse dinlerle geleneksel devletler, toplumsal düzeni sağlamak amacıyla gözetimi bir araç olarak kullanmışlardır. Bu sebeple, gözetim çok eski zamanlara dayanan bir olgu olup, toplumların yapısıyla doğrudan ilişkilidir.

Jeremy Bentham (1748–1832), 1791 yılında Londra'da yayımlanan ve aynı yıl Fransız Devrimci Meclisi tarafından Paris'te hızla yaygınlaştırılan *Panopticon* adlı eserinde gözetim kavramını, "bireyin zihni üzerinde daha önce benzeri olmayan bir zihinsel denetim kurma yöntemi" olarak tanımlamıştır. Bentham'ın bu yaklaşımı, gözetimin sadece fiziksel değil aynı zamanda psikolojik bir güç ilişkisi içerdiğine işaret etmektedir. Yasal faydacılık ekolünün kurucularından olan İngiliz profesör, birçok cezaevi reformu yasa teklifinin mimarı olarak, panoptikon kavramını cezalandırma yetkisi bağlamında geliştirdiği pragmatik ceza hukuku teorisiyle temellendirmiştir (Mattelart, 2012: s. 13).

Gözetim, bir kişinin ya da grubun verilerini, onları etkilemek veya kontrol etmek amacıyla toplanması ve işlenmesi anlamına gelir ve bu veriler ister tanımlı ister tanımsız olabilir (Lyon, 2006: s. 13). Günümüzde gözetimin en önemli aracı, bilgiyi depolama, kopyalama, geri çağırma, analiz etme, pazarlama ve paylaşma gibi işlevleri mümkün kılan bilgisayarlardır (Lyon, 1994b: s. ix).

TDK'nin sözlüğünde ise "gözetim" kelimesi, "koruma, denetleme işi, hukukta gözaltı veya nezaret" olarak tanımlanmıştır (Rizanaj, 2020: s. 74).

Lyon'a göre (2003: s. 30), "gözetim" kelimesinin genellikle, rutin, gündelik faaliyetlere işaret eden, aynı zamanda bireysel faaliyetlerin çaşıtlıkla, gizli soruşturmalarla takip edilmesini ve dolaysız çağrışmaları barındırmaktadır. Fransız

dilinde "izlemek" anlamına gelen "surveiller" fiilinden gelen gözetim, merak duygusunun arkasında, birey hareketlerinin dikkate alındığı süreçlere dayanmaktadır.

Weber'in ve farklı yönlerden Foucault'nun da açıkladığı üzere, 'gözetim' ile bağlantılı olan öz-disiplin modern kurumların işlemesi ve gelişmesi için gerekliyken, artık kimi diğer durumsal denetim motiflerinin de bu türde öz-disipline uygulandığını (ve kimi zaman bunun yerini aldığını) söylemek de mümkündür (Lyon, 2013: s. 13).

Gözetimin her zaman iki yüzü vardır. Tam olarak sözcük (Fransızca'da) "gözlemlemek, korumak" anlamına gelir. Türkçede bu terim "gözetim" olarak da kullanılır. Örneğin, günlük e-posta yazışmalarında bu durum gözlemlenebilir. E-posta, zaman ve mekân sınırlamalarını aşarak eş zamanlı iletişime imkân veren esnek bir iletişim biçimi olarak tanımlanmaktadır (Lyon, 2006: s. 14-15). Çok sayıda imkân sağlayan ve yeni özgürlükler sunan bir iletişim aracı olarak görülen e-postanın, farklı bir perspektiften daha az cazip yönleri de bulunmaktadır.

Modern dünyada günümüz insanını sarmalayan gözetim kavramı, herkesle ilgili her şeyi öğrenme ve bilme isteği olarak tanımlanmaktadır (Kütükoğlu, 2021: s. 105). Bu istek tatmin edilince, herkesin herkesle ilgili her şeyi bilmesine izin verilmiş olmaktadır (Niedzviecki, 2009: s. 15). Modern dönemde gözetim, farklı teorik yaklaşımlar çerçevesinde ele alınmaktadır. Karl Marx'a göre gözetim, kapitalist sistemin ekonomik ve politik yapısının ayrılmaz bir parçasıdır. Max Weber bu olguyu bürokratik yapılanmanın bir ürünü olarak değerlendirirken, Michel Foucault ise gözetimi, cezalandırma ve gösteri temelli bir anlayıştan bireyin kendi üzerinde kurduğu öz-disiplin biçimine evrilen bir süreç olarak tanımlamaktadır. Bu perspektiflerin her birinde, kendine has bir sistem ve birey anlayışı öne çıkmaktadır (Lyon, 2013: s. 15). XXI. yüzyılda gözetleme insan bünyesi üzerinde sonuçlar doğuran bir olgu olarak tanımlanmaya başlamıştır. Niedzviecki (2009: s. 27-28), "Gözetimin, modern teknolojik toplumda bireyleri sürekli dikkat çekme, eğlence ve gösteri amaçlı olarak açıkta bırakan ve toplumsal bilinci dönüştüren bir mekanizma olarak tanımlandığını" ifade etmektedir. Lyon (2006: s. 21), gözetimi, risk altındaki toplumların yönetilmesinde bilgi üretme biçimi olarak görmektedir. Bazı gözetim sektörleri belirli yaşam alanlarına diğerlerinden daha fazla müdahalede bulunmadıkça, bireyler gözetimden kaçamamaktadır.

XIX. yüzyıldan itibaren gelişen gözetim pratikleri, modernite bağlamında incelenmektedir. Sanayi kentlerinin yaygınlaşması, ulus-devletin güvenlik kaygıları

doğrultusunda kendini koruma refleksi, devletin idari yapılanması, askeri örgütlenmelerin güçlenmesi ve kapitalist üretim ilişkilerinin kurumsallaşması bu sürecin temel dinamikleri arasında yer almaktadır. Modernitenin bürokrasi ve fabrika temelli kurumları çerçevesinde şekillenen gözetim mekanizmaları, bireylerin gündelik yaşamındaki etkilerini nedensellik ilişkileriyle daha anlaşılır kılmaktadır. Teknoloji ile iktidar arasındaki etkileşim bağlamında ise, toplumsal gözetim ve denetim süreçleri, gözetim üzerine kurgulanan distopik anlatıların sınırlarını zorlayacak biçimde genişlemiştir (Çaycı ve Çaycı, 2017: s. 41).

Modern dünyada yaşayışımız ve çevremiz değişirken gözetim hakkında çeşitli gelişmeler de meydana gelmektedir. "Hiçbir zaman şahit olamayacağımız nesneler tarafından günde birkaç defa tedirgin edici bir seviyede yakın plan fotoğrafımız çekilmekte ve veritabanlarında depolanmaktadır. İnternette yaptığımız araştırmalarımız, cep telefonlarımız ve sosyal ağ hesaplarımız bizimle ilgili birçok bilgiyi ulaşır hale getirmektedir" (Draper, 2018: s. 65). Dijital gözetimin dünyaya yayılması mahremiyetin yitirilmesinde ve manasından uzaklaşması konusunda da çok önemlidir. Gözetim genellikle fark edilmeden gerçekleşir ve varlığı pek bilinmez. Ancak bu süreçler sadece bireysel anlamda değil, uluslararası ilişkilerde de mahremiyetin tehlikeye girmesine yol açmaktadır. Özellikle ülkeler arası geçişlerde, yolcuların kişisel bilgileri kayıt altına alınıp sınıflandırılmakta, bu da mahremiyet ihlallerini somutlaştırmaktadır.

Gözetim, bazı birey ve gruplara zarar verirken, bazı birey ve gruplara yönelik yarar sağlamak amacıyla kullanılmaktadır. Bu açıdan gözetleme, bireylerle ilgili bilgi toplama, yayma ve yorumlamaya ilişkin birtakım veriler sunmaktadır (Fuchs, 2014: s. 218).

Gözetimin araştırdığı kategoriler oldukça belirgin olabilir; ancak bunlar en genel haliyle, birçok farklı rolde sıradan vatandaşa dokunan grupları içerir. Gözetim verileri herkesten aynı şekilde ve aynı yoğunlukla toplanmaz. Gözetim, modern hayatın farklı yönlerinde oynanan rollerle ilgilenir. Bunun en açık türü, kendilerine ödenen ücretlerin karşılığını verip vermediklerini kontrol etmek amacıyla şirketler ve devlet kurumları tarafından gözetlenen işçilerdir. Tüketiciler satım ve promosyon gibi açık hedefler doğrultusunda pazarlamacılar tarafından izlenir ve profiller oluşturulur. Vatandaşlar bilhassa vergi, sağlık, iş güvencesi gibi önemli konularda etkin yönetim için doğum anından itibaren etiketlenirler. Bireyler pasaport, ehliyet veritabanlarıyla ilişkili diğer kimlik türlerini yanlarında taşımak, kimliklerini doğrulamak ve denetimi kolaylaştırmak

zorundadırlar. Çocuklar okullarda, sokaklarda gerek ebeveynleri tarafından eğitsel açıdan gerekse de gözetimden sorumlu emniyet organları tarafından 'güvenlik amaçlı' gittikçe daha sıkı izlenmektedir (Lewis, 2006). Saldırganlar ve şüpheliler gerek kurumlar içinde gerekse de elektronik etiketleme gibi uzaktan çalışan aygıtların gelişmesiyle beraber topluluk içinde üst düzey bir gözetleme ve denetlemeye tabi tutulmaktadır (Lyon, 2013: s. 37).

11 Eylül saldırılarının ardından, kamuoyu gözetim odaklı kamu güvenliği politikalarına yönelirken, havaalanlarındaki ulusal kimlik kartları ve biyometrik tedbirler gibi önlemlerin 'terörle mücadele'de kabul edilebilirliği tartışılmaya başlanmıştır. Genellikle bu tartışmaların biçimi ve gerekçeleri doğrultusunda, Avrupa ve Kuzey Amerika'da geniş çaplı bir onama süreci ortaya çıkmıştır (Zureik, 2003). Ne var ki, gözetim çalışmaları içinde, bütün koordinat türleri ilgi çekicidir; belli bir amaca dönük veri toplama eğilimi başka amaçlar için de kullanabilmektedir (Lyon, 2013: s. 36). Tüketici verileri, örneğin, polisin ilgisini çekerken, aynı zamanda ilaç firmaları tıbbi verilerle, sigorta şirketleriyse polis kayıtlarıyla ilgilenmektedir.

1.1.1. Gözetim Toplumu

Gözetim toplumu kavramı, Michel Foucault tarafından 1975 yılında kaleme alınan ve İngilizceye "Discipline and Punish: The Birth of the Prison" adıyla çevrilen "Surveiller et punir: Naissance de la prison" (Hapishanenin Doğuşu) adlı eserinde ayrıntılı biçimde incelenmiştir. Foucault, Panoptikon modelinin, bugünün toplumsal denetimlerini şekillendiren disiplin toplumu paradigmasının temelini oluşturduğunu vurgular. Önceki toplumlar egemenliklerini belirli bir alanla sınırlandırırken, disiplin mekanizmaları bireylerin bedenlerine dolaylı yollardan işler. Çünkü bu disiplin altında kalanlar, iktidarın desteklediği bir ortamla karşı karşıya kalır ve böylece sadece bu büyük disiplin düzeninin dişlilerinden biri haline gelirler.

Bireysel sosyal normları içselleştiren iktidarın üretkenliğinin teknolojik olarak serbest bırakılması, XVII. ve XVIII. yüzyıllardan başlayarak perde arkasında hazırlanmıştır. Norbert Elias bu süreci "Batı medeniyetinin medenileşme sürecinin izini sürerek" gösterir (Elias, 1973: s. 271). Bu medeniyet sadece hapishanelerde değil; cinsel davranışlardaki, sofra adabındaki ve şiddetteki değişimle başlar. İç ve dış baskılardaki gelgitler, giderek bağımlılık ve kısıtlamayla sonuçlanır; bu da yaşamı düzenleyen ve düzelten etkili bir iradeyle, kısaca kendi kendine hakim olmayla sonuçlanır.

Roger Clarke ise, gözetimi ilk aşamada "kişilerin ya da grupların iletişimlerinin ve eylemlerinin sistematik şekilde takip edilmesi" veya "bir kişinin hareketlerinin yakından izlenmesi" olarak tanımlamaktadır. Bugün "enformasyon (bilgi) toplumu" dediğimiz yapı, giderek 'gözetim toplumu'na dönüşmekte ve teknolojiyle birlikte günlük yaşamımız da bu sürece hızla adapte olmaktadır. Toplumların yönetim ve denetim süreçlerinde, iletişim ve bilgi teknolojilerine olan bağımlılık, onları aynı zamanda *gözetlenen toplumlar* haline getirir. Bu gözetim faaliyetlerinin etkisi, daha önce tarihte rastlanmamış bir şekilde gündelik yaşamda yoğun biçimde hissedilmektedir (Lyon, 2006: s. 11).

Gözetim toplumu kavramı, bireylerin mahrem yaşamlarına ilişkin tüm verilerin kamusal kurumlar ya da büyük ölçekli özel sektör kuruluşları tarafından sistematik biçimde toplanması, arşivlenmesi ve işlenmesi süreçleri çerçevesinde tanımlanmaktadır (Dolgun, 2005: s. 16).

Günümüzdeki gözetim toplumunu belirgin kılan üç temel unsur bulunmaktadır (Dolgun, 2005: s. 127). Bunlardan ilki, küresel terör olaylarına karşı geliştirilen ve güvenlik merkezli olarak uygulanan gözetim stratejileridir; bu uygulamalar bireysel mahremiyetin neredeyse tamamen ortadan kalkmasına yol açmaktadır. İkinci olarak, e-Devlet sistemlerinde ortaya çıkan izleme ve denetim mekanizmaları dikkat çekmektedir. Üçüncüsü ise, kapitalist sistemdeki dönüşümlerle birlikte yeni ekonomik yapı ve tüketimin ön plana çıkmasıdır. Bu bağlamda, tüketici davranışları da çok daha ayrıntılı biçimde izlenmektedir.

"Gözetleme toplumu iktidar açısından yarar sağlayarak toplumu kontrol altında tutabilmek amacıyla yeni güç sistemleri üretmektedir. Böylesi bir ortamda üretilen bu güç sistemleri toplumsal yaşamı askeri bir nizama ve göz hapsine çevirmektedir. Tek bir merkezin denetiminde olup, tüm bireylerin belirlenen kurallar içinde hareket ettiği bir toplumsal düzen, bireylerin özgürlüğünden mahrum bırakıldığını göstermektedir" (Çoban, 2016: s. 119). Günümüzde toplumların gözetim altında tutulduğu konusundaki kaygıların artmakta olduğu görülmektedir. İnternette paylaşılan görüntüler, cep telefonlarıyla çekilen kareler, şehirlerdeki güvenlik kameraları, bankamatiklerin kameraları, dronlar ve uydular, toplumların her anını izleyerek gözetim altında tutmaktadır. Bugün bilgi çağının giderek bir gözetim toplumu haline dönüştüğü açıktır. Sanayi Devrimi'yle yaşanan sosyo-ekonomik değişimlerin benzeri, günümüzde bilgi ve

iletişim teknolojilerinin yükselişiyle ortaya çıkmaktadır. Çalışma hayatı, ekonomi, eğitim, gündelik yaşam gibi pek çok konu sanal dünyaya göç etmektedir.

21. yüzyılda gözetlenen toplumlar, karmaşık iletişim ve bilgi teknolojisi ağlarına bağımlı hale gelmiştir (Lyon, 2006: s. 59). Bu iletişim ağlarının kendisi görünür olmasa da, videolar, uydular ve biyometrik gözetim gibi unsurları içeren tüm izleme biçimlerini desteklemektedir. Dolayısıyla iletişim altyapısı, bilginin temel taşıyıcısı olarak kabul edilmektedir. Gözetlenen toplumların pek çok ortak noktası vardır, ama ayrıca, ulusal değişikliklere ve ekonomik sektörlere bağlı olarak oldukça fazla farklılık da gösterirler. Yeni teknolojiler, gözetimin yeni şekillerde şiddetini artırmak ve düzenlemek için çalışırlar, ama hiçbir şeyi başlatmazlar.

Modern devlet yönetimi, bireysel bilgilerin toplanmasına ve kaydedilmesine dayanmaktadır. Öte yandan, modernliğin bir başka yönü olan kapitalist yatırımlar da kâr ve verimliliği artırmak amacıyla, çalışanları fark edilmeyecek derecede izler ve denetler. Böylece, modernlik; iktidarı sürdürmek ve yeniden üretmek için bilgiye ve veriye dayalı bir düzeni ifade eder. Bu verilerin büyük bir kısmı bireylere ait olduğundan, gözetim dikkatini özellikle kişisel bilgiler üzerine yoğunlaştırır (Lyon, 2006: s. 64).

"Gözetlenen toplum" kavramı, bilgi teknolojilerinin yarattığı yeni imkânların en yoğun biçimde hissedildiği bir dönemde ortaya çıkmıştır. Sosyolog Gary T. Marx, bu terimi ilk kez 1985'te, bilgisayar teknolojisi aracılığıyla tüm sosyal denetim engellerinin ortadan kalktığını gösteren Orwellvari bir durumu anlatmak için kullanmıştır (Marx, 1985). Gary T. Marx'ın hedefinde öncelikli olarak Amerika varken tarihçi David H. Flaherty, yakın bir tarihte "Batı endüstriyel toplumlarının bilgi toplumu olmanın bir parçası olan, gözetlenen toplum haline gelme riskinin arttığını -hatta belki de şimdiden geldiklerini-" ileri sürmüştür (Flaherty, 1989: s. 1). Flaherty'nin odak noktası Almanya, İsveç Fransa, Kanada ve Amerika'ydı. "Bazı şekillerinin demokratik bir toplumda elbette ki yasal olduğunu" kabul etse de, "bunların kişisel mahremiyet üzerindeki toplanmış etkisinin negatif" olduğu konusunda ısrar etmiştir. Marx gibi, Flaherty de yeni teknolojilerin gözetleme kapasitelerine önemli değişiklikler yaptığını görmüştür. Ayrıca, onun ve Colin Bennett'in (1992) çalışmaları, gözetleme yollarının bir ulusal ya da bölgesel konumdan diğerine değiştiğini göstermiştir.

Flaherty'nin vardığı sonuç, incelediği her ülkede, kişisel veri toplamasının otomasyonu için olan baskılar 'neredeyse karşı konulamaz' olsa da, o zamanlar, İsveç

kamusal ve özel veri tabanlarının birleştirilmesi yönünden diğer örneklerden daha ileridedir (Flaherty, 1989: s. 375). Fakat, Flaherty'nin öncelikle ilgilendiği konu, gözetlemenin analizinden çok mahremiyet ve verinin kontrolüdür. Gözetleme pratiklerini desteklemek amacıyla benzer teknik yöntemlerin kullanımı giderek artmakla birlikte, bu uygulamalar farklı şekillerde hayata geçirilmektedir. Örneğin, Almanya ve İsrail'de kimlik kartı taşıma zorunlu kabul edilirken, Avustralya ve Amerika'da ulusal kimlik kartı tasarıları bile kabul görmemektedir. Tayland ve Endonezya gibi ülkelerde ise, örneğin telefonu gizlice dinleme yoluyla, bir kişinin özel hayatına karışma, Kanada ve Yeni Zelanda'da olduğundan çok daha sıradandır.

Gözetlenen toplum kavramı, görünür olmayan gözetim biçimlerinin toplumsal yaşamda giderek yaygınlaştığına işaret eder (Lyon, 2006: s. 68). "Gözetim toplumunun en güçlü aktörlerinden biri olan sosyal medya platformları, bilgi madenciliği faaliyetleri açısından en aktif şekilde rol almaktadır. Bu ağlarda kullanıcılar hem diğerlerini gözetler hem de kendileri gözetim altına alınır. Ayrıca, kişisel mahremiyetleri, endüstrinin çıkarları doğrultusunda kullanılmaktadır" (Arık, 2018: s. 15).

İletişim temelli toplumlar, kaçınılmaz şekilde denetim altında tutulan yapılar hâline gelmiş olup, aynı zamanda modern teknolojilere yoğun bir şekilde bağımlılık göstermektedir. Fakat, buna ek olarak, gözetlenen toplumlar, enformasyon altyapısının birleşmişliğinin hürmetine, gözetimin toplumsal hayatın her sektörüne yayıldığı bir hale gelmiştir.

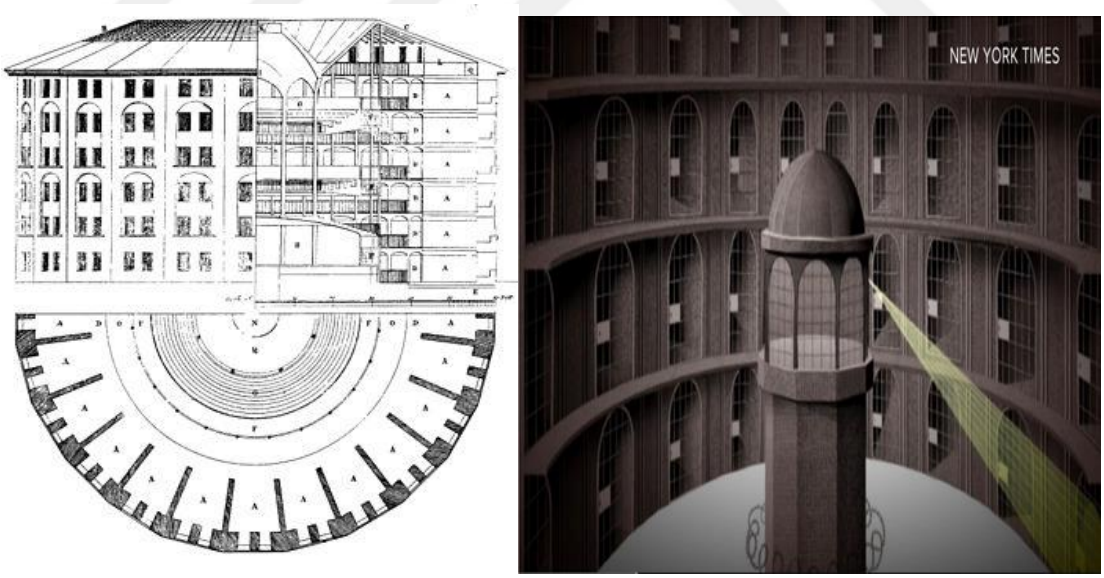
XXI. yüzyılın başında, sosyal değişimin farkına varmak için enformasyon ve komünikasyon teknolojileri çok önemli alana sahip olmuştur. Bilgisayar alışkınlığı, hem günlük yaşamlar hem de küresel bağlantıların bir parçası haline gelmiştir. Aslında, günümüzdeki küreselleşme ve günlük yaşam, kısmen, bizim bilgisayarlarla olan ilişkimiz tarafından kurumlaştırılmıştır. Hiçbir ülke, enformasyon altyapısının oluşumundaki yerini kaybetmek istemez. Özellikle, en azından, telefonlara, televizyonlara ve internete olan giriş izni söz konusu olduğunda, çok az vatandaş ya da müşteri enformasyon akımlarının iletişim ağlarının dışında kalmak ister. "Elektronik bağlantıların dünyası iki yönlü bir işleyişe sahiptir. Bir yandan, küresel köyü evimizin önüne kadar taşırken, diğer yandan kişisel verilerimizi alır; bu veriler işlenir, dönüştürülür ve 'piyasaya' sunulur, sonunda ise bizim yaşamımızı şekillendirmek amacıyla kullanılır" (Lyon, 2006: s. 218).

1.2. Gözetim Modelleri

Geçmişten bugüne kadar farklı gözetim sistemlerinin ortaya çıktığı görülmektedir. Bu sistemler hem gözetimin nasıl gerçekleştiğini hem de zaman içerisinde nasıl dönüştüğünü ortaya koymaktadır. İlgili literatür incelendiğinde *Panoptikon (Süperpanoptikon), Sinoptikon* ve *Omniptikon* şeklinde üç gözetleme modelinin karşımıza çıktığı görülmektedir. Burada bu modellerin üzerinde çalışmanın kapsamı bağlamında durulacaktır.

1.2.1. Panoptikon

1787 yılında Jeremy Bentham'ın ilk kez kullandığı "Panoptikon" kelimesi, Yunanca *"pan" (her şey) ve "optikos" (görmek için)* kelimelerinin birleşiminden türetilmiştir. Panoptikon, hapishanelerde denetimi sağlamak amacıyla tasarlanmış bir yapıdır. Burada, hücreler dairesel bir düzende yer alırken, merkeze yerleştirilmiş bir gözetleme kulesi vardır. Böylece gardiyan, mahkumları tek taraflı olarak izleyebilir. Mahkumlar gözetlendiklerinin bilincindedir; bu nedenle davranışlarını ona göre ayarlarlar ve kendilerini sürekli olarak tedirgin hissederler (Yıldırım, vb., 2006: s. 181). Yani, *azınlığın çoğunluğu izleme yöntemidir.*



Şekil 1. *Jeremy Bentham'ın Hapishane Modeli*
Kaynak: (Bentham, 2016: s. 7)

Şekil 1'e bakıldığında, bu mimaride binanın ortasında bir gözetleme kulesi yer alır ve hapishane müdürü bu kuleden, hücrelerin bulunduğu dairesel yapının tamamını görebilir. Hücrelerde yalnız kalan mahkumlar, gözetim altında olduklarını bilseler de

gözetleyeni göremezler (Mattelart, 2012: s. 13; Bıyıkbeyi, 2019: s. 26-27). Hücrelerin ışıkla tamamen aydınlatılması nedeniyle mahkumlar gözetimden kaçamaz; ancak gözlem kulesinin içini göremedikleri için tam olarak ne zaman izlendiklerini asla anlayamazlar.

Bu tür bir yapı, toplumu düzenleyen ayrıntılı bir tasarımın ifadesidir ve bir tür ütopya projesini destekler. Bentham, bu düşünceyi yalnızca hapishanelerle sınırlı tutmamış; cezaevleri, işçi yurtları, yoksul evleri, ıslah kurumları, fabrikalar, hastaneler, akıl hastaneleri, karantina bölgeleri ve okullar gibi farklı gözetim alanlarına da uygulanabileceğini savunmuştur. Bentham'a göre bu basit mimari yaklaşım sayesinde "sağlık yönetimi iyileştirilir, ahlaki düzen reforme edilir, sanayi güçlenir, eğitim yaygınlaşır, ekonomi eski gücüne kavuşur ve Sosyal Yardım Kanununun çözülmesi gereken düğümü de çözülmüş olur." (Evans, 1971: s. 21-37). Yine Bentham bunun devlet açısından daha az maliyetli olacağını, daha az hapishane müdürüne ihtiyaç duyulanların da sözleşmeli çalıştırabileceğini iddia eder. Ne var ki, Bentham'ın projelerinden hiçbiri - en azından hayal ettiği şekilde- gerçekleşmemiştir.

Panoptikon kavramı, haber anlatıda mutlaka bir tarafın gözetlenmesi anlamına gelmez. Elektronik olarak geliştirilmiş, her şeyi gören göz düşüncesi, her çeşit duruma uygundur (Gandy, 1993: s. 15). Fakat oldukça değişik kullanımları vardır. Bir taraftan, hapishane mimarisinin otomatlaşmış bir makine olduğu, modern faydacıl Benthamite çerçevesiyle ilintilidir. Diğer taraftan, daha postmodern bir durumda panoptikon, repertuvarı bir simulasyon içinde anlaşılan bir çeşit söylemdir. Buradaki soru, bu iki yaklaşımın ortaya konduğu tartışmada katılımcıların karşı karşıya mı geldikleri, yoksa, beraberce sorgulanan olayda bütün bir resim mi oluşturduğudur.

Bu, hem analitik hem de politik nedenlerden dolayı bir anlık bir sorudur. İlk olarak, sosyolojik içerikli bir soruyu ortaya çıkarır: Teori neden enformasyonel olarak doyuma ulaşmış sosyal çevre için yeterlidir? Her teori, kendine özgü bir dizi bağlamda farklı biçimlerde yorumlanabilir; bu durum, gözetimin dijital ortamlara taşınmasıyla daha da belirginleşmektedir. Fakat, ikinci olarak, pek çok kişi bu soruyu politik olarak değerlendirir. Özellikle düzenleme ve direnişi içeren, gelişmekte olan uygun karşılıklar, önemli bir şekilde bugün gözetlenen toplumlarda hangi çeşit bir gücün uygulandığını anlamaya bağlıdır (Lyon, 2006: s. 220-221).

"Bu konuda araştırma yapan birçok bilim insanı iletişim teknolojilerinde ortaya çıkan gelişmelerle birlikte günümüz toplumlarının bir çeşit panoptikonaya dönüştüğünü

belirtmektedirler" (Deborah, 2001: s. 113). Bugün, sesli ve görsel verileri işleyen, iletişimi ve ulaşımı kolaylaştıran araçların varlığı nedeniyle bireyler daha kolay izlenebilir, dinlenebilir ve kişisel verileri çeşitli amaçlar için kullanılabilir hale gelmiştir. Modern toplumlarda gözetim, kurumsal bir yapı hâline gelmiş ve farklı sosyal kuramcılar tarafından çeşitli teorik çerçevelerle analiz edilmiştir. Bununla birlikte, sosyal bilimlerde gözetim olgusunun sistematik biçimde ele alınması, Jeremy Bentham'ın düşüncelerinden hareketle Michel Foucault tarafından başlatılmıştır. Bu doğrultuda, gözetim modelleri içerisinde panoptikon metaforu, kuramsal açıdan büyük önem taşımaktadır (Dolgun, 2005: s. 3).

Foucault (2017: s. 302-303), panaptikonu hükümetin (iktidarın) insanların günlük yaşamlarına olan müdahalesinin göstergesi olarak yorumlamaktadır. Bentham ise, yalnızca özel bir kurum ve kapalı bir yapı olarak tanımlamıştır. Bu noktada, panaptikonun soyut bir tasarım olmadığını; aksine, ideal bir yönetim mekanizması olarak işlev gören, her türlü engelden arındırılmış, sade ve abartısız bir yapı şeklinde düşünülebileceğini belirtmiştir. Bu bağlamda iletişim teknolojilerinde meydana gelen gelişmeler gözetim teknolojilerini de geliştirmiştir. Ortaya çıkan bu yeni durum hayatın her alanında mahremiyeti ortadan kaldırarak gözetlenen bir toplumsal yapıyı inşa etmiştir.

Baban'a göre, demokrasi bulunmayan ülkelerde, iktidarı elinde bulunduranlar, her şeyi kontrol altına almak amacıyla bütüncül bir düzen kurmak isterken, bireyleri serbest bırakmış gibi görünmektedir. Ancak, Panoptikon modelinde olduğu gibi, onları sürekli gözetleyerek hem zihinsel hem de algısal düzeyde bir esaret ortamı yaratmaktadırlar. Bu durum, kimliğin yeniden şekillenmesinde de önemli sebepler oluşturur. Tüm bunlarla birlikte, iletişim teknolojilerinin gelişimiyle beraber gözetim teknolojileri de ilerlemiştir. Bu gelişmeler neticesinde yaygınlaşan panoptikon tipi iktidar mekanizmaları, yaşamın tüm alanlarında mahremiyetin giderek erozyona uğramasına sebep olmuştur. Bu süreç, hem bireysel hayatı hem de toplumsal yaşamı ilgilendiren temel soruların ortaya çıkmasına zemin hazırlamaktadır. Bu sebeple görünme isteği, bir arzusu görünür kılmaya çalışılmıştır" (Köse, 2011: s. 11).

Bugün dünyanın bir çok yerinde uygulanan e-devlet uygulamaları panoptikonun bir yansıması olarak ortaya çıkmıştır. Kavramın İngilizce karşılığı "e-Government" ifadesinde yer almakla birlikte, "elektronik hükümet" veya "elektronik yönetim" şeklinde

de tanımlanabilir. Ancak, Türkçe çevirilerde en yaygın olarak "e-Devlet" terimi kullanılmaktadır (Oğurlu, 2010: s. 15).

1.2.1.1. Süperpanoptikon

Yukarıda da değinildiği gibi, gözetim anlayışı panoptikon modeliyle, modernitenin ilerlemesiyle birlikte ortaya çıkmıştır. Bauman, günümüzde aynı yöntemin siber dünyada "süperpanoptikon" olarak adlandırıldığını ve bu yolla insanların kendi isteğiyle gözetim altına girdiklerini belirtmektedir. Öte yandan, bu bağlamda başkalarının panoptik sistemin içinde değil, dışında kaldığını ifade etmektedir (Akt. Nakıboğlu, 2015: s. 389).

Panoptikonun birliği ve elektronik gözetlemeyi teşvik eden Foucault'un analizleri olsa da, ilk ortaya çıkan, ironik bir şekilde Foucault takipçisi olamayan bir panoptikon versiyonuydu. Örneğin, Oscar Gandy, *Panoptik Çeşit*'te panoptik mecazı mükemmel bir şekilde kullansa da, bu tartışmacı bir yaklaşım değildir. Sosyolojik olarak, özellikle Weber ve Marx bakış açılarına yakın olarak gelenekseldir. Görünüşe göre panoptikon, söylem yükü olmadan var olan disiplin analizlerine ve sosyal kontrole uymaktadır. Foucault'un analizinin ayırt edici söylemsel bölümlerini aradan çekip çıkarmak, kendisinin hatırladığı gibi 'veri tabanlarının dilin konfigürasyonları olduğu' gerçeğiyle beraber, Mark Poster'e kalmıştır (Poster, 1996: s. 176). Bundan dolayı Poster, bilinçli bir şekilde, Marx ve Weber'in geliştirdiği davranış odaklı gözetleme teorilerinden dikkatini başka yöne çevirir. Poster için, veri tabanları sembollerle çalışır ve sunumlar onları postyapısal analize açar. Fakat, Melucci'nin bundan çıkardığı, Poster'in tersine, sembolik iletişimin dengesizliği ve itiraz edilebilirliğidir (Lyon, 2006: s. 232-233). Bu, şüphe götürmez bir şekilde, teoriyi daha postmodern bir çerçeveye taşımaktadır.

Poster'in gözlemlerine göre, Foucault'un ceza ve cinsellik üzerine anlattığı ünlü hikâyelerde olduğu gibi, iktidarın söylemsel kuramını doğrudan izlememektedir. Söylem gücünü, "baskının yapılarıyla öznenin ilişkilendirilip, sonrasında bu yapıların özne üzerinde işlev göstermesi" şeklinde açıklamaktadır (Poster, 1995: s. 181). Panoptikonun gücü yalnızca sürekli gözetleyen yetkililerde değildir; aksine, tüm sistem ve söylem uygulamaları, özneyi suçlu olarak tanımlamak, onu rehabilite ederek normalleştirmek veya ahlaki bir devrimle şekillendirmek amacını taşır. Poster'e göre, bilgisayar veri tabanları panoptikonu hapishanelerin dışına taşır ve süperpanoptikon olarak toplumun tamamını, öznenin kurumsallaşmasını yeniden düzenleyecek şekilde işler (Deleuze, 1992: 59, 3-7).

Günümüzde kullandığımız cep telefonları, sokaklarda bulunan kameralar, internet alışverişleri, dinleme cihazları ve sosyal medya, süperpanoptikon modelinin vazgeçilmez unsurları haline gelmiştir. Bu teknolojiler aracılığıyla iktidar, her noktaya ulaşabilmektedir. Elektronik verileri ve elektronik parmak izlerini toplayan kurumlar, bireyleri sınıflandırarak onların profillerini oluşturmaktadır. Elde edilen bu bilgiler, iktidarın gücünü pekiştirmektedir. Sokaklara yerleştirilen ve çevreyi sürekli izleyen kameralar, hapishanelerdeki panoptikonun modern ve elektronik bir versiyonu olarak kabul edilmektedir.

Her satın alma işlemi ve kredi kartı kullanımıyla çoğalan büyük veri yığınları, süperpanoptikon modelini hayata geçirmiştir. Biriken verilerle beraber kontrol edilen kişiler, gözetim mekanizmasının zorunlu ve bilinçli bir parçası haline gelmiştir. Bu durum, süperpanoptikon kavramını geleneksel panoptikon modelinden ayırmaktadır (Güven, 2014: s. 100).

Panoptikon modeli, kendi iç dünyalarını genişletmeye çalışan bireylere odaklanırken; süperpanoptikon ise kimliklerin bilgisayarlar tarafından nasıl oluşturulduğundan habersiz olan, dağınık ve parçalı kimliklere sahip nesneler ortaya çıkarmaktadır. Böylece, tekrar kaybolan bedenlerimizle baş başa kalırız. Ancak, postmodern gözetim bunu daha da öteye, kendilerinden ayrılmalarına, kimliklerin çoğalmasına ve her şeye rağmen verilerin oluşturduğu bireylerin yeniden birleştirebilmesine taşır. Poster'in de vurguladığı gibi, veri tabanlarına erişim yetkisine sahip bireyler ve organizasyonlar, kimliklerin tanımlanmasını sağlayan pozisyonlarda yer almaktadır (Poster, 1996: s. 188). Bu yüzden oluşturulan kimlikler, Baudrillard'ın 'hiperrealite' "hipergerçeklik" adını verdiği bir tür simülasyonla karşı karşıya kalmaktadır. Böylece bireyler, varlıklarının yeni formlarına sahip olmaktadır.

1.2.2. Sinoptikon

Bu kavram, literatürde ilk defa 1997 senesinde Norveçli sosyolog Thomas Mathiesen tarafından ortaya konmuştur. Sinoptikon, çoğunluğun azınlığı izlemesi anlamına gelmektedir ve oldukça yeni bir süreci ifade etmektedir. Sinoptikon modelinde bireyler, bulundukları yerden koparılmadan sanal ortama çekilmekte ve başkalarının hayatını gözetlemektedirler. Böylece sinoptikonun işleyiş biçimi yeni bir formda ortaya çıkmaktadır" (Kütükoğlu, 2021: s. 120).

İletişim literatüründe kitle iletişim araçları olarak ifade edilen ögeler, sinoptikon modelinin ana unsurları arasında yer almaktadır. Farklı yaşlardan, statülerden, cinsiyetlerden ve kültürel yapılardan gelen bireyler, *kültür endüstri*sinin ürettiği aynı mesajlara maruz kalmaktadır. Bu mesajlar ise çoğunlukla ünlüler, önemli şahsiyetler ve kurgusal ya da gerçek olaylar gibi unsurları içermektedir (Akt. Öztürk, 2013: s. 140).

Sinoptikon esas olarak görsel medya araçlarıyla hayata geçirilmektedir. Panoptikon ve süperpanoptikonun aksine başka bir gözetleme türü olan sinoptikon, panoptikonun tam zıttı bir şekilde işlemektedir. Burada *çoğunluk, azınlığı izlemekte* ve onların davranışlarını kendi yaşamlarına yansıtarak kendilerini onlarla özdeşleştirmektedir. Sinoptikon modelinin temelinde radyo ve televizyon gibi araçlar yer almaktadır (Demir, 2017: s. 60).

Bu açıklamalara bakıldığında, "Survivor", "Big Brother", "Gelinim Olur Musun?" ve "Biri Bizi Gözetliyor" gibi reality show formatındaki televizyon programları, sinoptikon modeline en iyi örnekleri oluşturmaktadır. Bu programlarda, insanlar yer değiştirmeden başkalarının yaşamlarını izlemektedir.

Ayrıca, internet üzerinden yapılan tüketici gözetimi, özellikle dünyanın varlıklı bölgelerinde hızlı bir şekilde yayılmaktadır. Tüketici toplumu içinde daha fazla yer almak isteyen her birey, özellikle online alışverişlerde, gönüllü olarak izinsiz bir gözetim sürecine maruz kalmaktadır. Dünyanın daha fakir bölgelerinde kitlesel medyanın umulduğu kadar fazla bir etkisinin olmamasıyla birlikte, kapitalist sistemin devamının sağlanması için önemli olan kültürel-ideolojik işlemlerini kuvvetlendirmek için daha etkili metotlar kullanılmaktadır.

1.2.3. Omniptikon (Ban-optikon)

"Omniptikon" olarak da bilinen "ban-optikon" terimi, gözetim modellerinin evriminde ulaşılan nihai evreyi ifade eder. Rosen'in yaklaşımına göre bu kavram, dijital iletişim çağında kimin gözetleyen, kimin gözetlenen konumunda olduğunu ayırt etmenin güçleştiği bir ortamda, bireylerin birbirlerini karşılıklı olarak izlediği yoğun bir gözetim ilişkisini ifade eder. Bu bağlamda omniptikon, siber uzamda bireylerin sürekli ve karşılıklı biçimde gözetim faaliyeti yürüttüğü bir düzeni betimlemektedir. Değişen gözetim pratiklerinin doğasından hareketle, gönüllü katılım yoluyla şekillenen bir yapıya sahiptir. Geleneksel panoptikon modelinde iktidarın yerel ölçekte gözetim ve denetim işlevi ön planda iken, sinoptikon evresinde bu yapı tersine dönerek, geniş kitlelerin sınırlı sayıdaki bireyleri izlemesi söz konusu olmuştur. Teknolojik gelişmelerin etkisiyle bu

evreyi, bireylerin karşılıklı olarak birbirlerini izleyebildiği ve gözetimin yataylaştığı omniptikon aşaması izlemiştir (Akt. Bitirim-Okmeydan, 2017: s. 61).

Kocabay-Şener'e göre, sosyal ağlardaki gözetim şekli omniptikon modeliyle açıklanmaktadır (Kütükoğlu, 2021: s. 122). Binark'a göre, bu model kapsamında bireylerin yaşamları; Facebook, Instagram ve X (eski adıyla Twitter) gibi sosyal medya platformları üzerinden sürekli olarak izlenmektedir. Bentham'ın zihninde şekillenen, Foucault tarafından akademik alana taşınan ve Orwell'in distopik bir versiyon olarak kurguladığı panoptik toplum, 21. yüzyılda dijital ortama taşınmıştır (Kütükoğlu, 2021: s. 122).

Panoptikonda gücü elinde bulunduran otorite gizli kalırken, omniptikon modelinde bu belirsizlik bir kat daha artmış ve kendisini daha iyi saklamayı başarmıştır. Panoptikonda baskı temelli gözetim hakimken, omniptikon düzeninde ise bireylerin isteyerek ve memnuniyetle katıldığı bir gözetim biçimine dönüşmüştür.

Alışveriş merkezleri ve güvenlikli siteler gibi halka açık alanları saran kameralar, ban-optikon cihazlarına örnektir. Bu cihazlar, sisteme uyum sağlamakta isteksiz olan bireyleri tespit etmektedir. Ban-optikon modeliyle, otoriteler merkezi gözetimin zorluklarını ortadan kaldırmayı başarmaktadır. Ban-optikonun bağımlısı haline gelen bireyler, tıpkı "Bin Dokuz Yüz Seksen Dört", "Cesur Yeni Dünya" ve "Biz" gibi romanlarda olduğu gibi, birbirlerini izlemeye dayalı bir düzen kurmuşlardır. Bu gelişme, özel hayatın kamusallaşması, parçalanması ve ifade özgürlüğünün kısıtlanması sonucunu doğurmuştur (Kütükoğlu, 2021: s. 122-123).

Sosyal medya ve iletişim teknolojileri sayesinde herkes birbirini görebilmekte, izleyebilmekte ve takip edebilmektedir. İletişim teknolojileri, yalnızca haberleşme şekillerini değil, aynı zamanda gözetim alışkanlıklarını da dönüştürmüştür. Eskiden yalnızca yerel ve tek yönlü gerçekleşen gözetim, özellikle sosyal medya sayesinde küresel bir boyuta taşınarak herkesi içine alan bir yapıya dönüşmüştür. Artık, gözetleme süreci tüm bireyleri kapsamaktadır.

İKİNCİ BÖLÜM

2. SOSYAL MEDYA VE MAHREMİYET YÖNELİMLERİ

2.1. Sosyal Medya Kavramına Genel Bakış

Toplumsal yapılar, iletişim süreçlerinin evrimi doğrultusunda dört büyük devrimsel aşamaya tanıklık etmiştir. Bell (2001: s. 309), bu devrimleri konuşma, yazı, matbaanın icadı ve telekomünikasyon olarak tanımlamaktadır. Her bir devrim, kendi dönemine özgü yeni yaşam tarzları ortaya çıkarmıştır. Vedder (2011: s. 23) ise, ilerleyen süreçlerde mevcut ve gelecek teknolojik atılımların dünyayı dönüştüren ve ileride de etkisini devam ettirecek üç ana faktörü olduğunu ifade etmektedir. Bunlar; sensörlerin ve bilgisayarların gelişerek küçülmesi, verilerin depolanması, iletimi ve işlenmesinin güçlenmesi, ayrıca kablosuz bağlantı imkânlarıyla şebekelerin yaygınlaşmasıdır.

Bu değişim sürecinin ilk aşaması "Web 1.0" olarak adlandırılmaktadır. Ardından, içeriğin kullanıcılar tarafından oluşturulmaya başladığı Web 2.0 çağı başlamıştır. "Web 2.0" kavramı, 2004 yılında Tim O'Reilly (2005) tarafından gündeme getirilmiştir. Web 2.0'ın öne çıkan özellikleri arasında; "güvenin radikal şekilde yeniden tanımlanması, merkeziyetçiliğin azalması, kullanıcıların aktif katılımı, sadece yayın yerine etkileşim, zengin kullanıcı deneyimi, verilerin kullanıcı tarafından kontrol edilmesi, verilerin yeni bileşimlerle sunulabilmesi, web'in bir platform olarak kullanımı, kolektif zeka, esnek tutumlar, oyunlaştırma, daha fazla kullanıcıyla daha iyi yazılımlar geliştirme ve öngörülemeyen kullanıcı davranışları" gibi unsurlar yer almaktadır (Fuchs, 2014: s. 50). Web 2.0 dönemi ayrıca Wikipedia gibi bilgi kaynaklarının, sosyal paylaşım sitelerinin, blogların ve dosya paylaşım platformlarının ortaya çıkışını simgelemektedir (Shcherbina, 2017: s. 86-87).

Web 2.0 teknolojisi sayesinde ortaya çıkan sosyal medya, son yirmi yılda hızla ilerleyen ve önemli bir yapı haline gelen bir olgudur (Boyd ve Ellison, 2007: s. 210). Günümüzdeki bu hızlı yükseliş, sosyal medyanın birçok insan için temel bir iletişim aracı olduğunu açıkça göstermektedir. Ancak, sosyal medyanın temel bir iletişim aracı olarak benimsenmesi, her zaman tamamen olumlu sonuçlar doğurduğu anlamına gelmemektedir.

Çevrimiçi platformlar, yani internet, kamusal ve özel alanlar arasındaki sınırları ortadan kaldırma ya da en azından yeniden şekillendirme ve "sosyal yaşamın iklimini dönüştürme" potansiyeli taşımaktadır (Meyrowitz, 1986: s. 6). Bu nedenle sosyal medya, mahremiyet ile kamusallığın birbirine geçtiği hem özel hem de toplumsal bir alanı temsil eder. Sosyal medya sayesinde mahremiyetin hem biçimi hem de kapsamı değişmiştir. Örneğin, sosyal medya sayesinde, önceden var olmayan ve yüz yüze ilişkilerin dışında kalan yeni bir mahremiyet türü ortaya çıkmıştır (Timisi, 2003: s. 170). Dolayısıyla sosyal medyanın kullanımı ve yaygınlaşması, mahremiyetin tartışmalı bir konu haline gelmesine neden olmuştur. Bu noktada, kişilerin kendilerine ait bilgileri yönetme ve akışını kontrol etme hakkı en önemli meselelerden biri haline gelmiştir. Bu bağlamda, kendi bilgilerini kontrol edemeyen bir bireyin mahremiyetini koruyabilmesi neredeyse imkânsız hale gelmektedir.

2.2. Sosyal Ağlar

Gerçekte, sosyal ağ kavramı yalnızca internet çağında ortaya çıkan bir olgu değildir. Çok eski zamanlarda bile insanlar sosyal yapılar kurmuşlardı. İnsanlar öteden beri toplumsal bir yaşam sürdürmüş ve hayatta kalabilmek için diğerleriyle bağlantı kurmuşlardır. Ancak kapitalizmin yeniden şekillenmesi ve bilgi teknolojilerindeki devrim, yeni bir toplumsal düzeni, yani *ağ toplumu*nu meydana getirmiştir (Castells, 2006: s. 3). Ağlar, sınırsız şekilde büyüyebilme kapasitesine sahip, ortak iletişim kuralları (örneğin, değerler veya başarı hedefleri) doğrultusunda yeni düğümlerle birleşebilen açık sistemlerdir. Ağ temelli toplumsal yapı, dengeyi kaybetmeden yenilikleri kabul edebilen, son derece açık ve hareketli bir sistem olarak tanımlanabilir (Castells, 2008: s. 623).

Yeni iletişim teknolojileri ve sosyal ağların hızla geliştiği günümüzde bireyler, sahip oldukları yerel ve kültürel kodların yerine giderek daha fazla küresel kültürün normlarını ve değerlerini benimsemektedir. Bu dönüşüm süreci; yaşam tarzı, aile yapısı, dil ve inanç sistemleri, tüketim alışkanlıkları, eğlence biçimleri, düşünsel kalıplar, toplumsal cinsiyet ilişkileri ve giyim anlayışı gibi pek çok alanda, özellikle genç kuşaklar arasında kültürel benzeşmeyi beraberinde getirmektedir. Bu kültürel benzeşmenin temel nedenlerinden biri ise küreselleşme olgusudur. Küreselleşmenin bu kadar hızlı ve etkili bir biçimde toplumsal yaşamı şekillendirmesinde iletişim teknolojileri ve sosyal ağların belirleyici rolünü unutmamak gerekir (Aktaş ve Çaycı, 2013: s. 10).



Şekil 2. *1 Dakikada İnternette Neler Oluyor?*

Kaynak: https://www.guvenliweb.org.tr/galeri-detay/internette-1-dakikada-neler-oluyor , Erişim tarihi: 25.05.2025

Bu görsel, 2020 yılında internette sadece bir dakikada gerçekleşfen inanılmaz yoğunluktaki aktiviteleri özetlemektedir. Grafik, dijital çağın ne kadar hızlı ve yoğun bir akışa sahip olduğunu açıkça ortaya koymaktadır. 1 dakikada Google'da 4,1 milyon arama sorgusu, WhatsApp ve Facebook Messenger'den 59 milyon mesaj gönderimi ve 4,7 milyon YouTube videosu izlenmesi gibi istatistikler, modern dünyanın dijitalleşme boyutunu çarpıcı biçimde göstermektedir. Ayrıca Netflix'te 764.000 saatlik içerik izlenmesi ve Instagram'da 694.444 akış paylaşımı gibi sayılar da, sosyal medyanın ve içerik platformlarının ne kadar önemli hale geldiğini kanıtlamaktadır. Bu tür veriler, hem kullanıcıların dijital alışkanlıklarını hem de veri güvenliği ve mahremiyet konularındaki hassasiyetleri düşünmemiz için önemli bir hatırlatma niteliğindedir.

Sosyal ağların mahremiyetle bağlantısını incelerken, öncelikle bu ağların gerçekten bir topluluk olup olmadığı sorusu gündeme gelir; bunun hemen ardından ise kullanılan araçların ortaya çıkardığı tehlikelere dair farkındalık önem kazanır. Postman'ın (1994: s. 174) vurguladığı gibi, kullanıcılar eğer araçların doğurabileceği tehditlerin farkında değilse veya bunları kavrayamıyorsa, o araçlar kullanıcı için bir tehlike gibi görünmemektedir. Kullanımın olduğu her durumda kötüye kullanım ya da istismar

ihtimali de mevcuttur (Bauman, 2001: s. 12). Bu bağlamda, sosyal ağların yapısı; kullanıcıların sürekli olarak kişisel bilgilerini ve görsellerini paylaşmaya yönlendirilmesi, mesajlarla sürekli bildirim almaları ve teşhirci ya da gözetleyici bir katılım çağrısıyla karşı karşıya kalmaları gibi özelliklerle şekillenmektedir.

Bu noktada, sosyal ağlarda üç temel mahremiyet sorunsal karşımıza çıkmaktadır. İlki, bireylerin kendi özel bilgilerini paylaşmalarıdır. İkinci sorun, kullanıcıların kendi sosyal ağ sayfalarında başkalarına ait içerikleri paylaşmalarıyla ilgilidir. Üçüncü mahremiyet sorunu ise diğerlerinden farklı bir boyuttadır ve esasen bireylerin çevrimiçi ortamda sürekli olarak izlenmesiyle ilgilidir. Bu durum, kullanıcıların tüm geçmiş hareketlerinin -örneğin, internetteki gezinme alışkanlıkları ve eski paylaşımları gibi- veri tabanlarında kalıcı bir şekilde saklanması sonucunu doğurmaktadır (Nissenbaum, 2009: s. 59-63). Bu gibi mahremiyet risklerini azaltmak için çevrimiçi mahremiyetin korunmasına ve kişisel kimlik yönetimine yönelik çeşitli yöntemler geliştirilmektedir. Ayrıca, Electronic Frontier Foundation (EFF) gibi bu alanda çalışan ve kullanıcıların dijital haklarını korumayı hedefleyen birçok kuruluş bulunmaktadır (Karaarslan vd., 2014: s. 191). Ancak, çevrimiçi mahremiyetin sınırlarının belirsizliği nedeniyle, bu yaklaşımların tümünün etkili sonuçlar vereceğini söylemek pek mümkün olmamaktadır. Dahası, günümüzde sayısı giderek artan pek çok sosyal ağın varlığı, mahremiyetin korunmasını daha da karmaşık bir hale getirmektedir. Ancak bunların birçoğu zamana karşı dirençsiz kalmaktadır. Buna karşın, zamana karşı dirençsiz olmanın tersine, gün geçtikçe daha çok yaygınlaşan ve popülerleşen Facebook, Instagram, X, YouTube, LinkedIn gibi ağlar ön plana çıkmaktadır.

Sosyal medya artık günlük yaşantımızın vazgeçilmez bir parçası haline geldi. İş dünyasında ya da kişisel yaşamlarımızda, kimimiz bu platformları sıkça, kimimiz ise neredeyse sürekli olarak kullanıyoruz. Hayatımızı daha keyifli ve verimli hale getiren en popüler sosyal ağlar arasında şunlar yer alır:

Facebook

Günümüzde en çok bilinen sosyal ağlardan biri olan Facebook, 2004 yılında Harvard Üniversitesi öğrencileri Mark Zuckerberg, Dustin Moskovitz, Chris Hughes ve Eduardo Saverin tarafından geliştirilmiştir (Fuchs, 2014: s. 212). Başlangıçta yalnızca Harvard Üniversitesi öğrencilerine özel olarak tasarlanan Facebook'a, sadece harvard.edu uzantılı e-posta adresine sahip olanlar kayıt olabiliyordu. Web 2.0 dönemi zamanla

Facebook, politikasını değiştirerek diğer üniversite e-posta adreslerini de kabul etmeye başladı. 2005 yılına gelindiğinde ise Facebook, lise öğrencilerinden profesyonel ağlardaki çalışanlara kadar pek çok farklı kullanıcıyı kucaklayacak şekilde yaygınlaştı.

Bugün Facebook, dünya genelinde 1,7 milyar kullanıcısı ile dev bir sosyal ağ haline gelmiştir. Türkiye'de ise 50 milyon kişinin kullandığı bu platform, her geçen gün artan kullanıcı sayısıyla değerini de sürekli yükseltmektedir (Ercan, 2019: s. 27). Facebook, iş arkadaşları ve akrabalar arasındaki iletişimi güçlendirirken; markaların müşterileriyle dijital ortamlarda bağlantı kurmasına, itibar kazanmasına ve müşteri memnuniyetini artırmasına yardımcı olmaktadır.

Facebook, sahip olduğu yüksek kullanıcı sayısı, dünya genelinde yaygınlaşması ve sürekli gelişerek yeni kullanım alanları oluşturması nedeniyle diğer sosyal medya platformlarına göre daha çok ilgi çekmektedir (Toprak vd., 2014: s. 37-38).

Kullanıcılar, farklı nedenlerle Facebook'a erişim sağlamaktadır. Bu nedenler arasında; fikirlerin, fotoğrafların, videoların ve müziklerin paylaşılması, oyun oynama, alışveriş yapma, etkinlik düzenleme gibi eylemler yer almaktadır (Toprak vd., 2014: s. 44). Ayrıca arkadaşlarla iletişim kurma ve bağlantı sağlama gibi motivasyonlar da bulunmaktadır (Van Dijk, 2016: s. 134). Facebook gibi platformların öne çıkmasındaki başlıca etkenlerden biri, web sayfaları, e-postalar, dijital görseller ve videolar, tartışma forumları, bağlantı dizinleri ile arama motorları gibi çok sayıda medya, bilgi ve iletişim teknolojisini tek bir bütünlük içinde bir araya getirmeleridir (Fuchs, 2014: s. 15).

Facebook, kullanıcılarına kişisel profilleri aracılığıyla kendilerini ifade etme ve tanıtma olanağı sağlamaktadır. Profillere eklenen bilgiler, kişinin kendini nasıl göstermek istediğine dair bir kimlik paketini yansıtır (Gardner ve Davis, 2013: s. 81-82). Başka bir deyişle, kullanıcılar Facebook üzerinde çeşitli kimlik inşalarına yönelir. Profil fotoğraflarından paylaşılan diğer görsellere ve kişisel bilgilere kadar yaptıkları tüm paylaşımlar, onların kimliklerini sergilemelerine ya da oluşturmalarına yardımcı olur (Toprak vd., 2014: s. 109).

Bunun yanı sıra, kullanıcılar paylaşımlarının kimler tarafından görüntülenebileceğine ve dijital kimliklerinin nasıl sunulacağına dair seçim yapma hakkına sahiptir. Ancak bu hak her zaman sınırsız değildir. Mesela, Facebook bazı durumlarda profil fotoğrafı olarak grup resmi yerine farklı bir görsel kullanılmasını

önerebilmektedir. Bu kapsamda, profil fotoğrafı yerine farklı bir resim ya da görüntü seçmek, bireylerin mahremiyetini koruma çabası olarak değerlendirilebilir. Yine de, kullanılan farklı görsellerin de bireyin kimliğine dair izler barındırabileceği unutulmamalıdır. Bu nedenle Stefanick (2011: s. 184), Facebook'un yalnızca çevrimiçi iletişimin tarzını değil, aynı zamanda kişisel kimliğin anlamını ve değerini de dönüştürdüğünü ifade etmektedir.

Facebook, günümüzün bir yansıma alanı olarak kendimizi göstermek istediğimiz bir platformdur. Burada asıl önemli olan şey, paylaşılanların ya da gösterilenlerin gerçek olup olmaması değil, bunların sergilenmesidir (Çoban, 2014: s. 303-304). Bu sebeple Facebook, dijital röntgenciliği teşvik etmekte ve toplumsal gözetim ile elektronik panoptikon gibi denetim mekanizmalarının amaçlarına hizmet etmektedir (Kabir, 2014: s. 296). Kapitalist bir şirket olan Facebook'un temel hedefi maddi kazanç elde etmektir. Bu yüzden milyonlarca kullanıcının kişisel verilerini toplamakta, analiz etmekte, karşılaştırmakta ve ticari amaçla satmaktadır (Fuchs, 2014: s. 226). Dolayısıyla, gözetimin değer kazanması gibi süreçler, Facebook gibi şirketlere büyük kazançlar sağlamaktadır.

Facebook'ta kullanıcıların paylaştığı ilk bilgiler, genellikle cinsiyet, doğum tarihi, memleket, aile üyeleri ve ilişki durumu gibi "temel bilgiler"den oluşur (Toprak vd., 2014: s. 124). Bu temel veriler, kullanıcıyı genel anlamda tanımlamak için yeterlidir. Özellikle cinsiyet ve ilişki durumu gibi seçenekler, özel hayatın kamusal alana taşınmasında önemli bir rol oynar. "İlişki durumu" seçenekleri –örneğin "bekâr, ilişkisi var, nişanlı, evli, medeni birliktelik içinde, beraber yaşadığı biri var, karmaşık ilişki, ayrı, boşanmış, dul" gibi ifadeler– bireyleri özel yaşamlarını açıkça paylaşmaya yönlendirmektedir (Livberber, 2018: s. 105-106).

Sonuç olarak, Facebook gibi sosyal ağlar sayesinde toplumsal etkileşim, herkesin erişebileceği kamusal bir zemine taşınmıştır. Günümüzde Facebook; etkinliklerin organize edilmesi, belgelenmesi ve yaşanan deneyimlerin paylaşılması için yaygın olarak kullanılan bir platforma dönüşmüştür (Gardner ve Davis, 2013: s. 106). Bununla birlikte, sosyal medya araçları yalnızca sosyal ilişkileri dönüştürmekle kalmamış, bu dönüşüm sürecini halen sürdürmektedir. Örneğin, evli kişilerin Facebook üz erinden kurdukları ikincil ilişkiler, geleneksel aldatma biçimlerinin değişmesine neden olmuştur. Facebook'un kimi zaman boşanma, evlilik, intihar, cinayet ve işe alım gibi önemli

kararları ya da dolandırıcılıkları etkileyebilecek kadar güçlü olduğu görülmektedir. Her ne kadar mahremiyet, özel yaşamın ve gizliliğin bir boyutu olarak tanımlansa da (Giddens, 2014: s. 126), Toprak ve arkadaşlarının (2014: s. 162-163) gerçekleştirdiği bir çalışmada, Facebook kullanıcılarına mahremiyete ilişkin görüşleri sorulmuş ve katılımcıların büyük çoğunluğunun Facebook'ta özel alanlarının bulunmadığını düşündükleri ortaya konmuştur. Bu durum, kullancıların Facebook'u kullanırken özel yaşam alanlarının ortadan kalktığının farkına vardıklarını ortaya koymaktadır.

Facebook, hem bilgi akışı hem de bireysel özerkliğin korunması açısından büyük bir etkiye sahiptir (Stefanick, 2011: s. 159). Bu nedenle, Facebook'un gizlilik politikası mahremiyet sınırlarını farklı yönlerden tanımlayan önemli bir unsur haline gelmiştir. Dolayısıyla, bu politikayı detaylıca incelemek oldukça önemli ve neredeyse zorunlu hale gelmiştir.

Kısacası, Assange ve ekibinin (2013: s. 52-95) ifade ettiği gibi, verilerin üçüncü taraflarca nasıl kullanılacağı ve hangi amaçlarla işleneceği konusunda ciddi bir gizlilik sorunu bulunmaktadır. Bilgilerin kimler tarafından görülebileceğine dair yapılan tüm ayarlamalara rağmen, paylaşım butonuna basıldığında veriler önce Facebook'a, sonra da paylaşılan kullanıcı grubuna ulaşmaktadır. Bunun da ötesinde, para aklama, uyuşturucu kaçakçılığı, terörizm ve çocuk istismarı gibi "mahşerin dört atlısı" olarak adlandırılan suç türleri, gizliliği koruyan teknolojilerin bastırılması için sürekli bir gerekçe olarak öne sürülmekte ve kullanıcı bilgileri denetim altına alınmaktadır. Bu durumun temelinde, denetim arttıkça kontrolün de aynı ölçüde güçlenmesi yatmaktadır.

Instagram

Kevin Systrom ve Mike Krieger tarafından 2010 yılında geliştirilen Instagram, 2012 yılında Facebook çatısı altına katılmıştır. Başlangıçta sadece iOS işletim sistemine sahip cihazlarda kullanılabilen uygulama, 2012'den itibaren Android cihazlarda da hizmet vermeye başlamıştır (Cılızoğlu ve Çetinkaya, 2016: s. 169). Fotoğraf çekme ve paylaşma alanında en popüler platformlardan biri olan Instagram (Hu, Manikonda ve Kambhampati, 2014: s. 595), akıllı telefonlardan erişim özelliği ve Facebook'un satın alması sonrası değerini 35 katına çıkarmasıyla dikkat çekmiştir (Tutgun, 2015: s. 55). Ayrıca, yılda 100 milyonu aşan büyüme oranıyla 600 milyondan fazla kullanıcıya ulaşmıştır (Statista, 2017).

Facebook'un satın almasıyla birlikte hızla yükselen Instagram, kullanıcı sayısını dünya çapında kısa sürede katlamıştır. Fotoğraf paylaşımı alanında ön plana çıkan platform, video özelliği eklemesiyle Twitter'a ait Vine uygulamasının neredeyse ortadan kalkmasına yol açmıştır. Fotoğrafın evrensel dili nedeniyle geniş bir kullanıcı kitlesi tarafından benimsenen ve beğenilen Instagram, bugün dünyada en yaygın kullanılan fotoğraf paylaşım aracı haline gelmiştir (Ercan, 2019: s. 28).

Instagram, filtreler yardımıyla hazırlanan fotoğraf ve videolar aracılığıyla, kullanıcıların yaşamlarındaki anları yakalayıp paylaşmalarını sağlayan bir platformdur. Diğer sosyal ağlardan genç ve çeşitli bir kitleye ulaşan Instagram, yapılan araştırmalarda kullanıcıların burayı gerçek hayattan bir kaçış aracı olarak kullandıklarını ve daha önce hiç karşılaşmadıkları insanlarla etkileşim kurduklarını göstermektedir (Lee vd, 2015: s. 555).

Instagram'da mahremiyetle kamusal alan arasındaki sınırın belirsizliği, farklı örneklerle kendini göstermektedir. Bunun tipik bir örneği, emzirme fotoğraflarına dair tartışmalardır. Locatelli'nin (2017: s. 3) aktardığına göre, doğum fotoğrafçısı Heather Bays'in, kızını emzirdiği bir fotoğrafın olumsuz yorum almasının ardından hesabı kapatılmış; ancak Bays'in tepkisi sonrası profil tekrar açılmıştır. Instagram, bu noktada diğer kullanıcılara karşı hassasiyet gösterilmesini isteyerek emzirme fotoğraflarını platformdan kaldırmıştır. Ancak bu ikinci sansür girişimi de tepkiyle karşılanınca, Instagram 2015 yılında politikasını değiştirerek -çıplaklık içermediği sürece- emzirme ve mastektomi izlerini paylaşmaya izin vermiştir. Böylelikle, emzirme fotoğrafları kadın bedeniyle ilgili kültürel ve estetik normlara, ayrıca sosyal medyada nelerin paylaşılabileceğine dair algılara meydan okumuş ve kamusal ile mahrem alan arasındaki sınırları yeniden tanımlamaya başlamıştır. Locatelli'nin çalışması, kullanıcıların çeşitli etkenlere verdikleri tepkilerin mahremiyet ve kamusal alanın algılanışını nasıl etkileyebileceğini göstermektedir. Instagram'da emziren kadınların fotoğraflarını paylaşmaları ya da emzirme anlarını kamuya açık hale getirmeleri, bu eylemi normalleştirerek emzirmenin görünürlüğünü artırmıştır. Bu nedenle, sürekli değişen kamusal ve özel alan sınırlarının net bir şekilde çizilemeyeceği anlaşılmaktadır.

Instagram'ın gizlilik politikası ise (Instagram, 04.01.2022) ağ üzerindeki mahremiyet sınırlarını net olarak ortaya koymamaktadır. Buna karşılık, "topladığımız bilgiler", "bilgilerinizi nasıl kullanıyoruz", "bilgilerinizin paylaşılması", "bilgilerin nasıl

saklandığı", "bilgilerinizle ilgili tercih haklarınız", "çocukların gizliliği", "diğer web siteleri ve servisler", "ölüm bildirimi", "iletişim" ve "gizlilik politikasındaki değişiklikler" gibi başlıklar yer almaktadır. Özellikle ilk beş başlık, mahremiyetin korunmasında temel öneme sahiptir ve bunların detaylarına bakmak yararlı olacaktır.

Bu başlıklar incelendiğinde, Instagram'daki içeriklerin anında paylaşılıyor olmasının yanı sıra, üçüncü şahıslarla ticari amaçla paylaşılma riskini de beraberinde getirdiği görülmektedir. Instagram'ın 2012'de Facebook'un bünyesine katılması nedeniyle, gizlilik politikalarının büyük ölçüde Facebook'unkilerle (Facebook, 14.11.2024) benzerlik taşıdığı söylenebilir. Bununla birlikte, Instagram'ın "bilgilerinizi nasıl depoluyoruz" başlığında, toplanan verilerin ABD'de ya da Instagram'ın, ortaklarının veya hizmet sağlayıcılarının bulunduğu ülkelerde saklanıp işlenebileceği açıkça ifade edilmektedir. Ayrıca, Facebook'ta yer almayan, hesap kapatıldığında ya da dondurulduğunda, içeriklerin yedeklenip arşivlenerek ticari gerekçelerle bir süre daha saklanabileceğine dair açıklamalar da mevcuttur. Bu ilkeler, kullanıcıların paylaştığı bilgilerin hiçbir zaman tamamen silinmediğini ve bir şekilde hep saklı kaldığını göstermektedir. Böylece, "unutulma hakkı" gibi bir hakkın Instagram için geçerli olmadığını ve bu nedenle tam anlamıyla mahremiyetten söz etmenin güç olduğunu ortaya koymaktadır (Livberber, 2018: s. 115).

X (Twitter)

Eskiden Twitter olarak bilinen X, 2006 yılında Jack Dorsey ve ortakları tarafından San Francisco'da kurulan ve "tweet" adını alan en fazla 280 karakterlik mesajlar paylaşmaya olanak sağlayan bir platformdur (Bayraktutan vd., 2012: s. 15; Rogers, 2016: s. 9). Twitter'ın çıkış noktası "yaygın bir şikayet mecrası" olmasının yanı sıra, hem kısa mesaj gönderme hem de kullanıcıların yararlandığı çeşitli iletişim hizmetlerine katkı sağlayacak bir yapı sunmaktı. Dolayısıyla, X (Twitter) başlangıçta bağımsız bir enformasyon aracı ve kamusal bilgi platformu olma hedefiyle geliştirilmiştir (Rogers, 2016: s. 10-11).

Toplumsal olaylar, gündem ve siyasi gelişmelerin tartışıldığı önde gelen sosyal medya mecralarından biri olan X, özellikle yazarlar ve siyasetçiler tarafından yoğun şekilde kullanılmaktadır. Aynı zamanda müşteri şikayetleri ve hak arayışı gibi konuların ele alınmasında da önemli bir rol oynamaktadır (Ercan, 2019: s. 28). Günümüzde X, dünya genelinde en çok tercih edilen sosyal ağlardan biri konumundadır. Türkiye'de en

sık ziyaret edilen platformlar listesinde 22. sırada yer almaktadır (Livberber, 2018: s. 115-116). Bu bağlamda, hem tek yönlü hem de karşılıklı bağlantılar kurulabilen X; haber alma, politika, iş dünyası, eğlence ve gündelik tartışmalar gibi pek çok alanda bir iletişim ve etkileşim alanı sunmaktadır.

X'te iletişimsel faaliyetler *üç temel katman*da toplanmaktadır: *mikro, mezzo* ve *makro*. *Mikro* katman, doğrudan kişilerarası iletişimi (@reply) içerir ve geçici bir niteliğe sahiptir. *Mezzo* katman, kişisel topluluklardan oluşan takipçi ağlarını kapsar; oluşumu zaman alır ve daha kalıcıdır. *Makro* katman ise #hashtag kullanımıyla ortaya çıkan, planlanmamış toplulukları ifade eder; hızla şekillenip hızla çözülür. Bu üçlü yapı, özellikle Facebook gibi diğer ağlardan X'i ayıran önemli bir özelliktir (Bruns ve Moe, 2016: s. 68-69). Bu yapı aynı zamanda içerik dolaşımı ve izleyici toplama biçimini de etkileyebilmektedir (Leavitt, 2016: s. 209).

Mahremiyet açısından bakıldığında, X kullanıcılarının gizlilik algılarını ve eğilimlerini incelemek önem arz etmektedir (Weller vd., 2016: s. 35). Schmidt (2016: s. 48, 55-56), Twitter gibi sosyal platformları "kişisel kamu" olarak tanımlamaktadır. Kişisel kamu, kamusal ve kişisel alanların iç içe geçmesini temsil ettiği için, mahremiyet ve kamusallık kavramlarını yeniden şekillendirmektedir. Örneğin, tatil anıları, aile aktiviteleri veya ruh hâli gibi özel kabul edilen bilgilerin paylaşımı "dijital teşhircilik" şeklinde yorumlanabilmektedir. Dahası, bu paylaşımlar kişiselleştirilmiş haber akışının bir parçasına dönüşmektedir.

Diğer yandan, Facebook gibi ağlarda oldukça detaylı gizlilik ayarları mevcutken, X kullanıcılara yalnızca iki seçenek sunmaktadır: ya tüm paylaşımlar herkese açık olur ya da belirli kullanıcılara görünür şekilde sınırlandırılır. Ayrıca X'te mahremiyet konusu güncel bir mesele olarak dikkat çekmektedir. Çünkü paylaşılan içeriklerin kısa ömürlü olması, kullanıcıların özel ve hassas bilgilerini paylaşma eğilimini artırabilmektedir. Ancak X'in sade gizlilik denetimi, tweetlerin kolayca paylaşılabilmesi ve platformun kamusal doğası, mahremiyet beklentisinin anlamsız olabileceği yönündeki tartışmaları da beraberinde getirmektedir (Zimmer ve Proferes, 2016: s. 243-248).

LinkedIn

Günümüzde LinkedIn, dünya çapında en çok tercih edilen sosyal ağlardan biri konumundadır (Livberber, 2018: s. 121). Kullanıcılar çevrimiçi profesyonel profiller oluşturarak iş ve okul arkadaşlarıyla iletişimde kalabilmekte, aynı zamanda yeni kariyer

fırsatları, iş ortaklıkları ve projeler keşfedebilmektedir. Kullanıcılar, eğitim geçmişi, iş deneyimleri ve yetkinliklerini LinkedIn üzerinden paylaşma imkânı bulmaktadır. Bu sayede LinkedIn, bireylerin geniş bir iş ağıyla bağlantı kurmasına olanak tanımaktadır (Uluç ve Yarcı, 2017: s. 90).

LinkedIn, neredeyse hiç sahte hesaba rastlanmayan, bu yönüyle en güvenilir sosyal platformlardan biri olarak değerlendirilebilir (Ercan, 2019: s. 28-29). Kurumlar, LinkedIn'i aktif şekilde kullanarak gerçek bir CV havuzu oluşturmakta ve yeni personel alımları gerçekleştirmektedir. Kullanıcılar, platformda genellikle resmi görünümleri ve kariyer odaklı paylaşımlarıyla yer almakta olup, aktif LinkedIn kullanıcıları iş yaşamında önemli avantajlar elde etmektedir. LinkedIn, iş dünyasında sosyal ticaret kategorisinde en fazla tercih edilen platformlardan biridir. Resmi olarak 2003 yılında hizmet vermeye başlayan LinkedIn'in merkezi Silikon Vadisi'nde bulunmakta ve dünya genelinde birçok ofisi vardır (LinkedIn Ofisi, 2025). Ayrıca LinkedIn, doğrudan bağlantılar dışında, ikinci ve üçüncü derece bağlantı kurma imkânı sunmaktadır. Bu özellik sayesinde kullanıcılar, henüz bağlantı kurmadıkları ancak dolaylı yoldan ilişkili oldukları kişilere ulaşabilir ve öneriler alabilirler. Bu mekanizma, üyelerin sosyal ağlarını büyütmelerine ve yeni profesyonel ilişkiler geliştirmelerine yardımcı olmaktadır.

LinkedIn'in gizlilik politikası (Gizlilik Politikaları, 2025) "Topladığımız Bilgiler", "Verilerinizi Nasıl Kullanıyoruz", "Bilgilerin Paylaşımı", "Tercihleriniz ve Yükümlülükleriniz" ile "Diğer Önemli Bilgiler" başlıkları altında toplanmıştır. Toplanan veriler arasında profil bilgileri, adres defteri, takvim, paylaşımlar ve kullanım bilgileri yer almakta; ayrıca çerezler ve konum bilgisi gibi detaylar da dâhildir. Bu veriler, LinkedIn'in hizmetleri olan SlideShare ve Pulse ile birlikte üçüncü taraflarla paylaşılabilmektedir. İlginç bir şekilde, bazı bilgiler hesap kapatılsa bile belirli bir süre saklanmaya devam etmektedir.

YouTube

YouTube (YouTube hakkında, 2025), "herkese sesini duyurma ve dünyayı tanıma fırsatı sağlama" misyonuyla 2005 yılında Jawed Karim, Chad Hurley ve Steve Chen tarafından kurulmuştur. Platformun temel amacı, televizyon içeriklerinin internet ortamında daha kolay erişilebilir olmasını sağlamaktır (Lister vd., 2009: s. 225). Başlangıçta "Your Digital Video Repository" (Dijital Video Deposu) sloganıyla yola çıkan YouTube, zamanla popülerlik kazandıktan sonra "Broadcast Yourself" (Kendin[i]

Yayınla) ifadesini kullanmaya başlamıştır (Burgess ve Green, 2009: s. 4). Bu değişim, YouTube'un ilk etapta yalnızca video depolama hizmeti vermek üzere tasarlandığını ancak ilerleyen süreçte içerik yayınlama işlevinin de ön plana çıktığını göstermektedir.

Günümüzde YouTube, dünya genelinde en çok tercih edilen sosyal medya platformlarından biri olma özelliğini taşımaktadır (Livberber, 2018: s. 119). Platform, kullanıcıların videolar aracılığıyla farklı düzeylerde sosyal etkileşim kurmasını sağlamakta ve geniş kapsamlı video paylaşımlarına olanak vermektedir. Ayrıca, kullanıcılarına "kanal sayfası" adı verilen kişisel profil sayfaları sunmaktadır (Boyd, 2006). Bu sayede bireyler, tek başlarına ya da arkadaş gruplarıyla birlikte çeşitli türlerde videolar hazırlayıp paylaşabilmektedirler. Özetle, YouTube kullanıcıları, çevrimiçi yorum yapma ve puan verme sistemleriyle içeriklerle ilgili düşüncelerini ifade edebilmekte, e-posta yoluyla videoların bağlantılarını paylaşabilmektedir. Sosyal bir platform olarak YouTube, kendini ifade etme, topluluk oluşturma ve kamuoyuna yönelik açıklama mekanizmalarının işlediği bir alan olarak değerlendirilmektedir (Strangelove, 2010: s. 4). Bu bağlamda, YouTube sadece yüksek trafik çeken bir internet sitesi olmayıp, aynı zamanda bir yayın platformu, medya arşivi ve sosyal ağ işlevi görmektedir (Burgess, 2009: s. 5).

YouTube, katılımcı bir kültürün parçası olan bir site olarak (Burgess, 2009: vii) dört temel özgürlük değer*i*ni ön plana çıkarmaktadır: ifade özgürlüğü, bilgi edinme özgürlüğü, fırsat özgürlüğü ve aidiyet özgürlüğü. Bu değerlerin nasıl uygulandığını anlamak açısından YouTube'un gizlilik politikası incelenmelidir. Google tarafından satın alınan YouTube, Google'ın gizlilik politikasıyla aynı kurallara tabidir. Diğer sosyal medya platformlarında olduğu gibi, cihaz bilgisi, günlük aktiviteler, konum bilgisi ve çerezler gibi çeşitli veriler toplanmakta, saklanmakta, işlenmekte ve üçüncü taraflarla paylaşılmaktadır. Ayrıca, YouTube'un politikalar ve güvenlik (YouTube, Politikalar ve Gizlilik, 2025) bölümünde; çıplaklık veya cinsel içerik, şiddet içeren veya rahatsız edici görseller, taciz ve siber zorbalık, spam, yanıltıcı meta veriler, dolandırıcılık, tehditler, gizlilik ihlalleri, kimlik taklidi, telif hakkı sorunları ve çocukların korunması gibi pek çok konuya dair açıklamalar yer almakta ve bu konularda hukuki yaptırımlar için kurumlarla iş birliği yapıldığı belirtilmektedir.

WhatsApp

Facebook'tan sonra dünya genelinde en yaygın kullanılan ikinci sosyal medya uygulaması olan WhatsApp, anlık mesajlaşma alanında rakiplerinin çok önünde yer almaktadır. 1.2 milyar aktif kullanıcısıyla, telefon görüşmelerinden bile daha sık tercih edilen bir uygulama haline gelmiştir. Ayrıca, görüntülü arama özelliğinin eklenmesiyle sunduğu hizmet kalitesi önemli ölçüde artırılmıştır (Ercan, 2019: s. 27-28).

Swarm

Foursquare mekan tanıtım işlerine girince check-in işleri Swarm'a kaldı ve Swarm ile istenilen her yerde check-in yapıp puan toplanabilmekte, mayor olunabilmektedir. Dünyanın birçok yerinde mayorluğun ayrıcalığı ve karizması farklıdır. Swarm ilgi çekmeye, mekanları puanlamaya devam etmektedir (Ercan, 2019: s. 28). Mayor olmak, bir mekanı en çok ziyaret eden kişi anlamı da taşımaktadır. Bu bağlamda Swarm kullanan kişiler arasında kıyasıya mayor olma yarışı bulunmaktadır.

Snapchat

Obama'nın başkanlığa veda videosu ile daha da popüler olmuştur. 24 saat içinde silinen mikro videolar ile bilinmektedir. 2 kişi arasındaki yazışmalar için ideal olan sosyal ağ, Türkiye'de diğer ülkelerdeki kadar ses getirmedi ama gençler arasında diğer sosyal ağlardan daha fazla kullanılmaktadır. Instagram'ın Snapchat'a benzer özellikler getirmesi, Snapchat'ın büyümesini biraz yavaşlatsa da, hala çekiciliğini korumaktadır (Ercan, 2019: s. 29).

Periscope

Twitter tarafından satın alınan Periscope, dünyanın ilk canlı yayın sosyal ağlarından biridir. Binlerce canlı takipçiye ulaşan yayınlar ile kısa sürede popüler hale gelmiştir. Facebook canlı yayın özelliğini devreye alsa da popülerliğini kaybetmemiştir (Ercan, 2019: s. 29).

TikTok

TikTok, kullanıcıların kısa videolar çekip paylaşabildiği bir sosyal medya platformudur. 2016 yılında Çinli teknoloji şirketi ByteDance tarafından kuruldu ve özellikle gençler arasında oldukça popülerdir. Kullanıcılar genellikle dans, şarkı, komedi ve eğlence temalı videolar oluşturur. TikTok'un algoritması, kullanıcıların ilgi alanlarına uygun içerikleri önerir ve bu sayede videoların hızla yayılmasına olanak tanır. "Sosyal

medyanın Çinli devi" olarak da adlandırılan bu platform, 2025 yılı itibariyle dünya genelinde 1,7 milyar aktif kullanıcıya sahip olduğu tahmin edilmektedir.

2.3. Tarihsel Düzlemde Mahremiyet Kavramı

Gözetim, çok yönlü bir olgudur. Bazıları için bu durum, işlerin yanlış gitmesi endişesiyle ilişkilidir. Özellikle kişisel veriler söz konusu olduğunda hatalar meydana gelebilir ve bu hatalar ciddi sonuçlar doğurabilir. Gözetleme, toplumların makul bulduğu her alanda hızla yaygınlaşmakta; bu durum, güvenlik ihlallerinin yaşanması ve kişisel bilgilerin kamusal alanda ifşa olması açısından şaşırtıcı değildir. Diğerleri için, mahremiyet sorunsalı, sistemler düzgün çalışırken bile en üstün konudur. Mahremiyet, bireysel detayların işlem görmesi söz konusu ise -en azından Batı'da-, herkesin aklına kolayca gelebilecek bir konudur. Bu da çok önemli olmakla beraber, mahremiyete gösterilen özen, gözetlemenin diğer boyutlarına gösterilen dikkati saptırabilir. Her şeyin ötesinde, mahremiyet, gözetlemenin, sosyal hayatın yaradılışında var olan bir meseleden, kişisel bir konuya indirgenmesine meyil verir (Lyon, 2006: s. 16).

Mahremiyet konusu, "yasaklanmış" anılarla birlikte insanlık tarihi kadar eskidir. Kutsal metinlerde yer alan Adem ile Havva'nın cennetten yeryüzüne inişi hikayesi, insanın günahla tanıştığı ve hem haram hem de özel sayılan bu sahnenin korunması gerektiğini gösterir (Gündoğan, 2019: s. 35). Batı dillerinde *privacy* kelimesinin kökeni Latince "privatus"tan gelir ve "özgür, ayrı tutulmuş" anlamındadır. *Privatus* sıfatı kişisel, özel ve gizli anlamlarını taşırken, isim olarak hem bireysel vatandaş hem de kamusal görevleri olmayan kişi anlamına gelir. Bu kelime, "ayrılmak, tecrit edilmek, kişiye ait olmak" gibi çağrışımlar taşır (Ernout ve Meillet, 2001).

Türk Dil Kurumu'na göre mahremiyet, gizlilik anlamındadır (TDK, 2019). Doğu kültüründe ise, özellikle İslami değerlerle şekillenen mahremiyet kavramı, Arapça "h-r-m" kökünden türemiştir ve hem yasak hem kutsal anlamlarını içerir. Mahremiyet, bir sınır çizme meselesidir ve bu yüzden kamusal ilişkiler ile hürriyet arasındaki bağlantıyı anlamak önemlidir (Şişman, 2019: s. 15). Modern bireyci mahremiyet anlayışı, Warren ve Brandeis'in 1890'da yayımladıkları makalede "yalnız kalma hakkı" olarak tanımlanmıştır (1890: s. 193). Vincent'in "Mahremiyet – Kısa Bir Tarih" adlı eserinde, mahremiyet kavramına dair modern çağdaki kişisel bilgilerin korunmasına yönelik tehditler ele alınmaktadır. 11 Eylül saldırılarının ardından, ABD liderlerinin belirttiği

gibi, dünya eskisi gibi olmamış ve devletler kamu güvenliği adına bireylerin ve sivil toplumun hayatına sınırsız müdahale hakkı kazanmıştır (Vincent, 2017: s. 7). Habermas (1989: s. 157-159) ise, modern gizlilik kavramının, özel ve kamusal alan ayrımına dayandığını belirtir. Ona göre gizlilik, yanıltıcı bir ideoloji olup gerçek anlamda tüketici topluluğunun bir parçasıdır.

Mahremiyet kavramı muhtemelen her kültürde var olmakla birlikte, değerlendirilişi tarih ve coğrafyaya göre değişiklik gösterir. Georges Duby'nin ifadesiyle (Lyon, 2006: s. 43), mahremiyet günlük yaşamda inziva ve rahatlama alanı olan "dokunulmazlık bölgesi"dir. Bu alan çoğunlukla ev içi olup, sadece yalnızlık değil daha fazlasını ifade eder. Modern Batı toplumunda kamusal ve özel alan ayrımı, toplumsal kimliklerin yerini de yansıtır; kadınlar daha çok özel alanla, erkekler ise kamusal alanla ilişkilendirilmiştir. Bu durum, erişimdeki eşitsizlikleri kavrama dahil eder. Benzer şekilde "özel mülkiyet" kavramında da sınır ihlali ve kanun karşıtlığı yasaklanmıştır. Kamusal ve özel alan ayrımı, modern şehirlerin anonim ve kişisel olmayan ilişkilerinin artışıyla yakından ilgilidir (Giddens, 1992: s. 152).

Özellikle Amerika'da mahremiyet büyük önem taşımaktadır. En azından bu ülkede mahremiyet arzusunun gözetim uygulamalarına zemin hazırladığı söylenebilir. Steven Nock'a göre, yabancıların oluşturduğu toplum, mahremiyete dayalıdır çünkü yabancıların bireylerin özel alanlarına erişimi sınırlandırılmıştır. Örnek vermek gerekirse, bir alışveriş işlemi sırasında yabancılar, ödeme gücünü ve güvenilirliği gösteren bir işaret talep ederler. Ancak eğer yabancı ya da kurum, sürekli ilişki kurduğu kişilerin itibarını, kimlik bilgilerini ve güvenilirliklerini birebir doğrulama imkanına sahip değilse, kimin güvenilir olduğu konusu belirsiz kalmaktadır (Lyon, 2006: s. 45).

Mahremiyet genel olarak *üç temel* türde ele alınabilir: Bireyin çevresini koruyan fiziksel alanı kapsayan *mekansal mahremiyet*, bireylerin haksız müdahalelerden korunması anlamına gelen *bireysel mahremiyet* ve özel bilgilerin toplanması, saklanması, işlenmesi ve paylaşımına ilişkin denetimin bireylere ait olduğu *enformasyon mahremiyeti* (Dolgun, 2015: s. 201).

Mekansal Mahremiyet

Mekan, insanın sınırlarını belirleyip çevresinden ayıran bir alan iken, mekansal mahremiyet ise bireyi çevreleyen ve koruyan bir boyuttur. Karakaya'ya göre mahremiyet, bireyin özel alanı ile kamusal alan arasında belirlediği mesafedir (2019: s. 67). Bu nedenle

mahremiyetin tanımlanması ve sınıflandırılmasında hem zaman hem de mekan kritik bir rol oynamaktadır. Antoine Prost, özel hayatın zamanın başlangıcından beri var olan doğal bir gerçeklik olmadığını; aksine, toplumdan topluma farklı şekillerde inşa edilen tarihsel bir olgu olduğunu ifade etmektedir (Rizanaj, 2020: s. 127).

Foucault, panoptikon tasarımını anlatırken, görünmeden gözetim sağlamaya olanak veren düzenlemeyi ve sürekli görme ile tanımaya izin veren mekansal birimleri açıklar. Hücre ilkesinin üç temel kuralı -kapatma, ışıktan mahrum bırakma ve gizleme- tersine çevrilmiştir. Artık yalnızca koruma unsurundan biri uygulanırken diğer iki unsur kaldırılmıştır. Tam ışık altında bulunmak ve gözetmenin sürekli bakışı, karanlıkta korunmaktan çok daha etkili bir denetim aracıdır çünkü görünürlük bir tuzak işlevi görür (Foucault, 1995: s. 200-201). Burada görünürlük, iktidarın bedeni kontrol altına almasını sağlar ve bu yönüyle Sartre'nin bakış fenomenine benzetilebilir. Günümüzde dünya, daha geniş bir panoptikon haline dönüşebilecek mekansal bir yapıya doğru evrilmektedir. Bu dönüşümde, özel ve kamusal alan kavramlarının tarihsel değişimi de göz önünde bulundurulmalıdır. "Görülmüş olma" durumu artık sadece kamusallıktan mahrum olmamak anlamına gelmemekte, bunun yerine denetim ve iktidar kurmanın bir aracı haline gelmiştir. Mahrem alanın gizliliği, kapalı oluşu ve dış müdahaleye kapalı olma özellikleri, modern panoptikonlarla birlikte giderek yok olmaktadır. Bu durum, mahremiyetin kaybının bir yönünü göstermektedir (Gündoğan, 2019: s. 41). Ayrıca siber dünya, sanal ve dijital çokluk ile fazlalığın mekânı olarak tanımlanmaktadır.

Bireysel Mahremiyet

Bireysel mahremiyet bağlamında bir diğer önemli husus da, kişinin mahremiyetinin ne ölçüde kendi istek ve tercihleri doğrultusunda şekillendiği konusudur. Bu noktada, mahremiyetin yalnızca kişisel tercih ve isteklerle belirlenemeyeceği; farklı iktidar ilişkileri ve yapıların da bunda pay sahibi olduğu açık bir gerçektir (Özbay ve diğerleri, 2011: s. 13).

Mahremiyet, kişinin benliğini inşa etmesinde ve diğer bireylerle yakın, samimi ilişkiler kurabilmesinde temel bir unsur olarak tanımlanmaktadır. Bununla birlikte, akademik alanda yapılan bu vurguya rağmen, günlük yaşam pratikleri bunun aksini göstermektedir. Günümüzde pek çok insan için özel hayat, korunması gereken bir değer olmaktan ziyade, şöhret ve tanınma arzusu uğruna feda edilebilecek toplumsal bir bedel haline gelmiştir. Reality şovlar, sosyal medya platformları, bloglar ve cep telefonları gibi araçlar, kişilerin mahremiyetlerini ifşa ettikleri, özel yaşamlarını sergiledikleri yeni

alanlar sunmaktadır (Şişman, 2019: s. 19). Ayrıca, siber toplumun normlarının şekillendiği dijital dünyada mahremiyetin anlamı yeniden yazılmaktadır. Başka bir deyişle, mahremiyet ortadan kaybolmaktan ziyade dönüşüme uğramaktadır. Bireylerin özgüvenle hareket eden öznelere dönüştüğü bu dünyada mahremiyetin ortadan kalktığı değil, sergilenmeye başladığı söylenebilir. Çünkü bireyler kendilerini paylaşımlar yoluyla ifşa ettikçe, mahremiyetin sınırlarını da değiştirmektedir. Bauman'ın ifadesiyle, "ifşa edilme korkusu, tanınma isteğiyle bastırılmaktadır" (Bauman ve Lyon, 2013: s. 31). Böylece bireyler mahremiyeti eski kodlardan bağımsız biçimde yeniden tanımlamayı, ona yeni anlamlar yüklemeyi veya eski tanımları görmezden gelmeyi tercih etmektedirler (Hazır, 2019: s. 148).

Hermann Hesse'nin (2016) *Bozkırkurdu* romanındaki kahraman gibi, günümüzde birçok insan birden çok benliğe sahiptir. Dolayısıyla her bireyin mahremiyet anlayışı, sahip olduğu farklı benliklere göre değişmektedir. Fakat bu farklı benliklerin tamamına hitap edebilecek bir dijital otorite bulunmamaktadır. Hazır'a göre, günümüzün dijital karakterleri "çoklu benliklere" sahip olarak, içlerindeki benlikleri birbirine karşı kullanmaktadır. Bu nedenle dün "bana özel" olan bir şey, bugün "şu anki ben" için aniden mahrem olmaktan çıkabilmektedir (Hazır, 2019: s. 153). Daha önce mahrem sayılan pek çok şey artık öyle algılanmamakta; dolayısıyla bireysel mahremiyet ve özel alan kavramlarının anlamlarında da bir değişim yaşandığı söylenebilir.

Enformasyon Mahremiyeti

Enformasyon mahremiyeti kavramı, enformasyon kavramı temel alınarak tanımlanmaktadır. Dijital çağın etkisiyle enformasyon mahremiyetinin önemi ve riskleri daha da artmaktadır. Yüksek teknoloji ve çeşitli uygulamalar, kişisel alanları ve sınırları giderek daraltarak, bireyleri kapsamlı bir denetim ve gözetim ağına sıkıştırmaktadır.

Mahremiyet, sanal ortamda "enformasyon mahremiyeti" adı altında ele alınmaktadır. Bu bağlamda, enformasyon mahremiyeti, bireylerin özel kabul edilen verilerinin hukuki olarak gözetim altına alınmasını ifade etmektedir. Elektronik ortamdaki mahremiyet, daha çok işlem odaklı bir biçimde incelenmek istenmektedir. Bunun nedeni, mahremiyet ihlallerine olay bazlı çözümlerle yaklaşmanın daha etkili olacağı inancıdır (Karagülle, 2015: s. 36). Ancak, benzersiz özelliklere sahip olan siber uzayda, mahremiyet ihlallerinin olay temelli olarak çözülmeye çalışılması doğru bir yöntem olarak değerlendirilmektedir.

Günümüz dünyasında bu durum bir "dijital devrim" olarak da görülmektedir; Tarım ve Sanayi Devrimi gibi, toplumsal koşullarda radikal değişimler meydana gelmektedir. Toplumun dijitalleşmesi (mikroçiplerin ve internetin gelişimi gibi unsurlar) bu dönüşümün en önemli ayaklarından biridir. İnternetin hem özel hem de profesyonel hayatımıza tamamen entegre olmasıyla birlikte mahremiyet konusu önemli bir değişime uğramaktadır. Akıllı telefonlar ve sosyal medyanın yükselişiyle birlikte, "anonimlik" kavramı da ortadan kalkmaktadır.

İnternet üzerindeki etkileşimlerin sınır tanımaksızın küreselleşmesi, "veri-özneler" olarak adlandırılan kullanıcıların kişisel bilgilerinin dünyanın dört bir yanında izlenip kontrol altına alınmasına ve kullanıcıların dijital ortamda savunmasız hale gelmesine yol açmaktadır. Enformasyon teknolojileri, mahremiyet ihlallerine sebep olmakta; gözetim uygulamaları ise yalnızca dijital alanda değil, günlük yaşamın her alanında sıradan bireyleri de içine alacak şekilde yaygınlaşmaktadır (Dolgun, 2015: s. 210-211). Bugün enformasyon toplumu ve teknolojileri, bireylere büyük avantajlar sunarken; aynı zamanda bireysel mahremiyet, enformasyon mahremiyeti ve mekânsal mahremiyet gibi alanlarda ciddi ihlallere neden olmaktadır.

2.4. Geleneksel Mahremiyetin Değişimi ve Gönüllü İfşa: Yeni Medyada Gözetim, Kontrol ve Yeni Mahremiyet

Mahremiyet kavramının sonunun başlangıcı, 1960'ların ortalarına kadar uzanmaktadır. Mahremiyetin ölümü olarak nitelendirilen bu olgu, artan yayınlar ve tartışmalarda defalarca dile getirilmiştir (Vincent, 2017: s. 178). Nitekim, Vance Packard, 1964'te yayımlanan *Çıplak Toplum* (The Naked Society) adlı kitabında, "vatandaşlara yönelik gözetimin artan yoğunluğundan" ve bu sürecin sürekli hale gelmesinden sorumlu olan, mahremiyetin altını oyan çeşitli güçlerden söz ediyordu (Packard, 1964: s. 34, 43).

1993'te World Wide Web (www)'nin kullanıma sunulması ve aynı dönemde kişisel bilgisayarların yaygınlaşması, mahremiyet konusunu sürekli olarak tartışılır hale getirmiştir. Buna göre, basılı ve dijital gazetecilikten kapsamlı akademik araştırmalara kadar pek çok alanda mahremiyetin defalarca "öldürüldüğü" ve her defasında yeniden gündeme gelip tekrar yok edilerek bir "zombi" durumuna dönüştüğü söylenebilir (Solove, 2008: s. 5). David Holtzman'ın 2006 yılında yayımlanan *Mahremiyet Kaybı* (Privacy Lost) adlı çalışmasında verdiği uyarı oldukça çarpıcıydı: "Mahremiyetimiz, kutuplardaki

buzulların erimesinden bile hızlı yok oluyor; teknoloji, hukukun koruyabileceğinden daha hızlı bir şekilde onu eritiyor. Bu eğilim geri dönüşü olmayacak kadar güçlüdür. Bildiğimiz haliyle mahremiyet artık kaybolmuştur" (2006: s. xix). 2010 yılında Mark Zuckerberg'in yaptığı konuşmada durumu, medyada da büyük yankı uyandıran şu sözlerle doğrulamıştır: "Mahremiyetiniz zaten sıfır seviyesine indi. Artık bunu kabullenin!" (Vincent, 2017: s. 183).

2013'te yayımlanan distopik roman *Çember* (The Circle), küresel bir sosyal ağ şirketini konu alarak, hakikat ve erdem gibi kavramlar uğruna kullanıcılarını mahremiyetin tüm kalıntılarından vazgeçmeye ikna eder. Çember'in eş başkanı, mesajını Orwell tarzında üç temel sloganla özetler: "Sırlar Yalandır. Paylaşmak Umursamaktır. Mahremiyet Hırsızlıktır" (Eggers, 2013: s. 303). Giddens, *Mahremiyetin Dönüşümü* (2010) adlı kitabında, plastik cinsellikten saf ilişkiye kadar, eskiden yalnızca kişisel bir mesele olarak görülen cinselliğin artık sürekli kamusal alanda konuşulduğunun altını çizerek modern toplumdaki mahremiyet dönüşümünü ele alır. Günümüzde ise Giddens'ın tartıştığı bu konular, daha ileri düzeylere yükselmiş ve hatta aşılmış bir hale gelmiştir (Rizanaj, 2020: s. 133).

Toplum sürekli bir dönüşüm sürecinden geçerken, mahremiyet de bu sürecin bir parçası olarak yeniden şekillenmektedir. Mesut Hazır, *"Siber Toplumda Mahremiyetin Dönüşümü"* başlıklı makalesinde mahremiyet kavramını şu şekilde dile getirir:

> "Bugün, postmodern endişelerin siber arenalarından biri olan sosyal medya, yalnızlığımızı hafifletmek için dahil olduğumuz sanal topluluklar sunuyor. Bunu yaparken tüm kimliğimizi açığa çıkarıyor, kendimizi siber uzayın bir parçası haline getirerek varlığımızı sürdürmeye çalışıyoruz. Tam da bu noktada mahremiyet devreye giriyor. Sosyal medya, duygularımızı, hislerimizi, duyarlılıklarımızı, anlam yüklü ifadelerimizi ve 'merhamet karnavallarını' aşırıya kaçarak paylaştığımız bir alan haline gelmiştir. Eskiden yalnızca yakın çevremizle ya da 'mahrem ötekiler' dediğimiz kişilerle sınırlı olan paylaşımlarımız, artık 'anonim ötekilerin' ve 'mutlak yabancıların' dikkatine de sunulmakta ve onların da radarına girmektedir" (Hazır, 2019: s. 147).

Bill Gates, "pencere" anlamına gelen Windows adını işletim sistemine vererek, internet devrimiyle birlikte bir "ağ toplumuna" açılan kapıyı en iyi ifade edenlerden biri olmuştur. Sosyal medya, hem dışarıyı izleyebildiğimiz hem de içerimizi gönüllü olarak

gösterebildiğimiz bir "pencere" işlevi görmektedir. Artık ev içi ve kamusal alan arasındaki ayrım ortadan kalkmış; sosyal medya aracılığıyla evimiz ve yaşamımız kamusal alanda sergilenir hale gelmiştir. Günümüzde, en korunaklı güvenlik önlemleriyle donatılmış ultra lüks sitelerde otursak bile, sosyal medyada yaptığımız paylaşımlar sayesinde mahremiyetin nerede başlayıp nerede bittiği; hangi durumların mahremiyet ihlali anlamına geldiği bilinemez duruma gelmiştir (Karakaya, 2019: s. 69). Özel ve kamusal hayat arasındaki sınırların belirsizleşmesi ve mahremiyetin daha akışkan bir hale gelmesi, bu dönüşümün ne zaman başladığını anlamamızı da zorlaştırmaktadır. Ancak bu ayrımın şifresi çözüldüğünde, dönüşümün izlerini görmek mümkün hale gelebilecektir.

Sosyal medya varoluşsal bir savaş alanı olarak görüldüğünde, mahremiyetin bilindik sınırları da zayıflamaktadır. Artık, G. Orwell'in ünlü distopyası (1984) ya da M. Foucault'nun panoptikon (2017) kavramında gördüğümüz, kişinin bilgisi dışında ve rızasına dayanmayan gözetim biçiminden ziyade, kullanıcıların yalnızca izlenen değil, sürecin aktif bir parçası oldukları bir denetim biçimi ortaya çıkmıştır. Görünürlük, daha fazla bakışlara açık olmak anlamına gelir olmuştur (Barbarosoğlu, 2015: s. 16). Günlük yaşamda mahrem olarak kabul edilen ve kimsenin erişemediği alanlar, sosyal medya aracılığıyla yabancılar da dahil olmak üzere geniş kitlelere sergilenebilir hale gelmiştir (Anık, 2019: s. 129). Artık dijital alanda mahremiyetin paylaşılması, yalnızca kullanıcının kendi özel hayatıyla sınırlı kalmamakta; toplumu oluşturan diğer bireylerin, çocukların ve tanıdıkların mahremiyetleri de sosyal medya sayesinde kamusal hale getirilebilmekte ve bir nesne gibi kullanılabilmektedir.

2.5. Sosyal Ağların Mahremiyet Algısı Üzerindeki Rolü

Hem yüz yüze hem de aracılı iletişimin öne çıktığı günümüzde sosyalleşmenin en önemli unsurlarından biri sosyal ağlardır. Nitekim, sosyal ağlar sosyal etkileşim süreçlerinin temel taşlarından biri haline gelmiştir. Bilgi ve iletişim teknolojilerindeki baş döndürücü ilerlemelerle birlikte bireyler, sosyal ağlar sayesinde dünyanın dört bir yanındaki insanlarla bağlantı kurabilmekte ve sosyal çevrelerini oldukça genişletebilmektedir. Sosyal ağlar yalnızca insanları birbiriyle daha kolay iletişim kurabilir hale getirmekle kalmamakta; aynı zamanda kişisel profillerin yayınlanabilmesi, bilgi ve içerik paylaşımı, uygulama paylaşımları ve kullanıcılar arasında yeni sosyal ilişkilerin kurulmasına da olanak tanımaktadır. Buna karşın, bu iletişim kanallarının sosyalleşmeyi destekleyip desteklemediği meselesi hâlâ tartışmalıdır. Çünkü sosyal ağlar,

bireylerin yaşamları üzerinde ciddi etkilere sahip olabilmekte ve doğru kullanılmadıklarında mahremiyet ihlallerine zemin hazırlayabilmektedir (Yüksel vd., 2013: 766-767).

Açıkça görüldüğü gibi, sosyal ağlar pek çok insan için artık sıradan bir günlük alışkanlık halini almış durumdadır. Akıllı telefonlar ve tabletler gibi taşınabilir yeni medya araçlarının da etkisiyle, bu ortamlarda sürekli aktif olmak isteyen birey, çevrimdışı kaldığında kendini *"dünyadan kopmuş, gelişmelerden habersiz"* hissetmektedir (Karakartal, 2013: s. 5). Dolayısıyla bu durum, araştırmacılar açısından artan bir kaygı unsuru haline gelmiştir. Bu noktada mahremiyetin korunması, kişisel verilerin paylaşımı ve sosyal ağlardaki uygulamalar kritik önem taşımaktadır. Her ne kadar sosyal ağlar mahremiyeti koruyabilmek için bazı özellikler sunsa da, pek çok kişi bu imkânlardan haberdar değildir ya da nasıl kullanılacağını bilmemektedir.

Sonuç olarak, sosyal ağların mahremiyet algısına olan etkileri inkâr edilemez. Sosyal medyanın sosyalleşme süreçlerindeki merkezi rolü, mahremiyet algısının biçimlenmesinde ve dönüşmesinde önemli bir yer tutmaktadır. Ancak, bu süreç yalnızca sosyal ağların kullanıcıları etkilemesiyle sınırlı değildir; aynı zamanda kullanıcıların mahremiyet tercihleri de sosyal ağlardaki davranışlarını şekillendirmektedir. Hangisinin daha önce geldiği ise tartışmaya açık bir konudur.

2.6. Dijital Mahremiyet ve Benlik Gösterisi

Gözetim teknolojileri ve çağdaş iletişim kanalları, bir yandan kişinin bilgisi dışında ve rızası olmadan mahremiyet alanındaki her türlü ayrıntıyı metalaştırıp dolaşıma sokarken, diğer yandan büyük kitlelere ulaşma vaadiyle bireyin gönüllü olarak mahremiyetini kamusal alana sunmasını teşvik etmektedir. Sanayi, özellikle sosyal medya platformları aracılığıyla kişiye kendini ifade etme ve öne çıkma fırsatı sağlarken, bu süreçte birey özünde mahremiyetini endüstrinin kontrolüne teslim etmektedir. Dijital teknolojiler, bireyin rızasına bakmaksızın onu bir nesne haline getirerek, kişisel bilgileri kullanmakta ve mahremiyet ihlallerini artırarak endüstrinin büyümesine katkı sunmaktadır.

Gözetim teknolojilerinin ve yeni iletişim yöntemlerinin etkisiyle güçlenen panoptik/sinoptik yapı, mahremiyetin her alanda geri dönülmez şekilde parçalanması ve ihlal edilmesine neden olurken, bu süreç aynı zamanda özel alanla ilgili önemli soruları da gündeme getirmektedir. Kendini gösterme ve görülme isteği, arzunun dışa vurumunu

aşarak belirleyici hale gelmiştir. Varlığın temel yapı taşlarından biri olan arzu, bireyin bedeni ve aklı üzerinde mutlak bir hâkimiyet kurma çabasıdır. Beden aracılığıyla deneyimlenen dünyevi zevkler, odaklı ve yeni bir sahiplenme biçimini ortaya çıkarmış ve fiziksel dürtülerin ticari değerini daha önce olmadığı kadar artırmıştır. Artık bireyin mahrem alanına giren duyguları, aile yaşamı, cinsellik, sağlık durumu, inançları, iş sırları, planları, yazışmaları, yalnızlık anları, yatak odası gibi pek çok unsur öyle bir şekilde alenileştirilmiştir ki, bu noktada gizlilik iradesinin koruyucu kutsallığı da tamamen ortadan kalkmıştır (Köse, 2011: s. 11).

Sosyal medya üzerinden, gerçekte olduklarından farklı olarak olmak istedikleri kişilikleri sergileyen bireylerin mahremiyetlerini açığa vurmasında, kabul edilme, takdir toplama, beğeni kazanma ve toplumsal statü sağlama gibi haz odaklı dürtülerin başrol oynadığı söylenebilir. Narsisizm ve bir anlık da olsa ünlü olma arzusu, günümüzde pek çok insanı harekete geçirmektedir. Örneğin, 2006'da ABD'de yapılan bir araştırmaya göre, 18-25 yaş arası gençlerin %51'i "ünlü olmayı" kuşakları için önemli bir hedef olarak belirtmiştir. Bu oran, "manevi olarak kendini geliştirme"yi önemli bulanların yaklaşık beş katıdır (Arık, 2018: s. 177). Aynı yıl İngiltere'de yapılan bir ankette ise çocuklara "dünyadaki en iyi şey nedir?" sorusu yöneltilmiş ve "ünlü olmak" cevabı en çok verilen yanıt olmuştur. Bu cevap, "iyi görünmek" ve "zengin olmak" yanıtlarıyla birlikte narsisistik üçlüyü tamamlamaktadır (Arık, 2018: s. 178). Görünen o ki, ünlü olmak ve narsist eğilimler arasında güçlü bir ilişki vardır. İlginç şekilde, 'Tanrı' bu popüler cevaplar arasında en son sırada yer almaktadır. Counting Crows grubunun 1993'teki şarkısında öngörüyle dile getirildiği gibi: "Televizyona baktığımda / Başrolde kendimi görmek istiyorum / Hepimiz büyük yıldızlar olmak istiyoruz / Ama nedenini ya da nasılını bilmiyoruz" (Twenge ve Campell, 2010: s. 140).

Nietzviecki, sosyal medyada paylaşım yapma arzusunu, bireyselliğimizi ortaya koyma şekli olarak tanımlar ve artık bir "dikizleme kültürü"nün varlığından bahseder (Nietzviecki, 2010: s. 15). Ona göre, insanların gönüllü katkısıyla gelişen bu *"dikizleme kültürü",* insanlık krizine sunulmuş çarpık bir çözüm gibidir: "Dikizleme, herkes hakkında her detayı bilme ve öğrenme arzusudur. Bunun karşılığında da başkalarının sizinle ilgili her şeyi öğrenmesine onay vermiş olursunuz. Kendimizi izlenir kıldığımızda ve insanlar bizimle ilgili yorum yaptığında, belki de ironik bir biçimde, birey olduğumuzun farkına varırız. İzlenerek, ne kadar özel ve ne kadar farklı olduğumuzu

başkalarına kanıtlamak isteriz. Ama bu aynı zamanda, sıradan ve olağan bir insan olduğumuz anlamına da gelir; çünkü tıpkı başkaları gibi bizim de başkalarına ihtiyaç duyduğumuz açıktır... Böyle bakıldığında, dikizleme; teknoloji çağında dünyaya gelmenin, sürekli alışveriş yapmanın ve küresel magazinin doğal bir uzantısı ve bunlara karşı geliştirilmiş bir tepkidir" (Nietzviecki, 2010: s. 15, 38).

Nietzviecki ayrıca, dikkat çekme, fark edilme ve yalnızlıktan kurtulma isteğinin, dikizleme kültürüne kapılan modern insanın en temel motivasyonu olduğunu şöyle belirtmektedir (2010: s. 235): "Elbette yalnızlıktan kurtulmak için tek çare bu değil; Facebook kullanmaktan webcam görüşmelerine, blog yazmaktan reality show'lara kadar pek çok yolla mahremiyetimizi kamusal alana taşıyarak anlam arıyor, ün ve maddi kazanç peşinde koşuyoruz. Kimi zaman kendimizi gönüllü bir şekilde ifşa etmeye razı oluyor, hatta bazen buna çaresizlikle başvuruyoruz; çünkü monitörün soğuk mavi ışığı yüzümüze vurduğunda, şehrin ortasında, mavi odalarımızda sessizce oturmaktansa, yaşadıklarımızın başkaları tarafından bilinmesini tercih ediyoruz. Özetle, mahremiyet kaybı, endişelerimiz arasında en son sıralarda yer alıyor. Facebook kullanıcıları üzerine yapılan bir araştırma ise, katılımcıların %90'ının sitenin gizlilik politikasını okumadığını, %60'ının gizliliğe hiçbir önem vermediğini, %30'unun ise az da olsa bu konuya önem verdiğini gösteriyor."

Benlik gösterisi, birey olmaya adanmışlık, saplantı derecesine ulaşmış gözetim arzusunun gölgesinde kalan mahremiyet ihlalinin günümüzde çok da önemsendiğini söylemek mümkün değildir. Sosyal medyanın gizlilik anlaşmalarını okuyan, hakkında bilgi sahibi olan ya da merak duyan kitlenin varlığı tartışılır. Genellikle haberleşmeye, düşündüklerini iletmeye ve inşa ettiği kimliğini ifşa etmeye odaklanmış bireyler, yapılan paylaşımların bugün ve yarın ne anlama geleceğini sorgulamaktan habersizdir demek mümkündür. Dolayısıyla mahremiyetin ifşasında toplumun büyük kısmının rızası olduğu ve bu paylaşımdan, beğeni, takdir, kişisel kazanç gibi 'faydalar' umduğunu imlemek gerekir. Sosyal medya, kullanıcılarının sosyalleşme ve popülerlik arzusunu karşılayarak onların görünür olma ihtiyacını tatmin ederken, günümüzde insanlar yaşamlarını daha önce hiç olmadığı kadar başkalarının gözü önünde sürdürmekte ve bu yeni norm hızla sıradan bir hale gelmektedir. Dikizleme kültürünün etkisi altında, dijital dünyadaki yaşamlar kalıcı ve mahrem bir biçimde ortaya serilirken, paylaşılan tüm içerikler farklı bağlamlarda ve farklı kişiler tarafından yeniden yorumlanmakta ve

anlamlandırılmaktadır. Bireye dair her şeyin metalaştığı böylesi bir ortamda, en mutlu anımız başkalarına üzüntü verebilmekte, en utandığımız anımız başkalarının eğlencesi olabilmekte ve unutturmaya çalışsak da artık mümkün görünmemektedir (Arık, 2018: s. 180-181).

Sosyal medyanın yaygınlığıyla beraber kamusal alan ile özel alan arasındaki sınır iyice belirsizleşmekte -ki sosyal medya tam da bu belirsizlikten güç almakta- ve mahremiyetin giderek daha fazla ihlal edilmesine rağmen, toplumsal tepkiler yetersiz kalmaktadır. Sosyal ağlar sürekli olarak ne yaptığımız, ne düşündüğümüzü, nerede olduğumuzu yoklarken, yaptığımız paylaşımlar ölçüsünde de karşımıza tüketim fırsatları çıkarmaktadır. Gözetlemekten ve gözetlenmekten haz duyan bir kitlenin varlığı, bu eylemlerden faydalanan şirketlerin de varlığı anlamına gelmektedir. Sözgelimi, bazı dijital platformlar size sormadan konumunuzu ele geçirmekte ve bulunduğunuz yere uygun tüketim seçeneklerini karşınıza çıkarmaktadır. Ya da bir alışveriş merkezine girdiğinizde, otomatik olarak cep telefonınıza o merkezde yer alan kuruluşların indirim seçenekleri düşmektedir. Bu etkileşimin odağında yer alan kuruluşların indirim seçenekleri düşmektedir. Bu etkileşimin odağında yer alan eylem ise, rızanızla verdiğiniz telefon mumaranızdan başka hiçbir şey değildir (Arık, 2018: s. 182-183).

2.7. Sosyal Medyada İhlal Tartışmaları

Facebook'un kuruluş yıllarında, Mark Zuckerberg "Facebook'ta yer almak istiyorsanız mahremiyetinizi bir kenara bırakmalısınız" şeklindeki meydan okuyucu söylemiyle mahremiyet ihlallerinin kullanıcıların isteğiyle gerçekleştiğini savunmuştu. Ancak 2018'de patlak veren büyük veri skandalı sonucunda ciddi bir itibar kaybı yaşamak zorunda kaldı; Senato'da ifade verdi ve hisse senetleri büyük bir değer düşüşü yaşadı. Merkezi Londra'da bulunan veri analiz firması "Cambridge Analytica"nın, 87 milyon Facebook kullanıcısının izinsiz bir şekilde elde ettiği verileri ABD ve İngiltere'deki önemli seçimleri etkilemek amacıyla yasa dışı kullandığı iddiaları, tüm dünyada sosyal medya ve mahremiyet ilişkisini yeniden gündeme taşıdı.

Cambridge Analytica'nın milyonlarca Facebook kullanıcısına ait verileri yasa dışı yollarla kullandığının açığa çıkmasından sonra, ABD'nin eski CIA ve NSA çalışanı Edward Snowden, bu skandalda Facebook'un "mağdur" değil, doğrudan bir "ortak" olduğunu dile getirmiştir (Arık, 2018: s. 163). NSA'nın dünya çapındaki izleme programı hakkındaki belgeleri ifşa ederek 2013'te Rusya'ya sığınmak zorunda kalan Snowden,

Cambridge Analytica Skandalı'yla gündeme gelen Facebook'u bir "istihbarat şirketi" olarak nitelendirmiştir. Facebook'un kullanıcı verilerini kötüye kullanan bir strateji izlediğini ve bu sebeple bir "istihbarat kuruluşu" gibi çalıştığını vurgulayan Snowden, 2014'te 50 milyon Facebook kullanıcısının verilerini toplayan Cambridge Analytica'nın, 2016 ABD Başkanlık seçimleri için Facebook'la işbirliği yaptığını hatırlatmıştır. Snowden, 2013'te Amerikan hükümetinin sosyal medya verilerine nasıl erişim sağladığını da çarpıcı bir şekilde ortaya koymuştu. Twitter'da "Cambridge Analytica Skandalı" hakkında şunları yazmıştır: "Facebook, insanların kendi rızalarıyla paylaştığı bilgilerin çok ötesinde, mahrem verileri kullanarak ve satarak gelir elde ediyor." Skandalda Facebook'un "kurban" değil, aslında "işbirlikçi" olduğunu ifade eden Snowden, şu sözleriyle durumu özetlemiştir: "Bir zamanlar özel hayatlara dair kapsamlı kayıtları toplayıp satanlara 'istihbarat şirketi' denirdi. Günümüzde ise kendilerini 'sosyal medya' olarak adlandırmaları, Savunma Bakanlığı'nın 'Savaş Bakanlığı' olduğu gerçeğini gizlemesinden beri yapılmış en büyük aldatmacadır" (Snowden, 2018).

Facebook'ta yaşananlar, sosyal medya dünyasında meydana gelen tek gizlilik ihlali değildir. Benzer vakalar diğer sosyal medya platformlarında da ortaya çıkmıştır. Örneğin, X (Twitter), 87 milyon Facebook kullanıcısının verilerini Cambridge Analytica'ya satan Aleksandr Kogan'a veri erişimi sağladığını kabul etmiştir. Şirketin de doğruladığı habere göre, Kogan'ın firması 2015 yılında Twitter'daki herkese açık verileri bir günlüğüne toplamak için ödeme yapmıştır (Arık, 2018: s. 164).

Yer bildirimi özelliği bulunan Foursquare gibi uygulamalar ve Instagram gibi platformlar da kişilerin nerelere gittiklerini, tercihlerini ve alışkanlıklarını pazarlamak için kullanılabilmektedir. Artık markalar, toplumsal statünün göstergesi haline gelmiştir. Aynı şekilde seyahat edilen ülkeler, gidilen restoranlar ya da özenle seçilmiş güzel fotoğraflar da statü arayışının bir ifadesi olarak görülebilir. Ancak burada çelişkili olan şey, ister gönüllü ister istemsiz olsun, insanlar tarafından yapılan paylaşımların nesneleşmesi ve izinsiz şekilde başka amaçlarla kullanıma sunulmasıdır. Forsquare'ın gizlilik beyanında, "servisimize yazdığınız ya da başka şekilde verdiğiniz bütün bilgiler kaydedilmektedir" denmektedir. Foursquare reklam almak için pazarlamacılara belli yerlerin yakınlarındaki insanlara erişme olanağından çok daha fazlasını sunduğu dikkate alındığında bu ifadenin mahremiyete etkisini anlamak daha kolay olacaktır (Arık, 2018: s. 165).

Her ne kadar günümüzde sosyal medyalardaki verilerin kullanım tasarrufu bireydeymiş gibi gözükse de sosyal ağların daha fazla mahremiyet talep ettiği hatta oralarda etkin bir şekilde var olabilme koşullarının bu mahremiyet paylaşımları ile doğru orantılı olduğu bilinmektedir. Mevcut sosyal medyaların, veri depolama odaklı yapılanması o kadar çok insanı rahatsız etmiştir ki, görece daha kapalı ve kişinin özeline sızma ve bunu dışarı sızdırma ihtimali olamayan yeni paylaşım ağlarının oluşması kaçınılmazdır. Hatta bu noktada Path ve Peach gibi kapalı sosyal ağlar Batı'da yaygınlaşmaya başlamıştır. Yaygın sosyal ağlardan farklı bir altyapı kullanan bu kapalı sosyal ağlar hem izin verilmeyen kimselerin paylaşımları görmesini hem ekran görüntüsü almasını engellerken hem de içeriklerin belli bir süre içinde otomatik olarak silinmesini sağlamaktadır. Çoğu kapalı sosyal ağa erişim mobil cihazlar üzerinden sağlanmakta ve üyelik sırasında telefon numarası ile onay istenmektedir (Arık, 2018: s. 165-166). Bu sebeple kapalı sosyal ağlarda 'trol' olarak adlandırılan sahte hesaplar yer alamamaktadır. Öte yandan daha kalıcı çözüm isteyen kimi insanlar ve aktivist kurumlar, internet aktörlerinin mahremiyet ihlallerine tepki gösterip, bu organizasyonları kişi hak ve özgürlüklerine daha duyarlı olmaya çağırsalar da şirketlerin bu konuda somut adım atmaları ekonomik rasyonalite açısından çok kolay değildir.

Kullanıcıların verilerini satmakla suçlanan Google'un avukatları ise şirketlerini şu sözlerle savunmuştur: "Tam anlamıyla bir mahremiyet istiyorsanız, bunun ancak bir çölde yaşayarak mümkün olabileceğini unutmayın. Keşiş değilseniz, toplum yaşamının doğal sonuçlarını kabul etmek zorundasınız" (Niedzviecki, 2010: s. 277). Benzer şekilde, Sun Microsystems'in CEO'su Scott McNealy de mahremiyetin artık kalmadığını ifade ederek, "Artık gizlilik diye bir şey yok; buna alışsanız iyi edersiniz" demiştir (Niedzviecki, 2010: s. 266). Görüldüğü üzere internet organizasyonlarının yöneticileri üzerinden para kazandıkları 'mahremiyet' meselesinden çok hoşlanmamakta, bu meselenin gündemde durmasından rahatsız olmaktadır. Şirketler, nette yer alan ve vatandaşları mahremiyetlerini koruma konusundaki bilgilendiren uyarı içeriklerini ise sadece ileride açılacak olası davalardan kendilerini korumak için yapmaktadır. Zaten bu tarz uzun bilgilendirmeleri ya da sözleşmeleri okuyabilen -okumak için vakit ayıran, okuduğunu kavrayabilen- insan sayısının genel ortalamanın çok altında olduğu bilinmektedir (Arık, 2018: s. 166). Mahremiyet ihlali şirketlere genişleme ve büyüme imkanı sunmakta, bu süreçteki kayıplar ise kazançların gölgesinde kalmaktadır.

2.8. Sosyal Ağlarda Alınması Gereken Güvenlik Tedbirleri

Sosyal ağların mahremiyeti ortadan kaldıran etkisine karşı önlem olarak da çeşitli görüşler ortaya konulmuştur. Konu bağlamında daha önce değinilen önlemlerin yanı sıra sosyal medya platformlarında mahremiyetin ve özel hayatın korunması, gözetimin sınırlandırılabilmesi için çeşitli öneriler de ortaya konulmaktadır. Bunun için göz önünde tutulması gereken çeşitli hususlar şöyle sıralanabilir (Yavanoğlu vd., 2012: s. 24; Erdoğan ve Bahtiyar, 2014: s. 271):

• Sosyal medya sitelerine üye olmadan önce, platformun gizlilik politikası incelenmeli ve paylaşılan içeriklerin izlendiği ya da denetlendiği bilinmelidir.

• Olası risklere karşı bilgiler yedeklenmelidir.

• Kişisel fotoğraflar sosyal medyada paylaşılmamalı, yüklendiyse etiketlenmemeli ve kişisel iletişim bilgileri paylaşılmamalıdır.

• Hesap ayarlarından gizlilik düzeyleri belirlenerek kısıtlamalar uygulanmalıdır.

• Bu gizlilik ayarları zaman zaman güncellenerek kontrol edilmelidir.

• Sosyal ağlara üye olurken güçlü ve tahmin edilmesi zor bir şifre seçilmeli, paylaşılacak bilgiler de başkalarının bilmeyeceği türden olmalıdır.

• Kullanılan uygulamaların reklam ve paylaşım izni olabileceği unutulmadan gerekli kısıtlamalar yapılmalıdır ve bağlantılar açılmadan önce güvenliği sağlanmalıdır.

• Sosyal medyaya ara sıra farklı bir kullanıcı hesabıyla erişmek yararlı olabilir.

• Sosyal mühendislik saldırılarına karşı, bilinmeyen topluluklara dahil olunmamalıdır.

• Tanımadığınız kişilerden gelen arkadaşlık istekleri reddedilmelidir.

• Arkadaşlık talepleri konusunda seçici davranılmalıdır.

• Davet alındığında, kabul etmeden önce detaylı bir araştırma yapılmalıdır.

• Sahte profiller ve sosyal mühendislik saldırıları sosyal medyada oldukça yaygındır. Kullanıcılar bu konuda daima temkinli olmalıdır.

• Çocuklar, sosyal medyadaki yaş sınırlarına uygun olarak hesap açmalı ve aileleri tarafından düzenli olarak takip edilmelidir.

Sosyal medya, kişisel bilgilerin yabancı ya da kötü niyetli kişilerin eline geçmesi açısından gün geçtikçe daha büyük bir risk oluşturmaktadır. Sosyal medya hesabı olmayan birey sayısı ise yok denecek kadar azdır. Bu nedenle, sosyal medyayı kullanırken güvenlik tedbirlerini dikkate almak çok önemlidir. Mahrem bilgilerin korunması için gösterilecek özen, olası sorunların ortaya çıkma riskini önemli ölçüde azaltacaktır.

ÜÇÜNCÜ BÖLÜM

3. KAZAKİSTAN ÖRNEĞİ ÜZERİNE BİR ARAŞTIRMA

3.1. Sosyal Medyada Gözetim Çalışmaları Çerçevesinde Mahremiyet Algısı

Günümüzde teknolojinin hayatımızdaki yerinin giderek artması, gözetim ve mahremiyet kavramlarının toplumsal ve bireysel düzeyde daha fazla gündeme gelmesine neden olmuştur. Gözetim, her zaman toplumsal yaşamın bir parçası olarak varlığını sürdürmüş olsa da, iletişim teknolojilerindeki gelişmelerle beraber biçim değiştirerek daha kapsamlı bir hale gelmiştir. Özel yaşam ile medya arasındaki karşılıklı ilişki ve gerilim dikkate alındığında, özellikle sosyal medya platformlarının bireylerin mahremiyet alanlarını ihlal etmesi meselesi, gözetim ve mahremiyet olgularının yeniden ele alınmasını gerektirmektedir (Rizanaj, 2020: s. 137).

Toplumsal değişimlerin etkisiyle mahremiyet kavramı, içinde bulunduğumuz dönemde farklı şekillerde yorumlanmaktadır. Mahremiyet Komisyonu'nun gerçekleştirdiği araştırmalarda mahremiyetin, pek çok durumda kişisel bütünlüğü tanımlayan bir kavram olduğu ileri sürülmektedir (A.g.e., s. 137). Bu noktada, "mahremiyet" ile "özel hayatın korunması" arasındaki farklılıkların özellikle vurgulanması önem arz etmektedir. Özel alanın korunması, "özel hayatın huzuru" gerekçesiyle daha da büyük bir öneme sahip olmakta ve bu husus, kolektif ya da toplumsal yapının işleyişiyle de doğrudan ilişkilidir. Somut olarak, kamusal alanda yapılan tartışmalarda ortaya çıkan "özel" hak kavramı da bu bağlamda değerlendirilmelidir. Öte yandan mahremiyet, yalnızca kişinin özel bir birey olarak sahip olduğu alan değil, aynı zamanda kamusal alandaki itibarının korunmasıyla da ilgilidir (Lokke, 2018: s. 24). Bireyin, kendisine ait kişisel bilgileri kontrol edebilme yetisine sahip olması, bu bilgilerin kaderi üzerinde mümkün olduğunca söz sahibi olabilmesi ve kimlerle neyi paylaşacağına dair karar verme özgürlüğüne sahip olması, mahremiyetin temel bileşenlerini oluşturmaktadır. Bu çerçevede, yürütülen araştırmanın temel amacı; gözetim ve mahremiyet algısındaki dönüşümleri ele alarak, bu iki kavramı kapsamlı bir şekilde incelemek ve tanımlamaktır.

3.2. Kazakistan'da Yükseköğretim Mezun ve Öğrencilerinin Sosyal Medya Kullanımında Mahremiyet ve Gözetim Algılarına Yönelik Araştırma

Bu bölümde, araştırmanın problemi, amacı ve yöntemi, varsayımlar ve sınırlılıklar, uygulama yöntemi, veri toplama süreci ve analiz aşamaları ele alınacaktır. Ayrıca, araştırma soruları ve elde edilen bulgular sunularak, elde edilen veriler kapsamlı bir şekilde değerlendirilip yorumlanacaktır.

3.2.1. Araştırmanın Problemi

Günümüzde sosyal medyanın yaygınlaşması ve dijitalleşmenin hız kazanmasıyla beraber, bir yandan teknolojinin sunduğu olanaklardan yararlanmakta, diğer yandan ise önceki dönemlere kıyasla bilgilerin gizli kalma olasılığının ortadan kalktığı ve toplumun daha şeffaf bir yapıya dönüştüğü gerçeğiyle karşı karşıya kalmaktayız. Bireylerin ister istemez veya isteyerek, özne ya da nesne olarak dâhil oldukları bu süreç, mahremiyet kavramını sosyal, dini, ekonomik, kültürel ve güvenlik boyutlarıyla farklı şekillerde dönüştürmektedir. Bu bağlamda, sosyal medyayı en yoğun şekilde kullanan yaş grubunun gözetim farkındalığı ve mahremiyet algısındaki değişim, bu çalışmanın temel araştırma sorusunu teşkil etmektedir.

Bu bağlamda çalışma, kartopu örnekleme yöntemi ve yarı yapılandırılmış görüşmeler yoluyla, dijital çağda gözetim olgusu ile sosyal medya mahremiyet algılarının incelenmiştir. Örneklem seçimi sürecinde akademik özgünlük ilkesi esas alınmış ve Kazakistan özelinde bir inceleme yapılmıştır. Kazakistan'ın piyasa ekonomisine dayanan bir yapıya sahip olması, internet kullanım oranlarının giderek artması, Orta Asya'da genç nüfus yoğunluğu açısından öne çıkan ülkelerden biri olması ve tüm bunların yanı sıra coğrafi konumu, kültürel, tarihsel ve siyasal dinamikleri nedeniyle çalışma için önemli bir örneklem oluşturduğu düşünülmektedir.

Orta Asya'nın parlayan yıldızı olarak sayılan Kazakistan, yüzölçümü açısından dünyada 9. sırada, nüfus bakımından 64. ülkesidir (kk.wikipedia.org, Kazakistan Demografisi, 2025). Kazakistan'da birçok etnik unsur barınmaktadır. Kazakistan 16 Aralık 1991 yılında eski SSCB'den ayrılarak bağımsızlığını ilan etmiştir.

1 Eylül 2022 tarihinde yayımlanan 2021 yılı nüfus sayımının sonuçlarına göre, ana etnik grupların payı şöyledir: Kazaklar - %70,4, Ruslar - %15,5, Özbekler - %3,2, Ukraynalılar - %2,0, Uygurlar - %1,5, Almanlar - %1,2, Tatarlar - %1,1, diğer uyruklar ve uyruğunu belirtmeyenler - %5,1 (kk.wikipedia.org, Etnik Gruplar, 2025). Pew

Araştırma Merkezi'ne göre ülke nüfusunun %75'i İslam dinine mensup. Nüfusun geri kalan %14'ünün Hristiyan, %4'ünün dinsiz ve %0,9'unun çoğunlukla Budizm veya paganizm olmak üzere diğer dinleri uyguladığı tahmin edilmektedir (kk.wikipedia.org, Kazakistan'da Din, 2025).

Kazakistan nüfusunun eğitim endeksi ve okuryazarlık oranı yüksek düzeydedir. 1990/91 eğitim-öğretim yılında Kazakistan'daki 55 yükseköğretim kurumunda 287,4 bin öğrenci eğitim görürken, 1999/2000 eğitim-öğretim yılında yükseköğretim kurumu sayısı 163'e, bu kurumlardaki öğrenci sayısı ise 365,4 bine ulaştmıştır. Son 10 yılda yerel halkın eğitiminde bir atılım yaşanıyor. Her 1.000 kişiden 126'sı yükseköğrenim görüyor. Özellikle Kazak gençliği aleyhine öğrenci sayısındaki keskin artış 1990'lı yılların başlarında başladı. Şu anda Kazak öğrencilerin yükseköğrenim kurumlarındaki oranı %67'dir. Ekonominin sektörlerindeki işçiler arasında yüksek ve ortaöğretim düzeyinde eğitim almış kişilerin oranı önemli ölçüde artmıştır: 1989 yılında 1 000 kişiye düşen yükseköğretimli kişi sayısı ortalama 130 iken, 1999 yılında bu sayı 212 olmuştur; Uzmanlaşmış ortaöğretim mezunlarının sayısı ise sırasıyla 234 ve 296'dır (kk.wikipedia.org, Okuryazarlık, 2025).

Kazakistan'da kişisel verileri düzenleyen temel yasal düzenleme, 21 Mayıs 2013 tarihli 94-V sayılı "Kazakistan Cumhuriyeti Kişisel Veriler ve Korunması Hakkında Kanun"dur. Ayrıca, kişisel veri koruma gerekliliklerini sağlayan bir dizi başka kanunlar da mevcuttur. Bunlar arasında "Bilgi Edinme Kanunu", "İletişim Kanunu", "Kazakistan İş Kanunu", "Çevrimiçi Platformlar ve Çevrimiçi Reklamcılık Yasası" yer almaktadır (DlaPiper, 2025).

Çevrimiçi Platformlar ve Çevrimiçi Reklamcılık Yasası uyarınca, ilgili çevrimiçi platformun sahibi ve (veya) yasal temsilcisi, çevrimiçi platformdaki kişisel verileri korumak için aşağıdakileri yapmalıdır: kullanıcıları kayıtlarını tamamlamadan önce çevrimiçi platformun gizlilik politikasıyla tanıştırmak; kişisel verilerin bütünlüğünü, güvenliğini ve gizliliğini sağlamak; kullanıcının veya yasal temsilcisinin izni olmadan kişisel verilerin yayılmasını önlemek; kişisel verilerinin gizliliğinin ihlal edilmesi durumunda kullanıcıyı derhal bilgilendirmek; Kişisel Verilerin Korunması Kanunu'nda öngörülen diğer görevleri yerine getirmek.

We Are Social'ın Şubat 2025'te yayımladığı *Digital 2025: Kazakhstan* raporuna göre, Kazakistan'ın toplam nüfusu 20,7 milyon kişidir ve bu nüfusun yaklaşık 19,2

milyonu (%92,9) internet erişimine sahiptir. Sosyal medya kullanıcı sayısı ise 15,7 milyon kişiye ulaşmaktadır. Ayrıca raporda, ülkede 26,6 milyon (%128) hücresel mobil bağlantı bulunduğu ve bunların %99,3'ünün Mobil İnternet Proxy'si aracılığıyla mobil cihazlar üzerinden sosyal medyaya erişim sağladığı ifade edilmektedir. Nüfusun cinsiyet dağılımına bakıldığında, %51,3'ünün kadınlardan, %48,7'sinin ise erkeklerden oluştuğu belirtilmiştir. Nüfusun ortanca yaşı ise 29,7'dir. Facebook'taki reklamların toplam potansiyel erişimi 2,60 milyon, Facebook reklam erişimi ve toplam nüfus %12,5. Facebook paylaşımının %52,8'i kadın, %47,8'i erkek olduğu bilgisine ulaşılmaktadır. Instagram'daki reklamların toplam potansiyel erişimi 12,4 milyon, Instagram paylaşımının %52,8'i kadın, %47,8'i erkektir (We Are Social, 2025).

Kazakistan'da Elektronik Hükümeti (e-Devlet) konsepti, bilgi ve iletişim teknolojilerinin geliştirilmesi, vatandaşların ve devletin etkileşiminin basit, rahat, erişilebilir ve anlaşılır olması için hazırlanmıştır (EGov.kz, 27.05.2024). "E-devlet" Portalı'nın oluşturulmasının temeli "Kazakistan Cumhuriyeti'nde 2005-2007 yıllarında E-devlet'in kurulması için devlet programına" ilişkin dönemin Cumhurbaşkanı Nursultan Nazarbayev'in 10 Kasım 2004 tarihli 1471 sayılı Kararnamesi ile oluşturulmuştur (Adilet.zan.kz, 25.11.2023). E-devlet, devletle vatandaşların yanı sıra devlet kurumları arasında bilgi teknolojileri aracılığıyla kısmi mutabakatı sağlayan tek bir etkileşim mekanizması olarak organize edilmiştir. Bu mekanizma devlet kurumlarında bürokratik işlemlerin, evrakların, sertifikaların, izin belgelerinin alınmasının basitleştirilmesine ve hızlandırılmasına izin vermiştir (Begen, 2024: s. 11).

Kazakistan elektronik hükümeti dört temel gelişim aşamasından geçmiştir. Bu aşamalardan ilki bilgi aşamasıdır. Bu dönemde E-devlet uygulamasıyla ilgili halkı bilgilendirmeye yönelik bir E-devlet portalı başlatılmıştır. İkincisi, portalda elektronik hizmetlerin ilk sağlanmasıyla başlayan etkileşimli (interaktif) aşamadır. Bu aşamada portalda etkileşimli hizmetlerin tanıtılması, belgelerin toplanmasında harcanan zamandan tasarruf edilmesine büyük ölçüde yardımcı olmuştur. E-hükümetin gelişmesinin üçüncü aşaması, somut işlemler yapılabilme aşaması olmuştur. Bu dönemde vatandaşlar devlet vergileri, ücretler, cezalar ve kamu hizmetleri (su, elektrik, ısıtma vb.) için ödeme yapma fırsatına sahip olmuştur. Bu gelişmelerle vatandaşlar herhangi bir zaman kaybı yaşamadan hizmetlere ilişkin ödemeleri çevrimiçi olarak gerçekleştirebilmeye başlamışlardır. Günümüzdeki E-Hükümet gelişmesinin dördüncü aşaması,

dönüşümseldir. Bu aşamadaki temel amaç vatandaşlara en hızlı şekilde hizmet sunumudur (EGov.kz, 27.05.2024).

E-Hükümetin başarılarına gelirsek, kuruluşundan bu yana Kazakistan Cumhuriyeti E-hükümeti oluşum ve gelişim aşamalarını geçerek olumlu bir görünüm sergilemiş ve çeşitli uluslararası kuruluşlarca yüksek bir takdir görmüştür. Buna uluslararası ve ulusal reytinglerdeki yüksek puanlar ve yarışmalarda kazanılan dereceler tanıklık etmektedir (EGov.kz, 29 Mayıs 2024). Örneğin, 2013'te Cenevre'de (İsviçre) WSIS Project Prizes 2013 Uluslararası Yarışma'da www.elicense.kz sistemi "E-Business" kategorisinde En İyi Projesi; 2013 yılında Dünya Ekonomik Forumu'nun (WEF) Kazakistan'ın Ağ Hazırlık Endeksi 144 ülkeden 43. sırada ve 2012 yılında Birleşmiş Milletler Ekonomik ve Sosyal İşler Dairesi tarafından 192 ülke içinde Kazakistan E-Hükümeti 38. sırada yer almıştır. 2012 yılında Kazakistan'da "Award.kz-2012" Ulusal İnternet Yarışları X. Yıldönümü Ödül Töreninde E-Devlet Hükümet Portalı "İktidar ve Öz Yönetimle" kategorisinde birincilik kazanmıştır. 2016'da Birleşmiş Milletler Ekonomik ve Sosyal İşler Dairesi, Dünyada e-devlet sistemleri içerisinde Kazakistan e-Hükümet uygulamasına 33. sırada yer vermiştir.

2017'de WSIS Prizers-2017 Dünya Zirvesi'nde Kazakistan Cumhuriyeti'nden sunulan üç proje: E-Devlet, Açık Hükümet ve 1414 Çağrı Merkezi yarışmanın kazananları arasına girmiştir. Ayrıca Avrasya ülkelerinin iş ve işletmeleri için önemli yıllık etkinliklerden biri, "Yılın No.1 Seçimi-2018" Projesi'nde "İnovasyon, Modernizasyon ve Kalkınma alanındaki ilerlemeler için" Organizasyon Komitesi Özel Ödülü'nün sahibi olmuştur. Kazakistan Cumhuriyeti E-Devleti'nin 2005-2020 yılları arasındaki başarıları Tablo 1'de verilmiştir.

Tablo 1. Kazakistan Cumhuriyeti E-Devleti'nin 2005-2020 Yılları Arasındaki Başarıları (Birleşmiş Milletler Dünya Sıralaması)

BM Dünya Sıralaması	**2005**	**2008**	**2010**	**2012**	**2014**	**2016**	**2018**	**2020**
E-Devlet Kalkınma Endeksi (EGDI)	65	81	46	38	28	33	39	**29**
E-Katılım Endeksi (EPI)	31	98	18	2	22	67	42	**26**

Kaynak: eGov.kz Portalı, "E-Hükümetin Başarıları" https://egov.kz/cms/kk/information/help/help-elektronnoe-pravitelstvo Erişim tarihi: 29.05.2024



Şekil 3. *EGov.kz'in Uluslararası Sıralaması*

Kaynak: eGov.kz Portalı: "Digital Kazakhstan" https://egov.kz/cms/en/digital-kazakhstan

Erişim tarihi: 28.05.2024

Kazakistan Cumhuriyeti E-Devlet Projeleri

E-devlet projeleri arasında onlarca farklı Bilgi Sistemi (BS), kayıtlar, Devlet Veri Tabanı (DVT), yüzlerce uygulama ve hizmet bulunmaktadır. Bunlar: "E-Akimat", "E-Noter", "Bireyler" BS DVT, Tüzel Kişiler DVT, Tapu Kayıt Belgesi DVT, Devlet Organlarının Birleşik Elektronik Belge Yönetimi Sistemi, Nüfus Hizmetleri Merkezi BS, E-lisanslama BS DVT, devlet kurumlarının internet portalı, E-devlet Ağ Yöneltici ve Ödeme Ağ Geçidi, Mobil Hükümet Bilgi Sistemi, Telegram, Facebook ve Vkontakte'deki sohbet botları vb. uygulamalardır. Aşağıda, yani vatandaşların kendi başına başvurabileceği hizmetlerden birkaçı verilmiştir (EGov.kz, 30.05.2024):

"E-lisanslama" Bilgi Sistemi

Projenin amacı, E-lisanslama Devlet Veri Tabanı Bilgi Sistemi lisanslama süreçlerini, izin belgelerini otomatikleştirmek ve devlet kurumları-lisans verenler ile Kazakistan Cumhuriyeti iş dünyası arasındaki etkin ve açık bir bilgi etkileşimi mekanizmasını sağlamak amacıyla kurulmuştur.

"E-Noter" Birleşik Noter Bilgi Sistemi

"E-Noter", noter faaliyetlerinin kontrolünü iyileştirmek ve noterlerin çalışmalarını optimize etmek için geliştirilmiş bir birleşik noter bilgi sistemidir.

Açık (Şeffaf) Hükümet

Açık Hükümet'in kurulmasına 2013 yılında başlanılmıştır. Açık Hükümet'te yer alan portalların amacı aşağıdaki gibi sıralanmaktadır:

Açık Veriler: devletin temel ve sosyal açıdan önemli faaliyet alanları hakkında halkın farkındalığını arttırmak ve açık verilere dayanarak yeni uygulamalar oluşturmak.

Açık Düzenleyici Yasal İşlemler: vatandaşların düzenleyici yasal düzenlemelerin taslaklarını ve devlet organlarının kanun tasarısı kavramlarını incelemeye katılımını sağlamak.

Açık Diyalog: vatandaşlara devlet organlarının ilk yöneticileriyle doğrudan etkileşim kurma fırsatı vermektir.

Açık (Şeffaf) Bütçeler: vatandaşların devletteki "bütçe" kavramını ve bütçe harcamalarının kamu kontrolünü daha kolay anlayarak aktif bir sivil konumun gelişmesini teşvik etmek.

Devlet Organlarının Faaliyetlerinin Etkinliğinin Değerlendirilmesi: vatandaşları devlet organlarının faaliyetleri etkinliğinin değerlendirilmesinin sonuçları hakkında bilgilendirmenin yanı sıra vatandaşların değerlendirme sisteminin yürütülmesine ilişkin anlayışının iyileştirilmesi.

EGov Mobile Uygulaması

Projenin amacı, Mobil Hükümet platformunun oluşturulması, cep telefonu iletişim cihazları aracılığıyla Kazakistan Cumhuriyeti halkına kamu hizmetlerinin sağlanmasının yanı sıra sürdürülebilir toplumsal kalkınmaya ulaşmak için ülke nüfusunun devletle etkileşimine ek ve etkili bir kanalı oluşturmaktır.

Smart Bridge

"Smart Bridge" Projesi, devlet organları ile özel sektör bilgi sistemleri arasında basitleştirilmiş bir süreçtir. Bu projenin amacı, entegrasyonun, devlet organlarının iş dünyasıyla etkileşimi ve rekabet ortamının geliştirilmesinde organizasyonel prosedürleri basitleştirmektir.

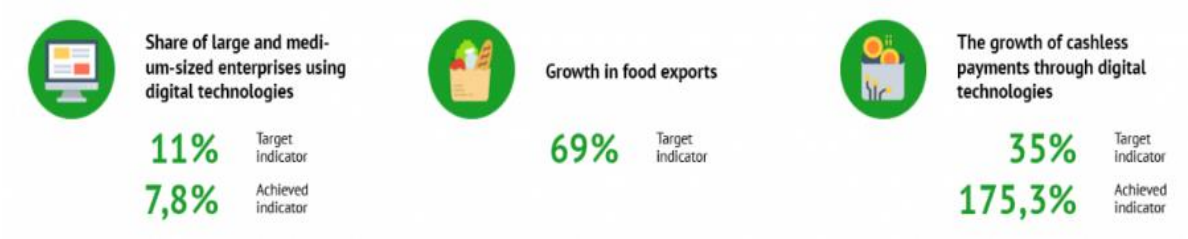
"Digital Kazakhstan"

"Digital Kazakhstan", Kazakistan ekonomisinin gelişme hızını hızlandırmak ve vatandaşlarımızın yaşam kalitesini iyileştirmek için tasarlanmış bir programdır. Programın amacı, Kazakistan Cumhuriyeti ekonomisinin gelişme hızını hızlandırmak ve nüfusun yaşam kalitesini iyileştirmek ve ekonominin yeni bir yörüngeye-gelecekteki dijital ekonomiye geçiş için koşulları yaratmaktır (EGov.kz, 28 Mayıs 2024).

Program 2018-2022 yılları arasında uygulanarak ülkenin amiral gemisi endüstrilerinin teknolojik modernizasyonu için ek bir ivme kazandıracak ve işgücü verimliliğinde büyük ve uzun vadeli büyüme için koşullar yaratamıştır.

"Dijital Kazakhstan" Programının beş temel hedefi bulunmaktadır:

1. Ekonomi Sektörlerinin Dijitalleştirilmesi



Şekil 4. *Ekonomi Sektörlerinin Dijitalleştirilmesi*

Kaynak: eGov.kz Portalı: "Digitization of Economic Branches", https://egov.kz/cms/en/digital-kazakhstan Erişim tarihi: 28.05.2024

Ekonomi Sektörlerinin Dijitalleştirilmesi Programı kapsamında en önemli hedeflerden biri zengin maden yataklarına sahip olan ülke endüstrisinin dijitalleştirilmesidir. Bu amaçla Dijital Madencilik ve Dijital Maden Alanı ile Modüler Dijital Fabrika projeleri hayata geçirilmesi hedeflenmektedir. Ekonomi Sektörlerinin Dijitalleştirilmesi Programının önceliğini bir başka alan da ulaştırma ve lojistik olarak belirlenmiştir. Ulaştırma ve Lojistiğin Dijitalleştirilmesi projesi kapsamında akıllı ulaşım sistemi, çok modlu taşımacılık uygulamaya geçirilmektedir. Aynı şekilde E-Ticaretin, Finansal Teknolojilerin ve Nakitsiz Ödemelerin Geliştirilmesi projesi kapsamında "Fulfillment Merkezi", "E-Commerce Merkezi", "Open API" ve Uzaktan Kimlik Tespiti gibi dijital uygulamalar hedeflenmiştir. Ekonominin dijitalleştirilmesi programı kapsamına tarım da alınmış, "Tarımsal Sanayi Kompleksinin Dijitalleştirilmesi" başlığı altında "Hassas Tarım", "Hayvancılık ve Bitkisel Üretiminde Kontrol Edilebilirlik" ve "E-Agrotrade" gibi uygulamaların hayata geçirilmesi hedeflenmiştir.

Bu projeler tamamlandığında Kazakistan ekonomi alanında önemli ölçüde dijitalleşme hayat geçirmiş olacaktır.

2. Dijital Devlete Geçiş



Şekil 5. *Dijital Devlete Geçiş*

Kaynak: eGov.kz Portalı: "Transition to the Digital State", https://egov.kz/cms/en/digital-kazakhstan Erişim tarihi: 28.05.2024

"Dijital Kazakhstan" Programının temel hedeflerinden bir diğeri de Dijital Devlete Geçiş'tir. E-Gov uygulamasıyla bu alanda önemli başarılar elde etmiş olan Kazakistan, yeni hedeflerle dijital devlete geçişi tamamlamayı hedeflemektedir. Bu amaçla başlatılan çalışmalardan biri "Devletten Vatandaşa" projesidir. Bu amaçla, Paper-free (Kağıtsız İş Akışı), Elektronik Emek Değişimi, "Birleşik Devlet Emlak Kadastrosu" Bilgi Sistemi, e-Health (Elektronik Sağlık Hizmetleri) gibi hizmetler devreye alınmaktadır.

Dijital Devlete Geçiş programı bağlamında hedeflenen bir diğer dijitalleşme de "Devletten İşletmeye" başlığıyla tanımlanan projedir. Bu kapsamda "İhracat ve İthalat İşlemlerinde Tek Pencere", "Küçük ve Orta Boyutlu İşletmeler İçin Desteğin Dijitalleştirilmesi", "Sanal Depolama Alanı" gibi projeler hayata geçirilmek istenmektedir. Yine "Devlet Organlarının İç Faaliyetlerinin Dijitalleştirilmesi" başlığı altında mevcut e-Gov platformunun geliştirilmesi hedeflenmektedir. Ayrıca, "Suçların Önlenmesi", "Akıllı Şehirler", Elektronik PİK (Daire sahiplerinin kooperatifi), Smart City ("Smart Almaty", "Smart Astana", "Smart Aktöbe", "Smart Karagandı", "Smart Ontüstik") gibi hedefler belirlenmiştir.

3. Dijital İpek Yolu

Dijital Kazakhstan Programının temel hedeflerinin üçüncüsü ise Dijital İpek Yolu olarak belirlenmiştir. Bunun için BİT altyapısının geliştirilmesi, Geniş Bant Erişimi, 5G bağlantısı, KazSat-2R uzay teknolojisi programı gibi projeler ortaya konulmuştur.

Dijital İpek Yolu kapsamında hedeflenen en önemli başlıklardan biri de "Siber Güvenlik"tir. Bunun için Big Data Analizi, Zararlı Yazılım Analizi, Bilgi Güvenliği Standartları gibi çalışmalar yapılmaktadır.

4. İnsan Sermayesinin Gelişimi

Dijital Kazakhstan Programının dördüncü temel hedefi de insan sermayesinin geliştirilmesi olarak belirlenmiştir. Bu proje kapsamında nüfusun niteliğinin arttırılması, ihtiyaçları karşılayabilecek öz nüfus birikimi oluşturulması istenmektedir.

5. İnovasyon Ekosisteminin Oluşturulması

"Dijital Kazakhstan" Programı kapsamında belirlenen son temel hedef ise inovasyon ekosisteminin oluşturulmasıdır. Bu hedefe ulaşabilmek için de "*Startup Kültürü*", "Yenilikçi gelişim için bir platform", elverişli koşullar yaratarak uluslararası girişimcileri çekmek amaçlı "teknoloji girişimcilik ve startup kültürü", "girişim

finansmanı" gibi projeler belirlenmiş ve inovasyonları güçlü şekilde destekleme kararı alınmıştır.

Öte yandan Kazakistan devleti, halkın en çok hangi elektronik hizmetleri aldığına dair EGov.kz portalının ana sayfasında bir bölüm açmıştır. "Elektronik Hizmetler Bloğu" adı altında açılan bu sekmede yer alan verilere göre, Kazakistan halkının en çok talep ettiği elektronik hizmetler şu şekildedir (EGov.kz, 28 Mayıs 2024):

1. Yaklaşan vergi ödemelerini gözden geçirme ve ödeme,
2. Elektronik portal üzerinden alınan hizmetlerin doğrulanması,
3. Elektronik dilekçe,
4. Vatandaşların mobil veritabanında kayıt olup olmadıklarını kontrol etmek,
5. Üçüncü taraflardan belgele alma hizmeti,
6. Elektronik imza almak veya yeniden e-imza başvurusunda bulunmak,
7. Bireylerin işlem hareketlerini kayıt altına alma ve kontrol etme hizmeti.
8. Temel emeklilik ödemesi miktarının hesaplanmasına ilişkin belge.
9. Belirtilen alıcıya devletin verdiği garantiyle ilgili atama ve ödeme bilgilerinin temin edilmesi.

Sonuç olarak, Kazakistan'da dijitalleşme uygulamaları devlet öncülüğünde her alanda genişlemekte ve gelişmektedir. Bu durum çeşitli avantajlara sahip olmakla birlikte çalışmamız bağlamında gözetleme ve mahremiyetin ortadan kalkması gibi çeşitli sakıncaların da artması anlamına gelmektedir.

3.2.2. Araştırmanın Amacı ve Önemi

Bu çalışmanın temel amacı, Kazakistan'daki yükseköğretim (lisans, yüksek lisans ve doktora) mezun ve öğrencilerinin sosyal medya platformlarında gözetim altında kalıp kalmadıklarını ve özel yaşamlarına ilişkin paylaşımlarında mahremiyet kaygısı taşıyıp taşımadıklarını incelemektir. Konuya ilişkin yapılan literatür taramasında, sosyal medya bağlamında mahremiyet ve gözetim kavramlarını ele alan birçok çalışmaya rastlanmıştır. Türkiye'de çeşitli şehirlerde gerçekleştirilen çalışmalarda, mahremiyet kavramının nasıl evrildiği ve sosyal medyanın mahremiyet algısı üzerindeki etkileri kapsamlı şekilde ele alınmıştır. Bu çalışmada ise, Kazakistan'daki gençlerin gözetim farkındalığı, mahremiyet algısı, sosyal medya ve teknoloji kullanımına dair düşünce ve davranışlarına odaklanılmıştır.

Öte yandan, Türkiye'de medya ve kitle iletişim araçları üzerinden bu konu hakkında düzenli bilgilendirmeler yapılmasına rağmen, Kazakistan'da durumun farklılık arz ettiği söylenebilir. Ülkede internetin 1994'te kullanılmaya başlamasıyla birlikte, mahremiyet ve gözetim gibi kavramların ele alındığı güvenlik, haber, yorum ve bilimsel araştırma içeriklerinin internet ortamında sınırlı sayıda olduğu görülmektedir. Bu nedenle, yürütülen araştırma bilimsel alanda bu konuyu ele alan ilk çalışma olma özelliğini taşımaktadır. Ayrıca, çalışmada ele alınan mahremiyet ve gözetim tartışmaları, yeni medya ile ilgili konulara da katkı sunabilecek nitelikte bir bilgilendirme projesi olarak değerlendirilebilir.

3.2.3. Varsayımlar ve Sınırlılıklar

Bu araştırmanın temel varsayımlarından biri, Kazakistan'da yaşayan bireylerin internette uzun süre vakit geçirmelerine rağmen, internet ve sosyal medya kullanımında mahremiyet ve gözetim konularına dair gelişmelerden yeterince haberdar olmadıkları yönündedir. Ayrıca, bu bireylerin genel anlamda mahremiyet kavramına ilişkin bir farkındalığa sahip olsalar da, mahremiyetin sosyal medya bağlamında nasıl dönüştüğü hususunda yeterli bilgiye sahip olmadıkları öngörülmektedir.

Çalışmanın örneklemi ise yalnızca Kazakistan'ın farklı bölgelerinden seçilmiş yükseköğretim öğrencileri ve mezunları ile sınırlı tutulmuştur.

3.2.4. Araştırma Yöntemi

Bu araştırmada kullanılan yöntem, görüşme sırasında ele alınacak soru ve konu başlıklarını içermektedir. Patton (1987: s. 111), "Görüşme formu yöntemi, aynı konu çerçevesinde farklı bireylerden benzer bilgilerin toplanmasını sağlamak amacıyla düzenlenir" ifadesini kullanmaktadır. Görüşmeyi yürüten kişi, daha önce hazırlanan konu ya da alanlara bağlı kalarak hem önceden belirlenmiş soruları sorabilir hem de gerek gördüğünde ek sorular yönelterek daha ayrıntılı bilgilere ulaşma fırsatına sahiptir. Soruların ya da konu başlıklarının belirli bir sıraya göre düzenlenmesi zorunlu değildir. Görüşme formu, araştırma konusunun tüm yönleriyle ele alınmasını ve ilgili tüm soruların yanıtlanmasını temin etmeye yönelik bir yöntemdir. Görüşmeci, görüşme sırasında soru cümlelerinin yapısını ya da sırasını değiştirme özgürlüğüne sahip olduğu gibi, sohbet havasında ilerleyen bir görüşme de gerçekleştirebilir (Yıldırım ve Şimşek, 2011: s. 122).

Nitel araştırma yöntemleri içinde, yarı yapılandırılmış derinlemesine görüşme tekniği en yaygın veri toplama aracı olarak kullanılmaktadır (Yıldırım ve Şimşek, 2011). Bu görüşme biçimi, katılımcıların kendi perspektiflerini ortaya koyarak dünyayı nasıl algıladıklarını ifade etmelerine olanak tanımaktadır. Katılımcıların bu dünyayı anlatabilmeleri için soruların çoğu zaman açık uçlu olması önem arz etmektedir. Bu tür görüşmelerde ya her soru esnek bir şekilde formüle edilmeli ya da görüşme, çeşitli yapılandırılmış tekniklerden yararlanılarak hazırlanmalıdır (Merriam ve Tisdell, 2013: s. 110-111).

Yarı yapılandırılmış görüşme tekniği birtakım avantajlar sunmaktadır. İlk olarak, araştırmacıya zaman açısından esneklik sağlamaktadır. Örneğin, görüşmeci yanıtlanmış soruları tekrarlamaktan kaçınabilir, bazı soruları atlayabilir ya da sormaktan vazgeçebilir. Ayrıca, belirli bir form üzerinden yürütülen görüşmeler sayesinde, farklı bireylerden elde edilen bilgiler daha sistematik ve karşılaştırılabilir bir biçimde toplanabilmektedir. Yapılandırılmamış görüşme tekniklerine kıyasla, bu yolla elde edilen verilerin düzenlenmesi ve analiz edilmesi daha kolaydır. Çünkü veriler, görüşme formunda yer alan soru ve konu başlıkları doğrultusunda sınıflandırılmaktadır (Yıldırım ve Şimşek, 2011: s. 122-123). Bu nedenlerle, çalışmada Kazakistan'da yükseköğretim gören ve mezun bireylerin gözetim ve mahremiyet kavramlarına ilişkin farklı bakış açılarını ortaya koyabilmek amacıyla nitel araştırma yöntemlerinden yarı yapılandırılmış görüşme tekniği tercih edilmiştir.

Görüşmeler sırasında ele alınacak soru ve konu başlıkları, yüz yüze ve telefonla yapılan görüşmelerle katılımcılara yöneltilmiştir. Ancak, bazı katılımcılarla Kazakistan'a gitme imkânı bulunmadığından dolayı, bu kişilere e-posta yoluyla görüşme formları gönderilmiş ve sorular bu formlar aracılığıyla yanıtlanmıştır. Açık uçlu sorular kullanılarak görüşme formunun sınırlarının ötesine çıkılmış, böylece yarı yapılandırılmış görüşme tekniği aracılığıyla katılımcıların görüş ve düşüncelerine ilişkin en kapsamlı veriler toplanmıştır.

Bu araştırmada yarı yapılandırılmış görüşme tekniğinin tercih edilmesinin temel nedeni, gözetim ve mahremiyet kavramlarının her toplum ve bireyde farklı şekillerde tanımlanıp yorumlandığını göz önünde bulundurarak, katılımcıların bu konudaki çeşitli görüşlerini kapsamlı bir şekilde ele alabilmek ve verilerin analiz aşamasında daha kapsamlı ve verimli sonuçlara ulaşabilmektir.

3.2.5. Veri Toplama Süreci ve Araştırmanın Örneklem Seçimi

Nicel araştırma paradigması içinde gelişen ancak araştırmacılar tarafından sınırlı düzeyde kullanılan olasılığa dayalı örnekleme yöntemlerinin aksine, amaçlı örnekleme teknikleri esasen nitel araştırma yaklaşımı çerçevesinde geliştirilmiştir. Patton'a (1987) göre, olasılığa dayalı örnekleme evreni temsil etme yoluyla geçerli genellemeler yapmayı mümkün kılarken, amaçlı örnekleme ise zengin ve derinlemesine bilgi sunabilen durumların kapsamlı incelenmesine olanak tanır. Bu bağlamda, amaçlı örnekleme yöntemleri birçok durumda olgu ve fenomenlerin keşfi ve açıklanması açısından önemli katkılar sağlamaktadır (Yıldırım ve Şimşek, 2011: s. 107).

Bu araştırmada, Kazakistan'da yükseköğretim gören ve öğrenim görmekte olan toplam 71 katılımcıyla görüşmeler gerçekleştirilmiş olup, değerlendirilmeye alınan yanıt sayısı 68'dir. Çalışmanın temsil gücünü artırmak amacıyla, katılımcılar farklı akademik bölümlerden ve ülkenin çeşitli eyaletlerinden (oblıs) seçilmiştir; ayrıca, geçici olarak yurt dışında bulunan bireyler de örneklem kapsamında yer almıştır. Örneklem seçiminde kartopu (zincir) örnekleme yöntemi uygulanmıştır.

Kartopu örnekleme sürecinde araştırmacı, incelediği olgu veya konu hakkında en fazla bilgiye sahip olduğunu düşündüğü kişi veya durumları belirleyerek, şu soruları sorarak süreci başlatır: "Bu konuda en fazla bilgi sahibi kimdir? Görüşmelere kiminle başlanmalıdır?" (Flick, 2009: s. 109). Araştırma ilerledikçe elde edilen yeni kişi ve durumlar, kartopunun büyümesi gibi artar ve belirli bir noktadan sonra bazı isimler daha fazla ön plana çıkar; bu aşamada görüşülmesi gereken kişi sayısı ve dikkate alınacak durumlar azalmaya başlar (Yıldırım ve Şimşek, 2011: s. 111).

Miles ve Huberman (1994) ile Patton (2005)'in yaklaşımlarından uyarlanarak nitel araştırmalarda kartopu ya da zincir örnekleme yöntemlerinin amacı "kişiden kişiye, oradan da durumlara geçerek farklı olguları açıklamak" şeklinde tanımlanmaktadır (Baltacı, 2018: s. 246-247). Bu yöntemin özellikle hassas konular veya erişilmesi güç topluluklara ulaşmak için etkin olduğu bilinmektedir. Bu çalışma bağlamında ise, sosyal medyayı yoğun kullanan katılımcılara erişimi kolaylaştırmak ve daha sağlıklı veri toplamak amacıyla kartopu örnekleme yöntemi tercih edilmiştir. Bu kapsamda, Kazakistan'da yükseköğretim gören ve görmekte olan bireyler ile çalışma yapılmıştır. Çalışmada 18-24, 25-34, 35-44, 45-54 yaş gruplarındaki yükseköğretim gören ve görmekte olan kişiler ile görüşülmüştür.

Görüşmeler, 2025 yılının Mart ve Nisan ayları arasında gerçekleştirilmiş olup, katılımcıların gönüllülüğü esas alınmıştır. Telefon aracılığıyla yapılan görüşmeler kayıt altına alınmış ve görüşme sırasında kısa notlar tutulmuştur. Ayrıca, katılımcılara e-posta yoluyla da anket formları gönderilerek, gönüllü olmaları koşuluyla bu formları doldurmaları talep edilmiştir. Anket soruları Kazakça, Rusça, Türkçe ve İngilizce olmak üzere dört farklı dilde hazırlanmıştır. Araştırmada elde edilen veriler katılımcıların kimliklerini gizleyecek şekilde anonimleştirilmiştir.

3.2.6. Verilerin Analizi

Araştırmada, katılımcılar tercih ettikleri dilde yanıtlarını vermiştir. İlk aşamada, Kazakça, Rusça ve İngilizce dillerinde alınan yanıtlar Türkçeye çevrilmiştir. Görüşme yöntemiyle toplanan veriler, sınıflandırılarak analiz edilmiş; böylece katılımcıların cevapları arasındaki benzerlikler ve farklılıklar ortaya konmuştur. Elde edilen bulgular, katılımcıların düşüncelerini daha doğru yansıtmak amacıyla doğrudan alıntılarla desteklenmiştir.

3.2.7. Araştırmanın Soruları

Bu çalışmanın temel amacı, Kazakistan'da yükseköğretim (lisans, yüksek lisans ve doktora) mezun ve öğrencilerin sosyal medya platformlarında maruz kaldıkları gözetim durumları ve özel hayatlarına ilişkin paylaşımlarında mahremiyet endişesi duyup duymadıklarını incelemektir. Ayrıca, çalışmada aşağıdaki temel sorulara da yanıt aranmıştır:

1. *Kazakistan'da yükseköğretim mezun ve öğrencilerin mahremiyet kavramını nasıl değerlendirdikleri ve zaman içinde bu kavrama ilişkin algılarında meydana gelen değişimlerin sebepleri;*
2. *Bu bireylerin sosyal medya platformlarında gözetim altında bulunduklarının farkında olup olmadıkları ve sosyal medyayı gözetim aracı olarak görüp görmedikleri;*
3. *İnternet ortamında kişisel bilgilerinin güvende olup olmadığına ilişkin algıları ile bu konuda herhangi bir koruyucu önlem alıp almadıkları;*

şeklinde belirlenmiştir.

3.3. Bulguların Yorumlanması

Bu bölümde, Kazakistan'da yükseköğretim mezun ve öğrencilerin yanıtları analiz edilmiştir. Öncelikle katılımcılar demografik özelliklerine göre sınıflandırılmıştır. Ardından, görüşme sırasında yöneltilen sorulara verilen yanıtlar konu başlıkları altında (mahremiyet algısı, gözetim farkındalığı gibi) kategorize edilerek detaylı bir şekilde incelenmiş, yorumlanmış ve içerikler arasındaki ilişkiler doğrultusunda değerlendirilmiştir.

3.3.1. Katılımcı Özellikleri

Görüşmeler, Kazakistan'da çeşitli disiplinlerde yükseköğretim mezun ve öğrencilerin katılımıyla gerçekleştirilmiştir. Katılımcıların demografik bilgileri Tablo 2'de sunulmaktadır. Araştırma grubunu, 18-64 yaş aralığında (altı farklı yaş grubu) bulunan 68 kişi oluşturmakta olup, bunların 45'i erkek, 23'ü ise kadındır.

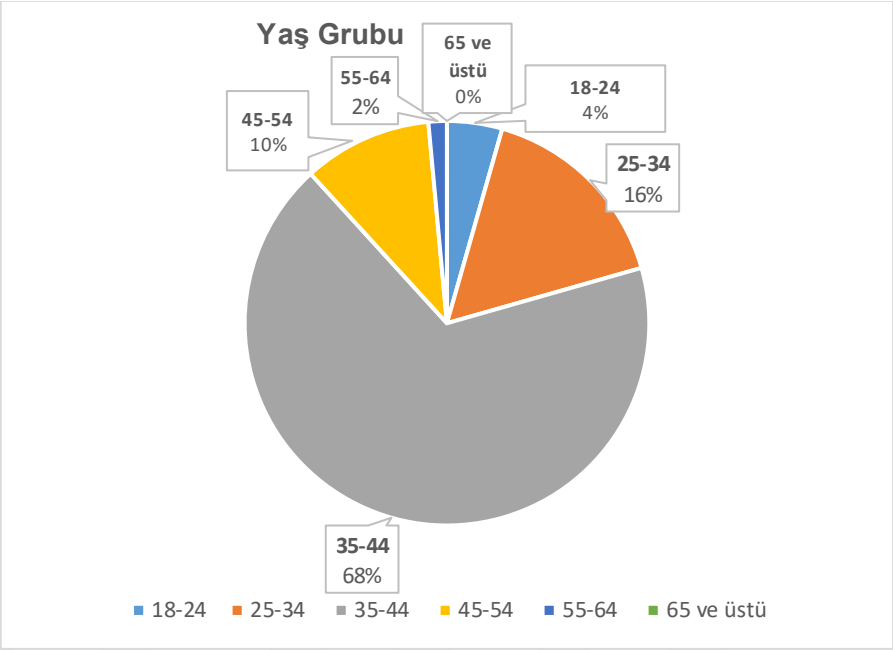
Tablo 2. Katılımcıların Özellikleri

Katılımcı No.	Yaş Grubu	Cinsiyet	Şehir / Ülke	Eğitim Durumu
Katılımcı 1	25-34	Erkek	Karagandı / Kazakistan	Lisans
Katılımcı 2	35-44	Kadın	Astana / Kazakistan	Yüksek lisans
Katılımcı 3	35-44	Kadın	Talgar (Almatı) / Kazakistan	Yüksek lisans
Katılımcı 4	45-54	Kadın	Antalya / Türkiye	Yüksek lisans
Katılımcı 5	35-44	Kadın	Astana / Kazakistan	Yüksek lisans
Katılımcı 6	35-44	Kadın	Astana / Kazakistan	Yüksek lisans
Katılımcı 7	35-44	Kadın	Kızılorda / Kazakistan	Lisans
Katılımcı 8	35-44	Kadın	Astana / Kazakistan	Yüksek lisans
Katılımcı 9	25-34	Erkek	Türkistan / Kazakistan	Yüksek lisans
Katılımcı 10	35-44	Erkek	Türkistan / Kazakistan	Doktora
Katılımcı 11	35-44	Erkek	Astana / Kazakistan	Doktora
Katılımcı 12	55-64	Erkek	Astana / Kazakistan	Yüksek lisans
Katılımcı 13	45-54	Erkek	Astana / Kazakistan	Lisans
Katılımcı 14	35-44	Kadın	Almatı / Kazakistan	Doktora
Katılımcı 15	35-44	Erkek	Astana / Kazakistan	Lisans
Katılımcı 16	35-44	Erkek	Almatı / Kazakistan	Lisans
Katılımcı 17	35-44	Erkek	Astana / Kazakistan	Yüksek lisans

Katılımcı 18	35-44	Kadın	Taraz / Kazakistan	Lisans
KKatılımcı 19	35-44	Kadın	İstanbul / Türkiye	Yüksek lisans
Katılımcı 20	35-44	Kadın	Astana / Kazakistan	Yüksek lisans
Katılımcı 21	35-44	Erkek	Aktöbe / Kazakistan	Yüksek lisans
Katılımcı 22	45-54	Erkek	Astana / Kazakistan	Yüksek lisans
Katılımcı 23	35-44	Kadın	Ankara / Türkiye	Yüksek lisans
Katılımcı 24	35-44	Erkek	Astana / Kazakistan	Lisans
Katılımcı 25	35-44	Erkek	Astana / Kazakistan	Doktora
Katılımcı 26	45-54	Kadın	Astana / Kazakistan	Lisans
Katılımcı 27	35-44	Erkek	Almatı / Kazakistan	Doktora
Katılımcı 28	35-44	Kadın	Türkistan / Kazakistan	Doktora
Katılımcı 29	35-44	Erkek	Astana / Kazakistan	Doktora
Katılımcı 30	35-44	Erkek	Kosşı (Akmola) / Kazakistan	Lisans
Katılımcı 31	35-44	Erkek	Aktöbe / Kazakistan	Doktora
Katılımcı 32	35-44	Kadın	Londra / İngiltere	Doktora
Katılımcı 33	35-44	Kadın	Öskemen / Kazakistan	Yüksek lisans
Katılımcı 34	25-34	Erkek	Astana / Kazakistan	Lisans
Katılımcı 35	35-44	Kadın	İstanbul / Türkiye	Yüksek lisans
Katılımcı 36	35-44	Kadın	Astana / Kazakistan	Yüksek lisans
Katılımcı 37	25-34	Erkek	Astana / Kazakistan	Doktora
Katılımcı 38	35-44	Kadın	Astana / Kazakistan	Yüksek lisans
Katılımcı 39	25-34	Erkek	Astana / Kazakistan	Yüksek lisans
Katılımcı 40	35-44	Erkek	Astana / Kazakistan	Yüksek lisans
Katılımcı 41	35-44	Kadın	Astana / Kazakistan	Yüksek lisans
Katılımcı 42	35-44	Erkek	Astana / Kazakistan	Yüksek lisans
Katılımcı 43	25-34	Erkek	Astana / Kazakistan	Lisans
Katılımcı 44	35-44	Erkek	Astana / Kazakistan	Doktora
Katılımcı 45	35-44	Erkek	Astana / Kazakistan	Yüksek lisans
Katılımcı 46	18-24	Erkek	Taldıkorgan / Kazakistan	Lisans
Katılımcı 47	18-24	Erkek	İstanbul / Türkiye	Lisans
Katılımcı 48	35-44	Erkek	Astana / Kazakistan	Lisans
Katılımcı 49	35-44	Erkek	Almatı / Kazakistan	Yüksek lisans
Katılımcı 50	35-44	Erkek	Atırau / Kazakistan	Yüksek lisans

Katılımcı 51	25-34	Kadın	Ankara / Türkiye	Doktora
Katılımcı 52	35-44	Erkek	Astana / Kazakistan	Lisans
Katılımcı 53	18-24	Erkek	İstanbul / Türkiye	Lisans
Katılımcı 54	35-44	Erkek	Türkistan / Kazakistan	Lisans
Katılımcı 55	25-34	Erkek	Astana / Kazakistan	Yüksek lisans
Katılımcı 56	35-44	Erkek	Astana / Kazakistan	Yüksek lisans
Katılımcı 57	25-34	Erkek	Astana / Kazakistan	Yüksek lisans
Katılımcı 58	35-44	Kadın	Niğde / Türkiye	Doktora
Katılımcı 59	35-44	Erkek	Aktau / Kazakistan	Yüksek lisans
Katılımcı 60	25-34	Erkek	Astana / Kazakistan	Doktora
Katılımcı 61	45-54	Kadın	Astana / Kazakistan	Doktora
Katılımcı 62	25-34	Erkek	Almatı / Kazakistan	Doktora
Katılımcı 63	35-44	Erkek	Astana / Kazakistan	Doktora
Katılımcı 64	45-54	Erkek	Taraz / Kazakistan	Doktora
Katılımcı 65	35-44	Erkek	Astana / Kazakistan	Doktora
Katılımcı 66	45-54	Erkek	Astana / Kazakistan	Lisans
Katılımcı 67	35-44	Erkek	Taldıkorgan / Kazakistan	Lisans
Katılımcı 68	35-44	Erkek	Kaliforniya / ABD	Doktora

Araştırmada, katılımcıların yaş dağılımlarını belirlemek için görüşme formunda *"Lütfen yaş grubunuzu seçiniz:"* sorusu yöneltilmiştir. Alınan yanıtlar doğrultusunda, yaş grupları *18-24* yaş arası 3 kişi, *25-34* yaş arası 11 kişi, *35-44* yaş arası 46 kişi, *45-54* yaş arası 7 kişi, *55-64* yaş arası 1 kişi ve *65 yaş üstü* ise 0 kişi olacak şekilde sınıflandırılmıştır. Bu sınıflandırma, Şekil 6'da görsel olarak sunulmaktadır.



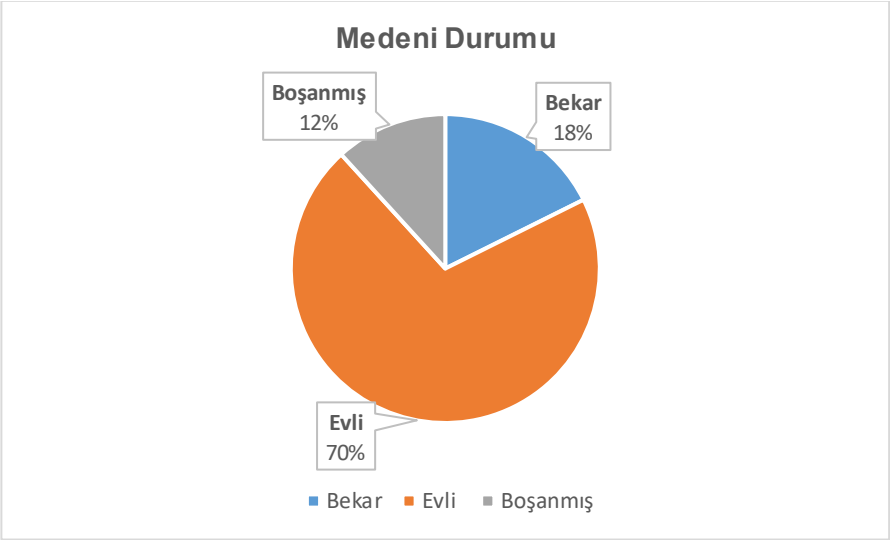
Şekil 6. *Katılımcıların Yaş Grubu*

45 erkek (%66), 23 kadın (%34) olmak üzere, katılımcıların cinsiyeti Şekil 7'de gösterilmiştir.



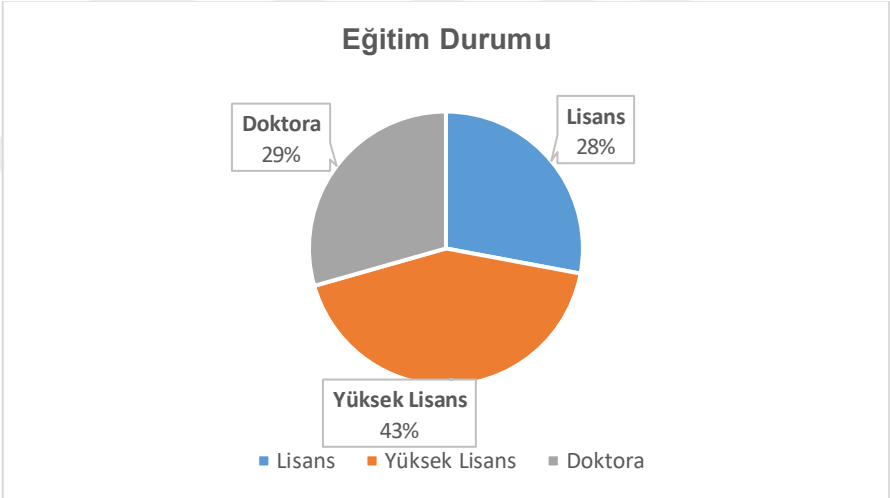
Şekil 7. *Katılımcıların Cinsiyeti*

Katılımcıların medeni durumu ise, *Bekar* 12 kişi, *Evli* 48 kişi ve *Boşanmış* 8 kişi ile ilgili veriler Şekil 8'de verilmiştir.



Şekil 8. *Katılımcıların Medeni Durumu*

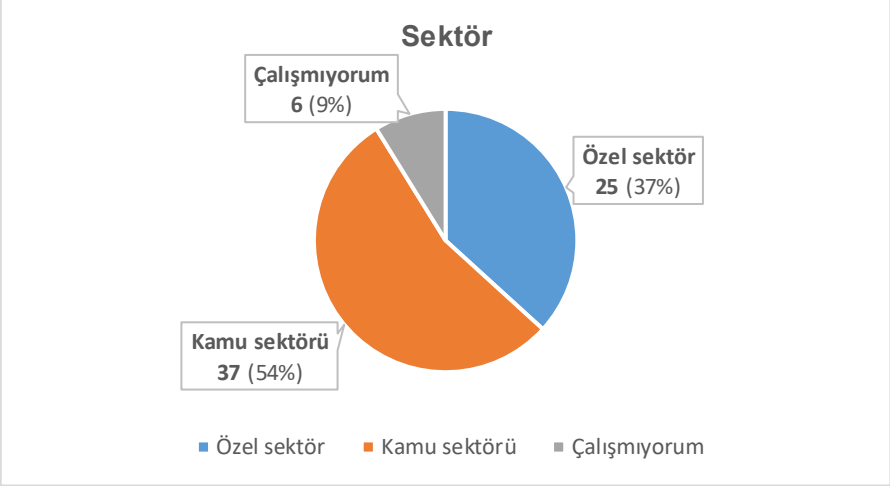
Katılımcıların (*Lisans* 19 kişi, *Yüksek lisans* 29 kişi ve *Doktora* 20 kişi) verdiği cevaplara göre, eğitim durumu Şekil 9'da görselleştirilmektedir.



Şekil 9. *Katılımcıların Eğitim Durumu*

Katılımcılar yükseköğretim mezun ve öğrenci bireylerdir. Şu anda 58 kişi Kazakistan'da, 8 kişi Türkiye'de, 1 kişi İngiltere'de ve 1 kişi ABD'de yaşamakta olan Kazakistan vatandaşlarıdır.

Araştırmada, katılımcıların çalışıp çalışmadığını tespit etmek amacıyla görüşme formunda *"Hangi sektörde çalışmaktasınız?"* sorusu sorulmuştur. Katılımcıların verdiği cevaplara göre, *Özel sektörde* 25 kişi, *Kamu sektörde* 37 kişi çalışmaktadır ve 6 kişi "*Çalışmıyorum"* yanıtını vermiştir (Şekil 10.).

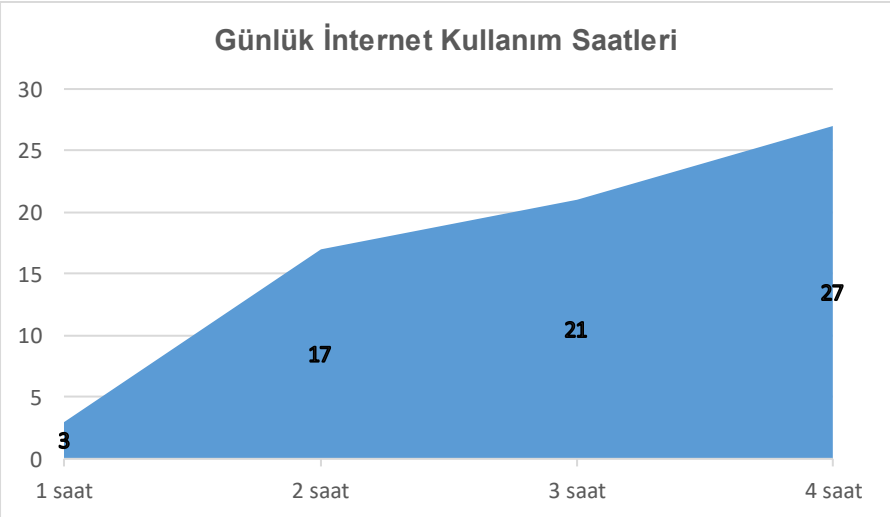


Şekil 10. *Katılımcıların Çalıştığı Sektörler*

3.3.2. Katılımcıların Sosyal Medya Alışkanlıkları

Araştırmada, katılımcılara *"Sosyal medya kullanıyor musunuz?"* sorusu yöneltilmiştir. Verilen yanıtlar sonucunda, tüm katılımcıların (%100) sosyal medya kullandığı belirlenmiştir. Ayrıca, *"Sosyal medyayı ne kadar süredir kullanıyorsunuz?"* sorusuna katılımcıların tamamı "4 yıl ve üzeri" şeklinde yanıt vermiştir.

Katılımcıların sosyal medya kullanım alışkanlıklarını anlamak için görüşme formunda *"Günde ortalama ne kadar süre internet kullanıyorsunuz?"* sorusu da sorulmuştur. Bu soruya verilen yanıtların ortalaması, Şekil 11'de grafik olarak sunulmuştur.



Şekil 11. *Günlük Sosyal Medya Kullanımı Saat Ortalaması*

Katılımcıların kullandığı sosyal medya platformları ve günlük internet kullanım süreleri farklılık göstermektedir. Bu çeşitliliği ortaya koymak için, katılımcıların aktif olarak kullandıkları sosyal medya araçları ve günlük internet kullanım süreleri Tablo 3'te yer almaktadır. Erkek katılımcıların (45 kişi) günlük sosyal medya kullanım süresi ortalama 3,02 saat iken, kadın katılımcıların (23 kişi) günlük ortalama sosyal medya kullanımı ise 3,13 saattir.

Tablo 3. *Katılımcıların Günlük İnternet Kullanım Süreleri ve Kullandıkları Sosyal Medya Araçları*

Katılımcı No.	**İnternete Bağlı Olunan Yaklaşık Süre (saat)**	**Kullanılan Sosyal Medya Araçları**
Katılımcı 1	2	WhatsApp, Instagram, Telegram, Mail.ru, Facebook
Katılımcı 2	4 saat ve üzeri	WhatsApp, Instagram, Facebook
Katılımcı 3	1	WhatsApp, Instagram, Facebook
Katılımcı 4	4 saat ve üzeri	Instagram, Facebook, WhatsApp
Katılımcı 5	3	Instagram, WhatsApp, Telegram
Katılımcı 6	1	Facebook, Instagram, LinkedIn
Katılımcı 7	4 saat ve üzeri	Instagram, TikTok, WhatsApp, Telegram
Katılımcı 8	4 saat ve üzeri	Instagram, WhatsApp, Telegram
Katılımcı 9	4 saat ve üzeri	Facebook, Telegram, Instagram
Katılımcı 10	3	WhatsApp, Telegram, Facebook, Instagram
Katılımcı 11	3	WhatsApp, Facebook, Mail.ru, VK
Katılımcı 12	4 saat ve üzeri	Facebook, WhatsApp, Mail.ru
Katılımcı 13	4 saat ve üzeri	Instagram, Facebook, TikTok
Katılımcı 14	4 saat ve üzeri	Instagram, Facebook, TikTok
Katılımcı 15	4 saat ve üzeri	Instagram, Facebook, WhatsApp
Katılımcı 16	4 saat ve üzeri	Instagram, Telegram, WhatsApp
Katılımcı 17	3	WhatsApp
Katılımcı 18	2	Facebook, Mail.ru, TikTok
Katılımcı 19	4 saat ve üzeri	Facebook, Instagram, WhatsApp, Mail.ru
Katılımcı 20	3	WhatsApp, Instagram, Telegram
Katılımcı 21	4 saat ve üzeri	Facebook, Instagram, Telegram
Katılımcı 22	4 saat ve üzeri	Telegram, Instagram, Facebook, TikTok

Katılımcı 23	2	WhatsApp, Instagram, Facebook
Katılımcı 24	2	Telegram, Whatsapp, Instagram
Katılımcı 25	1	WhatsApp, Facebook, Twitter
Katılımcı 26	3	WhatsApp, Instagram, Telegram
Katılımcı 27	3	WeChat, Facebook, TikTok, Mail.ru
Katılımcı 28	4 saat ve üzeri	Facebook, Instagram, WhatsApp
Katılımcı 29	4 saat ve üzeri	Facebook, Instagram, Telegram
Katılımcı 30	3	Facebook, WhatsApp, Instagram
Katılımcı 31	2	WhatsApp, Facebook, Instagram
Katılımcı 32	3	WhatsApp, Instagram, Facebook
Katılımcı 33	4 saat ve üzeri	Instagram, Facebook, WhatsApp, Telegram, LinkedIn
Katılımcı 34	2	WhatsApp, Facebook, Instagram
Katılımcı 35	3	WhatsApp, Instagram, LinkedIn
Katılımcı 36	2	Instagram, Facebook, WhatsApp, Mail.ru
Katılımcı 37	2	WhatsApp, Telegram, Facebook, Instagram
Katılımcı 38	4 saat ve üzeri	Facebook, WhatsApp, Instagram
Katılımcı 39	3	Facebook, Instagram, WhatsApp
Katılımcı 40	4 saat ve üzeri	WhatsApp, Telegram, Instagram
Katılımcı 41	4 saat ve üzeri	Facebook, Instagram, Telegram
Katılımcı 42	2	TikTok, Facebook, Instagram
Katılımcı 43	4 saat ve üzeri	WhatsApp, Telegram, Instagram, TikTok, Facebook
Katılımcı 44	3	Facebook, Instagram, WhatsApp
Katılımcı 45	4 saat ve üzeri	Facebook, Telegram, YouTube
Katılımcı 46	2	Instagram, WhatsApp, TikTok
Katılımcı 47	3	Instagram, Telegram, WhatsApp
Katılımcı 48	2	WhatsApp, Instagram, Facebook
Katılımcı 49	2	WhatsApp, Instagram, Facebook
Katılımcı 50	2	Telegram, Twitter, Facebook
Katılımcı 51	2	Instagram, WhatsApp
Katılımcı 52	2	WhatsApp, Facebook, Instagram
Katılımcı 53	3	Instagram, WhatsApp, TikTok
Katılımcı 54	3	Facebook, Instagram, WhatsApp
Katılımcı 55	3	Instagram, TikTok, Facebook

Katılımcı 56	4 saat ve üzeri	Facebook, Instagram, WhatsApp, Telegram
Katılımcı 57	2	WhatsApp, Instagram, TikTok, Facebook, Mail.ru
Katılımcı 58	3	WhatsApp, Instagram, Facebook, Telegram
Katılımcı 59	4 saat ve üzeri	WhatsApp, Telegram, Instagram
Katılımcı 60	3	Facebook, Instagram, Telegram
Katılımcı 61	4 saat ve üzeri	WhatsApp, Telegram, Facebook
Katılımcı 62	4 saat ve üzeri	Instagram, Facebook, Telegram
Katılımcı 63	4 saat ve üzeri	Facebook, Telegram, Instagram
Katılımcı 64	2	Facebook, WhatsApp, Telegram
Katılımcı 65	3	Instagram, Facebook, WhatsApp
Katılımcı 66	3	WhatsApp, Telegram, TikTok, Facebook, Instagram
Katılımcı 67	4 saat ve üzeri	WhatsApp, Instagram, TikTok
Katılımcı 68	3	WhatsApp, Facebook, Instagram

Katılımcılar sosyal medyayı farklı nedenlerle kullanmaktadır. Görüşme formunda yer alan bilgilere göre, çoğu katılımcı sosyal medyayı birden fazla amaç doğrultusunda kullanmaktadır. Örneğin, 47 katılımcı sosyal medyayı "Haberleri takip etmek" amacıyla kullanırken, 50 kişi "Bilgi edinmek" için sosyal medyadan yararlanmaktadır. Bunun yanı sıra, 11 kişi sosyal medyayı "Eğlenmek" ve 12 kişi ise "Boş vakit geçirmek" amacıyla kullanmaktadır. 10 katılımcı ise sosyal medyayı "Diğer" nedenlerle kullandığını ifade etmiştir. Katılımcıların sosyal medya kullanım amaçları Tablo 4 ve Şekil 12'de detaylı bir şekilde sınıflandırılmış olarak sunulmuştur.

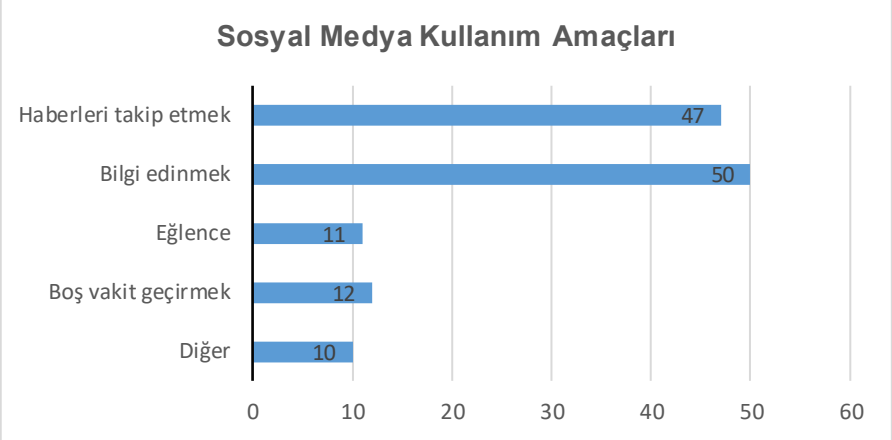
Tablo 4. *Katılımcıların Sosyal Medya Kullanım Amaçları*

Katılımcı No.	**Haberleri takip etmek**	**Bilgi edinmek**	**Eğlence**	**Boş vakit geçirmek**	**Diğer**
Katılımcı 1	✓	✓	✓	✓	
Katılımcı 2		✓			
Katılımcı 3	✓	✓			
Katılımcı 4		✓			✓
Katılımcı 5		✓			
Katılımcı 6	✓	✓	✓		

Katılımcı 7	✓	✓			
Katılımcı 8	✓			✓	
Katılımcı 9		✓			
Katılımcı 10	✓	✓			
Katılımcı 11	✓	✓			
Katılımcı 12	✓	✓			
Katılımcı 13	✓	✓			
Katılımcı 14	✓	✓			
Katılımcı 15		✓		✓	
Katılımcı 16	✓	✓			
Katılımcı 17		✓			
Katılımcı 18		✓			
Katılımcı 19		✓			
Katılımcı 20	✓	✓	✓		
Katılımcı 21	✓	✓			
Katılımcı 22	✓		✓	✓	
Katılımcı 23	✓				
Katılımcı 24		✓			
Katılımcı 25	✓	✓			
Katılımcı 26	✓	✓	✓		✓
Katılımcı 27	✓	✓		✓	✓
Katılımcı 28					✓
Katılımcı 29					✓
Katılımcı 30	✓				
Katılımcı 31	✓				
Katılımcı 32	✓	✓		✓	
Katılımcı 33					✓
Katılımcı 34	✓	✓			
Katılımcı 35	✓	✓			
Katılımcı 36	✓				

Katılımcı 37		✓			
Katılımcı 38	✓	✓	✓		
Katılımcı 39	✓	✓			
Katılımcı 40	✓	✓			
Katılımcı 41	✓	✓			
Katılımcı 42	✓	✓	✓	✓	
Katılımcı 43	✓	✓		✓	
Katılımcı 44	✓				
Katılımcı 45	✓	✓			
Katılımcı 46			✓	✓	
Katılımcı 47	✓	✓	✓	✓	
Katılımcı 48	✓	✓		✓	
Katılımcı 49	✓				✓
Katılımcı 50	✓				
Katılımcı 51					✓
Katılımcı 52		✓			✓
Katılımcı 53	✓	✓	✓		
Katılımcı 54	✓				
Katılımcı 55		✓			
Katılımcı 56	✓	✓			
Katılımcı 57		✓			
Katılımcı 58	✓	✓			
Katılımcı 59	✓	✓			
Katılımcı 60	✓				
Katılımcı 61		✓			
Katılımcı 62					✓
Katılımcı 63	✓				
Katılımcı 64	✓	✓			
Katılımcı 65	✓	✓			
Katılımcı 66	✓	✓	✓	✓	

Katılımcı 67	✓	✓			
Katılımcı 68		✓			



Şekil 12. *Katılımcıların Sosyal Medya Kullanım Amaçları*

Yarı yapılandırılmış görüşmede, katılımcıların sosyal medyayı bilgi edinmek, haberleri takip etmek, boş vakit geçirmek, eğlence ve diğer amaçlar için kullanımını gösteren veri Şekil 12'de verilmiştir.

Sosyal medyayı "Diğer" amacıyla kullanan 10 katılımcı şöyledir:

"Sosyal ağları mesleğim İngiliz dilini öğretmek ve Kazakların dahisi, büyük şair Abay Kunanbayoğlu'nun "Dolu/Olgunlaşmış Adam (Толық адам)" öğretilerini yayma projesinde ve bisiklet yarışçısı olarak çalışmalarımı tanıtmak için kullanıyorum." (Katılımcı 52)

"Sosyal medyayı Qazbilim.kz şirketi reklam amaçlı kullanmaktayız." (Katılımcı 29)

"...kendi hukuk büro işimde kullanıyorum." (Katılımcı 49)

"Günümüzde sosyal medya bilinçsizce, sanki bu bir alışkanlık haline gelmiş gibi..." (Katılımcı 51)

"Sosyal medyayı bilgi edinmek dışında içerikler paylaşmak ve kendi işimi yürütmek için kullanıyorum." (Katılımcı 4)

"Akrabalarım, yakınlarım ve meslektaşlarım ile iletişim halinde olmak için..." (Katılımcı 26)

"Sosyal medyayı yaratıcı çalışmalarımla (edebiyat) bağlantılı olarak reklam için kullanmaktayım." (Katılımcı 62)

"Ticaret ve eğitim amacıyla kullanıyorum." (Katılımcı 28)

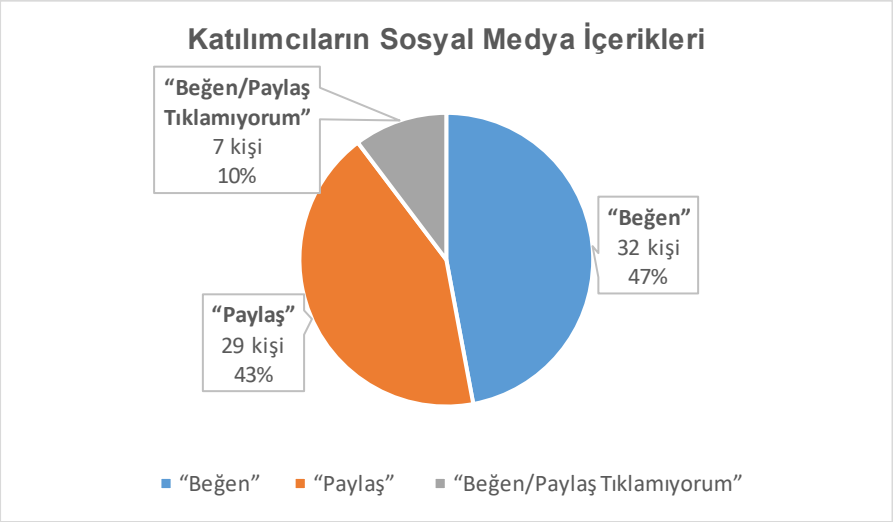
"Genelde sosyal medyayı iş için ve balıkçılık işimi yaygınlaştırmak ve eğitim vermek için kullanıyorum." (Katılımcı 27)

"Reels, kişisel marka gelişimi için kullanıyorum." (Katılımcı 33)

Araştırmada, 68 katılımcılardan 50'si sosyal medyayı "Bilgi edinmek" amaçlı kullanmaktadırlar. Genel olarak katılımcılardan 47'si "Haberleri takip etmek" için kullandıkları ve 12'si ise "Boş vakit geçirmek" ve 11 katılımcının "Eğlence" amaçlı kullandıkları tespit edilmiştir. Sosyal medyayı "Diğer" amaçlı kullanan 10 katılımcılar ise; kendi işi, mesleği, ticaret, eğitim ve yakınları ile iletişim kurmak için kullandıklarını belirtmiştir.

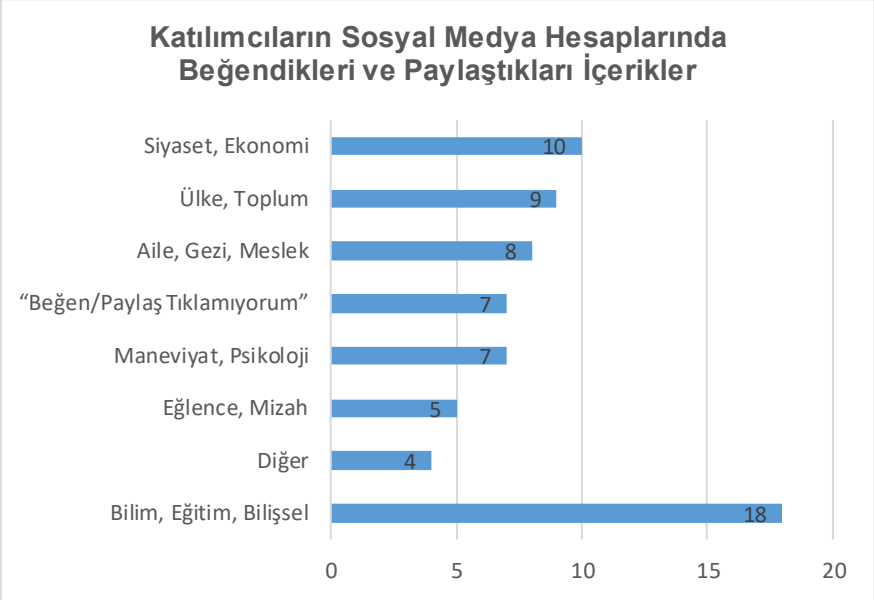
3.3.3. Katılımcıların Sosyal Medya İçerikleri

Katılımcıların sosyal medya hesaplarında ne tür içerikleri paylaştıklarını tespit etmek amacıyla görüşme formunda *"Sosyal medya hesaplarında en çok ne tür içerikler paylaşıyorsunuz ve ne tür içeriklerle ilgili "Beğen" ve/veya "Paylaş" yapıyorsunuz?"* sorusu sorulmuştur. Katılımcıların verdiği cevaplara göre, 32 kişi "Beğen", 29 kişi "Paylaş" butonunu basıyorum ve 7 kişi "Beğen/Paylaş'ı Basmıyorum" şeklinde ifade etmiştir. Şekil 13'te katılımcıların sosyal medya içeriklerle ilgili "Beğen" ve/veya "Paylaş" yapıldığı görselleştirilmektedir.



Şekil 13. *Katılımcıların Cevaplarına Göre Sosyal Medya Hesaplarında İçeriklerin Değerlendirilmesi*

Görüşmede, katılımcıların sosyal medya hesaplarında ne tür içerikleri beğendikleri ve paylaştıklarını gösteren veri Şekil 14'te verilmiştir.



Şekil 14. *Katılımcıların Sosyal Medya Hesaplarında "Beğen" ve "Paylaş" Yaptıkları İçerikler*

Katılımcılardan çoğu sosyal medya hesaplarında bilim, eğitim, bilişsel, spor vb. alanlardaki içeriklere "Beğen" butonunu bastığını dile getirmiştir.

"Sık sık "Beğen" tuşuna basıyorum. Çok beğenirsem, yazara bakmaksızın içerik önemli olduğu sürece paylaşırım." (Katılımcı 27)

"Genelde spor, arabalar, efsaneler ve teknoloji ile ilgili içeriklere "Beğen" yapıyorum." (Katılımcı 66)

"Eğitici dersler, tarihi filmler ile ilgili bilgileri beğeniyor ve paylaşıyorum." (Katılımcı 18)

"Eğitici ve anlamlı içeriklere Beğen'i tıklıyorum." (Katılımcı 10)

"Bilgilendirici, anlamlı, yararlı içerikleri beğeniyorum." (Katılımcı 28)

"Facebook ve WhatsApp'ta değerli, ilginç ve yararlı bilgileri paylaşıyorum." (Katılımcı 11)

"Analiz ve ilgi çekici içeriklere "Beğen"i tıklarım." (Katılımcı 63)

"Eğitim ve bilgilendirici haberleri beğeniyorum." (Katılımcı 41)

"Öğrenme ve eğitim, eğlence ve arkadaşlarımın içeriklerini beğeniyorum." (Katılımcı 47)

"Faydalı, bilgilendirici ve düşündürücü içerikleri beğeniyorum." (Katılımcı 22)

"Halka açık fotoğraflar ve ilginç içerikli materyalleri repost yapıyorum." (Katılımcı 8)

Katılımcılardan 10'u siyaset, iş, ekonomi içerikli bilgileri beğendiğini ve paylaştıklarını ifade etmiştir.

"Sosyo-politik meseleler ve kişisel hayatımdan çeşitli durumlar hakkındaki düşüncelerimi sıklıkla paylaşıyorum. Siyasi konularla ilgili içerikleri çok seviyorum ve çok fazla derin hiciv içeren videolar paylaşıyorum." (Katılımcı 37)

"Siyaset, bilim ve faydalı bilgilerle ilgili içerikleri sık sık paylaşıyorum." (Katılımcı 32)

"Haberlerle veya sanat dünyasıyla ilgili içerikleri beğeniyorum." (Katılımcı 3)

"Siyasi bilgi ve görüşler, yurtdışında eğitim ile ilgili doğru bilgileri paylaşıyorum." (Katılımcı 4)

"Ulusal, siyasal-toplumsal, bilimsel, tarihsel, edebi-kültürel içerikli bilgileri beğenirim." (Katılımcı 65)

"Haberler, Siyaset, Ekonomi, İş içerikli bilgileri beğeniyorum." (Katılımcı 50)

"Topluma faydalı olan siyasi kararları, hükümet programlarını, hibeleri ve önemli etkinlikleri paylaşıyor ve beğeniyorum. Ayrıca spor, sağlık, bilim ve eğitim hakkındaki yazılara da "Beğen"i tıklıyorum." (Katılımcı 60)

Katılımcılar sosyal medya hesaplarında birbirinden farklı tür içeriklerle kullanmaktadır. Katılımcılardan 9'u ülke ve toplum için faydalı olan içerikleri beğendiğini ve paylaştıklarını ifade etmiştir.

"Topluma gerçekten yararlı olduğunu, zararlı olmadığını ve başkalarının da görmesi gerektiğini düşündüğüm içerikleri beğenip, paylaşıyorum." (Katılımcı 55)

"Çoğu zaman eğitim, kuşakların yetiştirilme tarzı ve milliyet konularını paylaşırım. Kazakça yazılmış faydalı bilgilere çok "Beğen"i tıklıyorum." (Katılımcı 29)

"Genel olarak toplum/ülke için faydalı, anlamlı eğitim, bilim, kültür ve bazen toplumdaki güncel konuları bazen paylaşıyorum." (Katılımcı 45)

"Yararlı bilgileri paylaşmak, beğenmek ve onları indirmek..." (Katılımcı 7)

"Ülkemiz için faydalı olan bilgileri, ilgimi çeken şeyleri ve saygı duyduğum kişilerin kişisel paylaşımlarını beğenirim, ama bunları paylaşmam." (Katılımcı 44)

Katılımcılardan 7'si sosyal medyayı takip etmediğini ve içerikleri beğenmeyip paylaşım yapmadıklarını ifade etmiştir.

"Sosyal medyayı pek çok takip etmiyorum." (Katılımcı 6)

"Daha fazla insanın bilmesi gerektiğini düşündüğüm içerikler benim için çok önemlidir. Bu, farklı durumlara ve güncel meselelere göre değişmektedir. Her zaman yalnızca belirli bir türdeki içeriği beğendiğimi veya paylaştığımı söyleyemem." (Katılımcı 61)

"Sosyal medyada herhangi bir bilgiyi paylaşmamaya çalışıyorum." (Katılımcı 31)

"Beğen" ve "Paylaş"ı basmam da, paylaşmam." (Katılımcı 14)

"Sosyal medya hesaplarımda hiçbir şeye tıklamıyorum, paylaşım da yapmıyorum." (Katılımcı 39)

"İçeriklere pek "Beğen" butonunu basmam." (Katılımcı 48)

"İnternet ortamında paylaşım yapmıyorum." (Katılımcı 25)

Katılımcılardan 7'si manevi ve psikoloji konularında içerikleri beğendiğini ve paylaştığını belirtmiştir.

"İslam hakkında faydalı içerikleri beğeniyorum." (Katılımcı 24)

"Manevi ve eğitim ile ilgili içerikleri beğeniyor ve paylaşıyorum." (Katılımcı 5)

"Sosyal medyada psikoloji, ebeveynlik, yemek tarifleri ve yaşam tüyoları hakkında içerikleri beğenirim." (Katılımcı 26)

"Genel olarak manevi konularda ve sanat alanındaki içerikleri beğeniyorum." (Katılımcı 19)

"Maneviyat ile ilgili içerikleri paylaşıyorum. Ayrıca kitap, sinema, tiyatro, edep vb. içerikleri de paylaşmayı severim." (Katılımcı 23)

"Paylaş" tuşunu çok tıklıyorum. Farklı içerikli bilgileri: psikoloji ağırlık içerikleri tercih ederim." (Katılımcı 51)

Katılımcılardan birçoğu sosyal medyada eğlenceli içeriklere "Beğen" ve/veya "Paylaş" bastığını söylemiştir.

"Mizah videoları, haberler, yaban hayatı, doğa ile ilgili içerikleri beğeniyorum." (Katılımcı 53)

"Yaşamım ve toplumum için faydalı olan içerikleri, mesleğimle ilgili önemli bilgilere ve bazen de eğlenceli olan komik içeriklere "Beğen" ve "Paylaş" yapıyorum." (Katılımcı 1)

"Genelde komik içerikleri beğeniyorum." (Katılımcı 59)

"Toplumun dikkatini çekmek ve yardım etmek için yapılan eğlenceli içerikleri paylaşıyorum." (Katılımcı 38)

"Sosyal medyada eğlenceli içerikleri beğeniyor ve paylaşıyorum." (Katılımcı 20)

Sosyal medya hesaplarında kendi mesleği, kişisel ve aile hayatı ile ilgili içerikler paylaştığını da düşünenler de var:

"Kişisel ve aile hayatımda, toplumsal veya uluslararası konulardaki görüşlerimin mutlu anlarını sıklıkla paylaşırım." (Katılımcı 68)

"Genellikle sosyal medyada çok fazla sevdiğim edebi tür içeriklerini paylaşıyorum." (Katılımcı 15)

"Sosyal medyada Like basmayı pek sevmiyorum. Herkesin bildiği haberlere Like'i tıklamıyorum. Çünkü herkes onu biliyor ve Instagram algoritmasının bunları bana tekrar tekrar göstermesini istemiyorum. Sadece bakış açıma uyan paylaşımları beğeniyorum. Örneğin, Kazakistan'ın birliği, ulusal kimliği ve IT alanındaki haberleri ve trendlere Like basarak, destekliyorum. Çünkü beğeniler aracılığıyla fikrimi ifade etmek istiyorum, bu da algoritmaya göre sayfamda görüneceği ve tıkladığım beğenilerin arkadaşlarım tarafından görülebileceği anlamına gelmektedir. Bakış açımı ve fikrimi bu şekilde ifade ediyorum.

"Paylaş" konusuna gelince, ben pek paylaşım yapmam. Know-how haberleri paylaşıyorum, çünkü sosyal medyadaki arkadaşlarımın bunları görmesi gerekiyor." (Katılımcı 9)

"Sosyal medyayı aktif olarak kullanan biri değilim. Ancak gelişmelerden ve gündemlerden haberdar olmak için farklı sosyal hesapları takip ediyorum. Ben genellikle yakınlarımın ve tanıdıklarımın mutluluk ve başarı anlarına "Beğen"i tıklıyorum." (Katılımcı 35)

"Seyahat, iş, aile ve faydalı bilgiler içeren içeriklere "Beğen"i tıklıyorum." (Katılımcı 57)

"Paylaştığım içerikler gazetecilik ile ilgili makaleler ve Telegram'daki bilgi linklerdir. Çok farklı içeriklere "Paylaş" yapıyorum." (Katılımcı 13)

"Yaptığım faaliyetler, işimle ve gezdiğim yerlerle ilgili paylaşımlar yaparım..." (Katılımcı 58)

"Sosyal medyada olumlu ve iyi haberleri beğenir, paylaşırım." (Katılımcı 30)

Bununla beraber, genel olarak katılımcılardan 16'sı sosyal medyada hem "Beğen" hem "Paylaş" butonunu bastığını ifade etmiştir.

"Genellikle kendimle ilgili bilgileri paylaşıyorum ve ürün satıyorum. Çeşitli içeriklerdeki "Beğen" ve "Paylaş" düğmelerine tıklıyorum." (Katılımcı 33)

"Instagram videoları beğeniyor ve paylaşıyorum." (Katılımcı 16)

"Beğen" ve "Paylaş" butonlarını tıklıyorum." (Katılımcı 62)

"İlginç bilgileri ve güzel fotoğrafları beğenip, paylaşıyorum." (Katılımcı 2)

"Sosyal medyada hem "Beğen" hem "Paylaş"ı da tıklıyorum." (Katılımcı 64)

"Genelde "Beğen" ve "Paylaş"ı çok nadiren kullanıyorum." (Katılımcı 34)

3.3.4. Katılımcılardan Mahremiyet Algıları

Tüm katılımcılara öncelikle "mahremiyet" kavramının kendileri için ne anlam taşıdığı, hem gündelik yaşamlarında hem de dijital ortamda bu kavramı nasıl tanımladıkları sorulmuştur. Katılımcılar, bu soruları yanıtlarken müdahale edilmeden, kendi ifadeleriyle mahremiyeti nasıl gördüklerini anlatmışlardır. Böylelikle katılımcıların mahremiyet anlayışları net bir şekilde ortaya konmuştur.

Beş katılımcı, *"Size göre, "mahremiyet" ve "sosyal medyada mahremiyet" kavramı neyi ifade ediyor?"* sorusunu yanıtsız bırakmıştır. 43 katılımcı ise mahremiyet

kavramını bireysel, özel ve kişisel bilgiler şeklinde tanımlayarak, bu bilgilerin başkaları tarafından bilinmemesi gerektiğini vurgulamıştır. Katılımcıların büyük bir bölümü, kişisel kimlik bilgileri ve açık adresin en mahrem veriler olduğunu ifade etmiştir. Bunun dışında kişisel fotoğraflar, telefon numarası, konum bilgileri, kişisel mesajlar, ziyaret edilen web siteleri gibi unsurlar da katılımcılar tarafından kişisel ve mahrem bilgiler olarak değerlendirilmiştir.

"Kamuya açıklanmayan her şey mahrem bilgilerdir." (Katılımcı 6)

"Mahremiyet kavramı benim için, sosyal ağlarda kişisel verilerin başkaları için kullanılmamasıdır" (Katılımcı 1)

"Mahremiyet, güvenlik kavramına eşdeğerdir." (Katılımcı 43)

"Mahremiyet, herhangi bir bilgi veya olayın yalnızca sınırlı sayıda kişi tarafından bilinmesi ve korunması anlamına gelmektedir. Sosyal medyada mahremiyet, bir kişinin kimliği, coğrafi konumu, mesajları, sağlığı ve kişisel pozisyonuna ilişkin bilgilerin güvenliği, korunması ve ifşa edilmemesi anlamına gelmektedir." (Katılımcı 60)

"Mahremiyet kavramı benim için, kişisel verilerimi kimseye ifşa etmemek demektir." (Katılımcı 4)

"Mahremiyet, kişisel bilgilerin başkasına verilmemesi." (Katılımcı 46)

"Mahremiyet olarak bilgileri iznim olmadan kullanmak demektir" (Katılımcı 3)

"Kişisel bilgilerim güvenli bir şekilde korunması ve yetkisiz amaçlar için kullanılmaması veya dağıtılmamasıdır." (Katılımcı 47)

"Mahremiyet, kişisel bilgiler anlamına gelir" (Katılımcı 2)

"Kişinin kişisel bilgilerinin ve yaşamına ilişkin verilerinin saklanması ve korunmasını amaçlar. Mahremiyet, bireyin seçim yapma hakkını güvence altına alır ve yabancıların mahremiyetine müdahalesini sınırlar. Kişisel bilgileri ifşa etmemek, hayatını başkalarından gizli tutmak anlamına gelmektedir." (Katılımcı 39)

"Mahremiyet, kişisel etiği temsil eder." (Katılımcı 62)

"Mahremiyet, kullanıcının başkalarına aktarmak istemediği herhangi bir bilginin güvenliği." (Katılımcı 8)

"Mahremiyet, kişisel verilerin güvenilir şekilde korunması." (Katılımcı 30)

"Kişisel bilgilerin gizliliği..." (Katılımcı 22)

"Kişisel verilerin üçüncü şahıslarla paylaşılmasının önlenmesi." (Katılımcı 31)

"Kişisel verilerin anonimleştirilmesi." (Katılımcı 63)

"Kişisel bilgilerimin tamamen güvenli bir şekilde saklanması ve başka zararlı amaçlar için kullanılmamasıdır." (Katılımcı 32)

"Bana göre mahremiyet, Face ID demektir." (Katılımcı 16)

"Mahremiyet kavramı benim için, kişisel sınırdır." (Katılımcı 64)

Genel katılımcılardan 7'si mahremiyetin ve sosyal medya mahremiyetinin birey için önemli olduğunu ve korunması gerektiğini dile getirmiştir.

"Her ikisi de birey için önemlidir. Herkesin kendine göre bir sırrı olmalı. Başkalarının benim hakkımda çok fazla şey bilmesinden hoşlanmıyorum." (Katılımcı 11)

"Mahremiyete ihtiyacımız var. Zorunlu!" (Katılımcı 21)

"Kişisel verilerimin korunması gerektiğine inanıyorum." (Katılımcı 13)

"Kişinin kendi kişisel sınırları olmalı, mahremiyeti korunmalıdır! Çok fazla ayrıntı açıklanmamalı." (Katılımcı 7)

"Mahremiyet, hakkınızdaki kişisel bilgilerin bir kanun kaçağının eline geçemeyeceği koşuludur." (Katılımcı 24)

"Bana göre mahremiyet, başkalarıyla kişisel ilişkiler, yazışmalar, kişisel anlaşmalar ve sözleşmelerdir." (Katılımcı 29)

"Kişisel verilerimin tamamen güvenli bir şekilde saklanması ve diğer zararlı amaçlar için kullanılmaması." (Katılımcı 32)

Diğer 3 katılımcı ise mahremiyet kavramını sadece ailelerine dair bilgileri gizli tutmak olarak değerlendirmektedir.

"Bana göre, insanın özel hayatındaki korumak istediği aile ve özel hayatı, insanlar ile ilişkisi, yaşadığı alan, kişisel bilgileri, sağlık durumu hatta beslendiği sofralar da bir "mahremiyet"tir. Ancak insanlarda doğal olarak "merak" etmek, bir sırrı öğrenmek isteği olduğundan, dijital platformlarda bile bu ilgilerini sürdürüyorlar. Sosyal medyada fenomen kullanıcıların mahremiyet kavramının sınırlarını açtığı için takipçiler tarafından cazip geldiğini düşünüyorum." (Katılımcı 35)

"Bana göre mahremiyet, aileniz ve kişisel bilgilerinizle ilgili ayrıntılardır. Örneğin, kredi geçmişi, banka kartları, kimlik ve pasaportlar vb." (Katılımcı 67)

Bazı katılımcılar ise, mahremiyet algılarını gündelik yaşam ve sosyal medya bağlamında birlikte ele almakta, sosyal medyaya olumlu yaklaşanların da olduğu gözlemlenmektedir.

"Sosyal ağlar gizli bilgilerimizi ve kodlarımızı mümkün olduğunca korumaya çalışmaktadır." (Katılımcı 44)

"Bana göre sosyal medya mahremiyeti, bunlar doğrudan doğruya vatandaşların kişisel güvenliğine zemin hazırlayan kavramlardır. Kişisel görüşlerinizi yazmak, kişisel haberlerinizi ve fotoğraflarınızı yayınlamak belli bir düzeyde risk taşımaktadır. Ama bu hayatımızın ayrılmaz bir parçası haline gelmektedir." (Katılımcı 34)

"Sosyal medya mahremiyeti, halka açık bir hesabınız olmadığında takipçi (arkadaş) olarak kabul ettiğiniz kişiler sayfanızı görebildiğinde, başka hiç kimse göremez..." (Katılımcı 57)

Bununla birlikte, 6 katılımcı, mahremiyetin sanal dünyada, günlük yaşamdan farklı bir anlam taşıdığını belirtmiştir. Bu kişiler, sosyal medyada mahremiyetin tamamen ortadan kalktığını, her şeyin artık kamuya açık hale geldiğini ve bunun da günlük hayatı etkilediğini dile getirmişlerdir. Sosyal medyanın güvenilir bir ortam olmadığını düşündüklerinden, her bilginin paylaşılmaması gerektiğini savunan ifadeler de mevcuttur.

"Sosyal medya mahremiyeti, çevrimiçi dünyada kişisel bilgilerin ve içeriklerin nasıl korunacağı, paylaşım sınırlarının nasıl çizileceği ve kullanıcıların mahremiyet haklarının ihlal edilmemesi için alınması gereken önlemlerdir." (Katılımcı 58)

"Bazı durumlarda "Sosyal ağlar" ve "mahremiyet" kavramlarının birbiriyle çeliştiğine inanıyorum. Sosyal medyada aktif kalabilmek için "mahremiyet" düzenini sağlamak zor görünüyor." (Katılımcı 40)

"Sosyal medyada kişisel verilerim bazen olumlu ve olumsuz bir yönde bana karşı kullanıldığını farkettim." (Katılımcı 65)

"Kişisel veriler gizli tutulmalı ve başka kişilerin ve sosyal ağların yararına (dolandırıcılık faaliyetleri, reklamcılık vb.) kullanılmamalıdır." (Katılımcı 61)

"Sosyal medyada sır yoktur." (Katılımcı 49)

"Benim için mahremiyet kavramı hiçbir şey, artık gizlilik ortadan kalkmaktadır." (Katılımcı 66)

Ayrıca, hem sosyal medyada hem de günlük hayatta mahremiyetin korunmasına ve kişisel verilerin izinsiz kullanılmamasına vurgu yapan 9 katılımcı, bu düşüncelerini mahremiyet kavramı kapsamında dile getirmiştir.

"Mahremiyet kavramı, kamusal alanda ifşa etmek istemediğim kimliğimle ilgili herhangi bir bilgi. Sosyal medyada mahremiyet ise, gizlilik ve kimliğimle ilgili ifşa edilmeyen veya yayınlanmasına izin verilmeyen herhangi bir bilgi/veridir (video, fotoğraf, bilgi, konum)." (Katılımcı 37)

"Kişisel, aile, mali ve diğer yasal olarak korunan verilerin bireyin izni olmadan üçüncü bir tarafa ve/veya sosyal medyada yayılmasının önlenmesidir..." (Katılımcı 68)

"Kişisel verileri yalnızca şirket kullanabilir, üçüncü şahıslarla paylaşamaz." (Katılımcı 33)

"Mahremiyet, sosyal medyada kişisel verilerin ifşa edilmemesi." (Katılımcı 56)

"Benim için "mahremiyet" kavramı, bir kişinin özel hayatına, kişisel verilerine, düşüncelerine, duygularına ve eylemlerine müdahale etmeme hakkı anlamına geliyor. "Sosyal medya mahremiyeti" ise, hakkınızdaki bilgileri kimlerin görebileceğini kontrol etmekle ilgilidir." (Katılımcı 50)

"Bilgi ve verilere ancak bu bilgilerin sahibinin bildirimi ve izni ile erişilebilmektedir." (Katılımcı 38)

"Kullanıcının izni olmadan kişisel bilgilerin ifşa edilmemesi." (Katılımcı 53)

"Bir kişinin verilerini kendi takdirine bağlı olarak kullanma yeteneği, bir kişinin kişisel verilerinin paylaşılmayacağının garantisi, hiçbir şirketin kişisel verilerini kendi çıkarları doğrultusunda ifşa etmeyeceği." (Katılımcı 55)

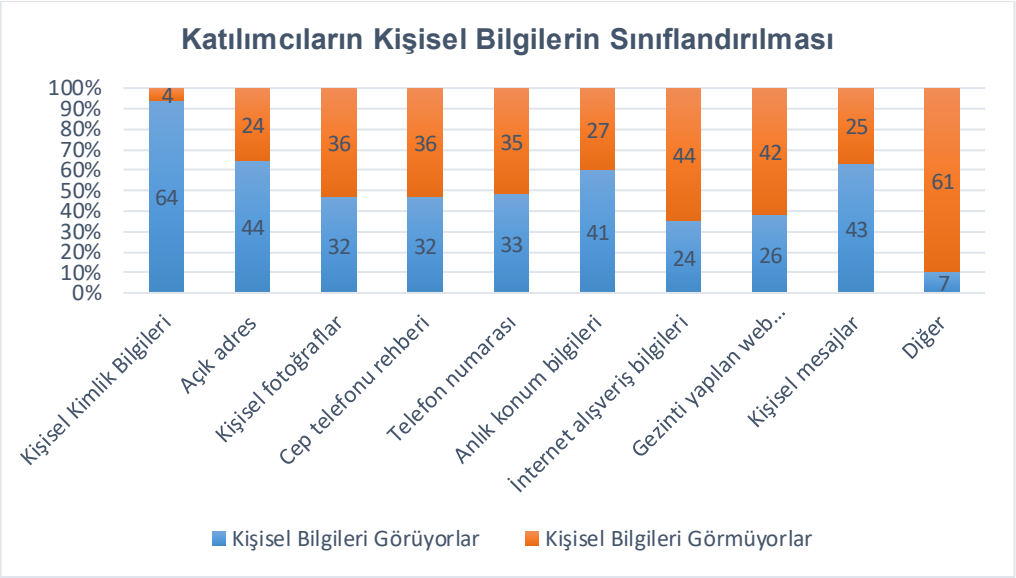
"Kişisel bilgilerim başkaları tarafından çeşitli amaçlarla kullanılmamalıdır." (Katılımcı 51)

Genel olarak elde edilen yanıtlar, tüm katılımcıların mahremiyet konusunda farklı bakış açılarına sahip olduklarını, ancak mahremiyet algısının ortak bir temada birleştiğini göstermektedir.

3.3.5. Katılımcıların Kişisel Veri Sınıflamaları

Katılımcılara, görüşmeler sırasında kişisel veri örnekleri içeren 10 farklı içerik sunulmuş ve *"Hangisini/hangilerini kişisel veri olarak görüyorsunuz?"* sorusu yöneltilmiştir. Katılımcıların bu soruya verdikleri yanıtlar Ek 3'te detaylı şekilde yer almaktadır.

Ayrıca, hangi verilerin kişisel olarak değerlendirildiği ve hangilerinin değerlendirilmediği de Şekil 15'te görselleştirilmiştir.



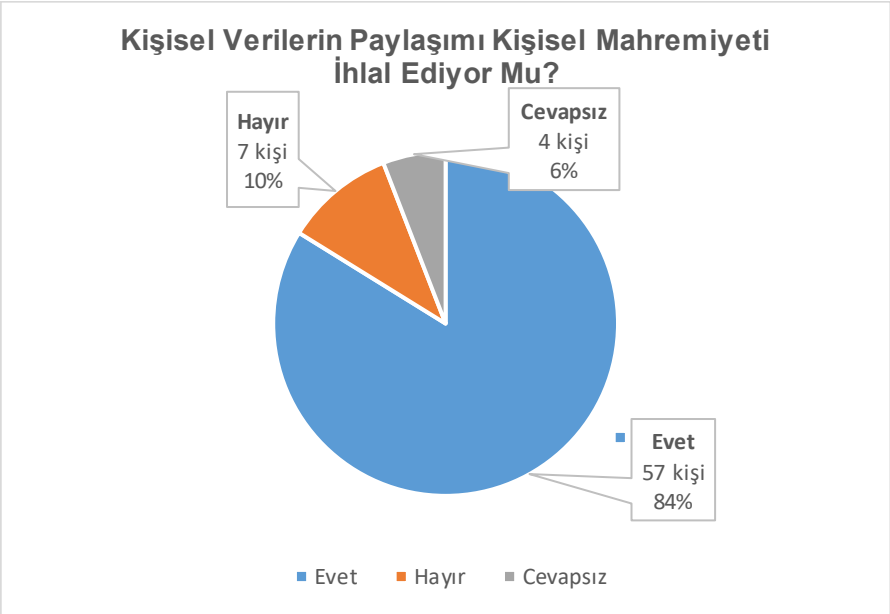
Şekil 15. *Katılımcıların Cevaplarına Göre Kişisel Verilerin Değerlendirilmesi*

Yanıtlar incelendiğinde, katılımcıların hangi bilgileri kişisel veri olarak gördüklerinin farklılık gösterdiği anlaşılmaktadır. Örneğin, "Kişisel kimlik bilgileri" 64 katılımcı tarafından kişisel veri olarak görülürken, 4 katılımcı tarafından kişisel veri

olarak değerlendirilmemiştir. "Açık adres" verisini 44 katılımcı kişisel veri olarak belirtmiş, 24 katılımcı ise, bu veriyi kişisel veri olarak kabul etmemiştir. "Kişisel fotoğraflar" ve "Cep telefonu rehberi" verilerinde ise, 32 katılımcı bunları kişisel veri olarak ifade ederken, 36 katılımcı kişisel veri olarak değerlendirmemektedir. "Telefon numarası" ile ilgili olarak 33 katılımcı kişisel veri olduğunu, 35 katılımcı ise olmadığını dile getirmiştir. "Anlık konum bilgileri" için 27 katılımcı kişisel veri olmadığını, 41 katılımcı ise kişisel veri olduğunu belirtmiştir. "İnternet alışveriş bilgileri" verisini ise, yalnızca 24 katılımcı kişisel veri olarak nitelendirirken, 44 katılımcı bunu kişisel veri olarak görmemektedir. "Web siteleri gezinti geçmişi" konusunda ise 42 katılımcı kişisel veri olarak görmediğini, 26 katılımcı ise kişisel veri olarak gördüğünü ifade etmiştir. "Kişisel mesajlar" 43 katılımcı tarafından kişisel veri olarak tanımlanmış; buna karşılık 25 katılımcı bu veriyi kişisel veri olarak kabul etmemiştir. Ayrıca, "Diğer" yanıtını veren 61 katılımcı, bu verileri kişisel veri olarak görmediklerini; yalnızca 7 katılımcı ise kişisel veri olarak değerlendirdiklerini dile getirmiştir.

3.3.6. Katılımcıların Kişisel Verilerinin Paylaşımı ve Kişisel Mahremiyet

Araştırmada, 68 katılımcıdan 57'si kişisel verilerin paylaşımı kişisel mahremiyeti ihlal ettiğini düşündüğünü ifade ederken, yalnızca 7 katılımcı kişisel verilerin paylaşımı kişisel mahremiyeti ihlal etmediğini düşündüğünü belirtmiştir. 4 katılımcı ise, yanıt vermemiştir.



Şekil 16. *Katılımcıların Kişisel Verilerinin Paylaşımında Kişisel Mahremiyeti İhlal Edip Etmediğine Dair Görüşleri*

Şekil 16'da katılımcıların kişisel verilerinin paylaşımında kişisel mahremiyeti ihlal edip etmediğine dair görüşleri yer almaktadır. Katılımcıların 7 kişisel verilerin paylaşımı kişisel mahremiyeti ihlal etmediğini düşünürken, 57 katılımcı kişisel verilerin paylaşımı kişisel mahremiyeti ihlal ettiğini ifade etmektedir. Bu bağlamda, katılımcılara *"Size göre kişisel verilerin paylaşımı kişisel mahremiyeti ihlal ediyor mu, ediyorsa niçin?"* sorusu sorulmuştur. Katılımcıların çoğu ihlal ettiğine dair cevapları şöyle ifade etmiştir.

> *"Kişisel veriler kesinlikle mahremiyeti ihlal eder. Şahsen kişisel verileri hiç yayınlamamaya çalışıyorum."* (Katılımcı 11)

> *"Kişisel verilerin paylaşımı, kişisel mahremiyeti ihlal edebilir, ancak bu durum paylaşılan verilerin türüne, paylaşımın nasıl yapıldığına ve bu verilerin kimlerle paylaşıldığına bağlıdır. Eğer kişisel veriler, ilgili kişinin izni olmadan paylaşılıyorsa, bu kişisel gizliliğin ihlali anlamına gelir. Özellikle, özel bilgiler veya hassas veriler izinsiz paylaşıldığında, bu durum mahremiyetin ihlali anlamına gelebilir."* (Katılımcı 58)

> *"Elbette ihlal ediyor. Örneğin, mali durumum veya sağlığım vb. ilgili bilgilerin olası yayınlanması."* (Katılımcı 63)

> *"Evet, bu bir ihlaldir, kişisel bilgilerinizi paylaşmak için o kişiden izin almanız gerekir. Kimin neyi, nerede paylaştığı belli olmadığından kesin bir cevap vermek zor. Elbette, birinin kişisel bilgilerinin kamuoyuna açıklanması, en azından medya etiğine uygun olarak kabul edilemez."* (Katılımcı 60)

> *"Elbette. Bu bireyin özgürlüğü ve hürriyeti için tehlikeli olabilir."* (Katılımcı 62)

> *"Evet, eğer kişisel sınıra zorla girilirse ve taciz veya aşağılanma durumları varsa, ihlal edildiğini düşünüyorum."* (Katılımcı 5)

Katılımcılardan bazıları ise, kişisel verilerin paylaşılması günümüzde yaygın bir dolandırıcılığa da yol açtığını dile getirmiştir.

> *"Evet, sosyal ağları kullanan ve iyi niyetli olmayan çok sayıda insanın olduğu göz önüne alındığında, bu durum kişisel mahremiyeti ihlal ettiği anlamına gelmektedir."* (Katılımcı 8)

> *"Dolandırıcılığın arttığı bir çağda, her şeye karşı giderek daha güvensiz hale geliyoruz."* (Katılımcı 23)

"Evet, ihlal ediyor. Bireyin kişisel verilerinin, hükümet kuruluşları hariç olmak üzere, yalnızca kendisinin bilmesi gereken bilgiler olduğuna inanıyorum, bu nedenle bu verilerin paylaşılması günümüzde yaygın bir dolandırıcılığa yol açıyor." (Katılımcı 1)

"Dolandırıcılığı önlemek için kimlik ve banka kartı bilgileri gizli tutmak lazım." (Katılımcı 22)

"Evet, bu başkalarına "ulaşılabilir olmak" demektir." (Katılımcı 21)

"Evet, banka hesap numaralarına göre finansal dolandırıcılarla karşılaşabilir." (Katılımcı 19)

"Günümüzde kişisel mahremiyet dolandırıcılar tarafından ihlal ediliyor maalesef" (Katılımcı 66)

"İnternet dolandırıcıları kişisel bilgileri kendi yararına kullanıyor." (Katılımcı 65)

"Evet. Tanımadığım kişilerin kişisel bilgilere kolayca erişebilmelerine karşıyım." (Katılımcı 26)

"Elbette. Eğer yetkisiz bir şekilde birinin eline geçerse o zaman ihlal edilir." (Katılımcı 30)

Katılımcılardan 5'i ise, bu konuyu Kimlik kartı bilgilerinin paylaşılması kişisel mahremiyetin ihlal edildiğini belirtmişlerdir.

"Kişisel verilerin paylaşılması mahremiyetin ihlalidir." (Katılımcı 16)

"Kimlik kartı, JSN numaralarının (Türkiye'deki TC Kimlik No. gibi) paylaşılması gizliliğin ihlalidir." (Katılımcı 54)

"Tabii ki. Kimlik bilgilerimin sosyal medyada dağıtılması veya sosyal ağlarda özel mesajlarımın paylaşılması haklarımı ihlal ediyor." (Katılımcı 15)

"Sorun şu ki, örneğin bir kişinin kimliğine ilişkin bilgiler, ki bunlara sıklıkla kişisel bilgi denir ve hangi verilerin ne zaman işlendiğini belirlemek zor değildir. Sorun, başkalarıyla yapılan anlaşmaların ve kişisel yazışmaların, örneğin mesajlaşma programlarındaki diyalogların gizliliğinin sağlanmasıdır." (Katılımcı 29)

"Birinin kişisel verilerimi başka birisine verme hakkı yoktur." (Katılımcı 13)

Katılımcılardan birisi kişisel verilerin paylaşımı kişisel mahremiyeti ihlal edip etmediğine dair görüşünü şöyle açıklamıştır:

> *"Bu, özel bir duruma bağlıdır. Kendi aile bireylerimle bilgi paylaşımının yanı sıra, bazen özel bir talep kapsamında avukatımla, noterimle, kamu kurumu temsilcileriyle, akrabalarımla ve bireysel arkadaşlarımla kişisel verilerimi paylaştığım durumlar da oluyor. Ben yalnızca karşılıklı güvenin sağlandığı ve kişisel bilgilerin yalnızca hukuka uygun olarak kullanıldığı durumlarda izin veriyorum. Dolayısıyla buradaki durumun kişisel mahremiyeti ihlal ettiğine inanmıyorum. Ve eğer bu kişiler benim kişisel verilerimi benim iznim olmadan ve bana karşı amaçlarla kullanırlarsa ve bunları üçüncü bir tarafa veya sosyal ağlara yayınlarsa, bunu hukuka aykırı bir eylem olarak kabul ediyorum ve bunun sorumluluğunu üstleneceğim. Böyle bir durumla karşılaşırsam polise veya mahkemeye başvurmam gerektiğini düşünüyorum."* (Katılımcı 68)

Diğer taraftan, katılımcılardan birisi kişisel verileri iki kategori altında değerlendirerek şöyle ifade etmiştir.

> *"Öncelikle kişisel verileri iki kategori altında değerlendirmek istiyorum. Bunlardan biri, bizim kendi rızamız dahilinde açık sunduğumuz bilgiler olup gizlilik ihlali sayılmayan kategoridir. Örnek olarak, eğer bu bilgi bir açık adres (iş yeri ve ikamet adresi) ise gizliliğin ihlali olarak görmüyorum. Çünkü artık binlerce kilometre uzaklıktan size gelen bir kargo paketi üzerinde ve farklı kişilerin bilgisi dahilinde olacak bir bilgidir. Bir cep numaranız da buna dahildir. İkinci kategoride ise, bizim rızamız olmaksızın paylaşılan bilgiler. Bu bir kişisel fotoğraf, sağlık durumu raporları, banka hesabı gibi bilgiler olabilir. Dolayısıyla, bana göre birinci kategorideki durumlar gizlilik ihlali olmuyor ikincisi ise gizlilik ihlalidir."* (Katılımcı 35)

Katılımcıların cevaplarında genel olarak kişisel veriler ilgili kişinin izni/rızası olmadan paylaşılıyorsa, bu kişisel gizliliğin ihlali anlamına geldiğini, internet dolandırıcılarının kişisel bilgileri kendi yararına kullandığını ve Kimlik kartı ve Sağlık bilgilerinin paylaşılmaması gerektiği görülmektedir. Buradan hareketle Kazakistan yükseköğretim mezun ve öğrencilerini temsil eden araştırma örneklemimdeki katılımcıların kişisel verilerin paylaşımı kişisel mahremiyeti ihlal ettiğinden haberdar oldukları söylenebilir. Katılımcıların bazıları kimlik (JSN) ve banka kartı bilgilerini gizli

tuttuğunu ve kişisel verileri hiç yayınlamamaya çalıştığını düşünmekteyken, bazıları da kendi rızasıyla kişisel verilerini paylaşmasının kendi tercihi olduğuna inandıklarını sanmaktadırlar.

Bazıları ise, kendi rızasıyla kişisel verilerin paylaşılmasının kendi tercihi olduğunu ve kimilerine göre bunun için çok fazla ihlal etmediklerini yalnızca günümüzde artık bunu normal olarak karşıladığını öne sürenler de vardır.

"Herkesin kendi rızasıyla kişisel verilerini paylaşmasının kendi tercihi olduğuna inanıyorum." (Katılımcı 40)

"Eğer kendiniz bilgileri paylaşıyorsanız, bunu bilerek ve rızanızla veriyorsunuz demektir." (Katılımcı 42)

"Hayır, ihlal etmiyor. Günümüzde artık bu normal kabul ediliyor." (Katılımcı 44)

"Çok fazla ihlal edeceğini düşünmüyorum." (Katılımcı 18)

"Hayır, kişisel verilerin paylaşımı kişisel mahremiyeti ihlal etmiyor ." (Katılımcı 2)

"Evet, kişisel verilerim yalnızca benim iznimle yayınlanabilir/paylaşılabilir. Ancak benim iznim/onayım olmadan kullanılması ve benim bundan habersiz olmam, kişisel mahremiyetimin ihlal edildiği anlamına gelir." (Katılımcı 37)

"Değişimin kendisi bir ihlal değildir; bireyin rızası olmadan yapılan alışveriş bir ihlaldir." (Katılımcı 38)

"Paylaşılan bilgi iki kişi arasında kalırsa ve onların bilgisi dışında açıklanmazsa gizliliğin ihlal edilmediğine inanıyorum." (Katılımcı 53)

Kişisel bilgiler üçüncü şahıslar tarafından izinsiz paylaşmaması gerektiğini ve kişisel veriler yasalarca korunması gerektiğini düşünenler de vardır.

"Elbette bu yasa normlara tabidir. Üçüncü bir tarafın kişisel verileri paylaşma hakkı, rıza/izin yoluyla kanunun normları aracılığıyla kullanılır. İhlal edilirse, idari ve ceza normlarına uygun olarak mahkemeye sunulur." (Katılımcı 45)

"Yetkili makamların talebi üzerine talepte bulunulması halinde kişisel mahremiyet ihlal edilmeyecektir. Ve üçüncü tarafların kişisel bilgilere erişiminin bir suç olduğuna inanıyorum." (Katılımcı 31)

"Evet, paylaşmadığım, paylaşmak istemediğim bilgileri paylaşmanın mahremiyetimin ihlali olduğuna ve yasalarca korunması gerektiğine inanıyorum." (Katılımcı 50)

"Sanki belli bir seviyede ihlal ediyor gibi. Çünkü bu, herkesin çevrimiçi olduğu ve verilerimizin onlar için erişilebilir olduğu anlamına gelir. Bana öyle geliyor ki, bu bakımdan herkes için ortak bir koruma olacak bir yasa çıkarmak zor." (Katılımcı 34)

"Evet. Üçüncü bir şahıs ihlal ederse, hakkında dava açılacaktır." (Katılımcı 49)

"Verilerim iznim veya bildirimim olmadan satılırsa, dağıtılırsa veya kamuya açıklanırsa bu bir mahremiyet ihlalidir." (Katılımcı 47)

"Üçüncü şahısların kendi amaçları doğrultusunda kullanımı ve dağıtımı ihlaldir." (Katılımcı 43)

"Ancak bu bilgiler daha sonra üçüncü şahıslarla paylaşılırsa ihlal edildiğini düşünüyorum." (Katılımcı 20)

"Şüphesiz öyle görünüyor, çünkü hiçbir yabancı sizin bilginiz olmadan bunları değiştiremez." (Katılımcı 57)

"Eğer bir başkası benim kişisel verilerimi iznim olmadan, benim adıma kullanıyorsa, evet bu bir ihlaldir. Çünkü, bu sadece bana ait bir bilgidir, kişisel bilgiler paylaşılamaz." (Katılımcı 51)

Mahremiyetin ortadan kalkmasına teknolojinin ilerlemesi ve mobil uygulamaların katkıda bulunduğunu düşünenler de mevcuttur.

"... evet, çünkü her internet devinin bize karşı tutumunun, ürünlerini en son modern teknolojiyi kullanarak sunmak için çeşitli hilelere ve manipülasyonlara yol açtığını düşünüyorum." (Katılımcı 55)

"Tabii ki kişisel veri, bireylere ait kişisel bilgilerdir. Kişisel veriler paylaşılmamalıdır. Çünkü bir kişinin kişisel, hayati ve finansal verileri oldukça önemli bilgiler olarak değerlendirilmektedir. Örneğin, Kazakistan'da bu tür verilerin tümü (kişisel ve aile bilgileri, finans, ev belgeleri vb.) Kaspi.kz mobil uygulamasında mevcuttur. Elbette ki, teknolojinin bugünkü durumu göz önüne alındığında Kaspi.kz iyi bir şeydir. Ancak, üçüncü şahsın bu uygulamanın şifresini

veya kodunu bilmesi durumunda, kişinin kişisel verileri ve sırları ifşa edilebilir ve gizlilik ihlal edilebilir." (Katılımcı 67)

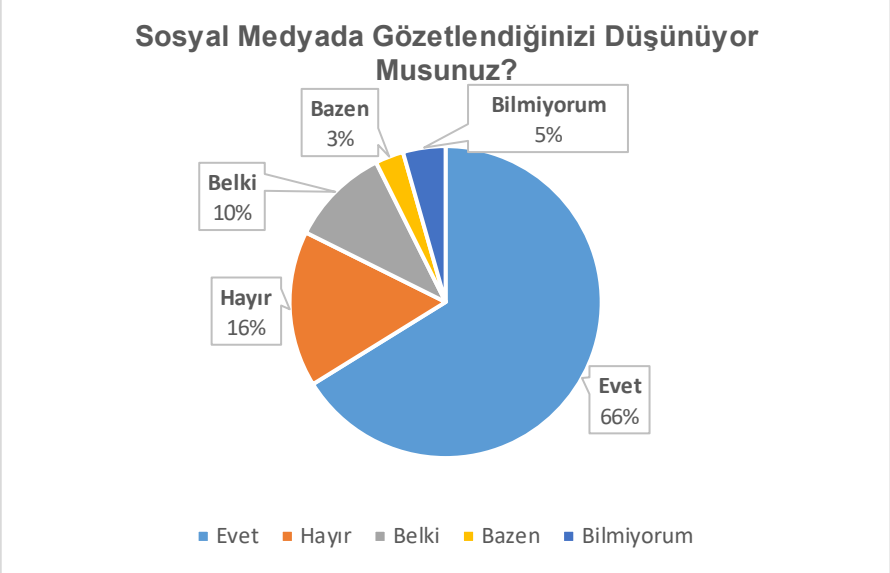
"Elbette buna izin verilmemeli. Kişisel bilgiler suçluların eline geçerse, yapay zeka veya diğer yollarla o kişiyi aldatabilir ve ona zarar verebilirler." (Katılımcı 33)

3.3.7. Mahremiyet İhlali ve Gözetim

Günümüzde günlük yaşamda fotoğraf ve videolar gibi içeriklerin çevrimiçi olarak sürekli paylaşıldığı görülmektedir. Facebook, Instagram, X (Twitter), YouTube, Flickr ve Dailymotion gibi sosyal paylaşım platformlarına her ay milyonlarca yeni fotoğraf ve video yüklenmekte ve arşivlenmektedir. Google ve YouTube'un verilerine göre, bu platformlara her dakika yaklaşık on üç saatlik video yüklenerek veri tabanlarına eklenmektedir. Böylece yaşamlarımız, daha önce olmadığı kadar herkese açık biçimde kaydedilmekte ve depolanmaktadır (Niedzviecki, 2010: s. 17).

Bununla birlikte, bu paylaşımların bir başkası tarafından izlendiği ve kontrol edildiği ise çoğu kişi tarafından tam olarak fark edilmemektedir. Bu çerçevede yapılan yarı yapılandırılmış görüşmelerde, katılımcıların sosyal medya aracılığıyla gözetlendiklerinin farkında olup olmadıkları ve sosyal medyayı bir gözetim aracı olarak görüp görmedikleri araştırılmıştır.

Araştırmada, katılımcıların sosyal medyada gözetlendiğini tespit etmek amacıyla görüşmede *"Sosyal medyada gözetlendiğinizi düşünüyor musunuz?"* sorusu sorulmuştur. Katılımcıların verdiği cevaplara göre, 45 kişi *"Evet"*, 11 kişi *"Hayır"*, 7 kişi *"Belki"*, 2 kişi *"Bazen"*, 3 kişi *"Bilmiyorum"* şeklinde sosyal medyada gözetlendiğini belirtmiştir. Aşağıdaki Şekil 17'de katılımcılar sosyal medyada gözetlenip gözetlenmediği gösterilmiştir.



Şekil 17. *Katılımcıların Cevaplarına Göre Sosyal Medyada Gözetim*

Katılımcılardan 45'i sosyal medyada gözetimin var olduğunu bildiği; paylaşılan her şeyin (kişisel verilerimiz, fotoğraflar, görüşlerimiz vb.) depolanıp gözetlendiğini ya da denetim amacıyla kullanıldığını bildiği anlaşılmaktadır. Katılımcılardan 45'i, sosyal medyada paylaşılan her şeyin (örneğin kişisel veriler, fotoğraflar, görüşler vb.) depolanıp gözetlendiğini ve denetim amacıyla kullanıldığını ifade etmiştir.

> *"Doğrudan bir gözetleme yaptıklarını sanmıyorum, ama gerektiğinde sosyal ağlardaki verileri benim aleyhime kullanabilirler."* (Katılımcı 8)

> *"Evet, gözetlendiğimi düşünüyorum. Ama her zaman değil."* (Katılımcı 1)

> *"Tabii ki gözetlendiğimi biliyorum, çünkü ben aktif bir sosyal medya kullanıcısıyım."* (Katılımcı 27)

> *"Evet. Sosyal medya izlediğiniz ve beğendiğiniz içeriklere göre size videolar önermektedir."* (Katılımcı 24)

> *"Elbette, kişiselleştirilmiş reklamcılık diye bir şey var ve siz bir şey söyledikten sonra bile bu o gün websitesinde yer alıyor, sunuyor..."* (Katılımcı 33)

> *"Tamamen gözetim altında olduğumu düşünüyorum."* (Katılımcı 29)

> *"Sosyal medyada kişisel olarak değil, toplumun bir parçası olarak bir sınıf bazında takip edildiğimi düşünüyorum. Örnek, yaş kategorisi, yaşadığım ülke bazında, eğitim düzeyim bazında vs."* (Katılımcı 35)

"Elbette. Yetkili makamların ve kişilerin denetim sahibi olması meşrudur." (Katılımcı 68)

"Sosyal medyada takipçiler takip ediyor, gözetliyor..." (Katılımcı 3)

"Evet, bu günde her şey gözetlenmektedir" (Katılımcı 18)

2 katılımcı bazen gözetlendiğini ve 3 katılımcı ise bu konu hakkında bilmediklerini dile getirmiştir. Katılımcıların 11'i ise, sosyal medyada gözetlenmediğini ve bunu sorun olarak görmediklerini düşünmektedirler.

"Eğer birinin bana ihtiyacı varsa, gözetlenirim. Ama eğer sıradan bir insansam, kimin bana ihtiyacı olur ki..?" (Katılımcı 44)

"Hayır. Hukuk çerçevesinde kişisel verilere yönelik bir ihlalin söz konusu olmadığını düşünüyorum." (Katılımcı 31)

"Büyük ihtimal, hayır." (Katılımcı 57)

"Sanmıyorum. Ama sosyal medyadaki etkinliğime göre bana reklamlar, fotoğraflar ve blog yazarları önerilmektedir. Çünkü algoritma böyle işliyor. İnternet kullanıcılarının her platformdaki etkinliği analiz edilir." (Katılımcı 60)

Genel olarak yanıtlar, katılımcıların çoğunun gözetlendiklerini bildiklerini; ancak bunun özellikle büyük şirketlerin amaçlarından biri olduğunu düşünenlerin de bulunduğunu göstermektedir.

"Evet, elbette. Dev şirketlerin hedeflerinden biri de insanları yönetmek olduğundan eminim." (Katılımcı 55)

"Evet. İster sistem olarak, ister toplum olarak bakalım, gözetlendiğimiz aşikar. Foucault'nun Panopticon kavramı buna örnek olabilir..." (Katılımcı 51)

Katılımcılardan 7'si sosyal medyada "belki gözetlendiğini" ileri sürmektedir. Cevap veren katılımcılardan birisi gözetimin sorun olmadığını, diğeri ise "net fikrim yok" şeklinde düşünmektedir.

"Belki gözetleniyorum. Bu benim için sorun değil." (Katılımcı 4)

"Sanırım bunun sebebi, bir kişinin hayatına dair çok fazla kişisel veri ve olay barındırıyor olması ve gerektiğinde gözetlenebilmesi olabilir." (Katılımcı 67)

"Belki, pazarlamacılar gözetim yapıyordur..." (Katılımcı 25)

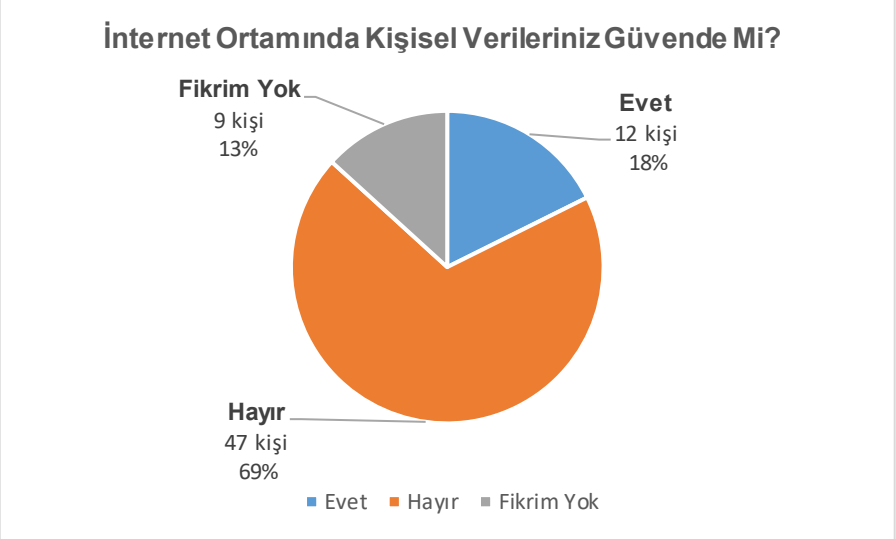
"Belki de. Benim net bir fikrim yok." (Katılımcı 34)

Endişe verici bir cevap veren katılımcılardan 1'si gözetimden dolayı sosyal medyayı bırakmak istediğini belirtmiştir.

"Evet. Ayrıca tamamen çevrimdışı olup, sosyal medyayı kullanmamayı düşünüyorum." (Katılımcı 23)

3.3.8. İnternet Ortamında Kişisel Verilerin Güvenliği

Araştırma sonuçlarına göre, 68 katılımcıdan 47'si internet ortamında kişisel verilerinin güvende olmadığını (Hayır) düşündüğünü belirtmiştir. 12 katılımcı verilerinin güvenli olduğunu (Evet) ifade ederken, 9 katılımcı ise bu konuda "Fikrim Yok" yanıtını vermiştir.



Şekil 18. *Katılımcıların İnternette Bilgilerinin Güvende Olup Olmadığına Dair Görüşleri*

Katılımcıların internetteki veri güvenliği hakkındaki görüşleri Şekil 18'de sunulmuştur. Katılımcıların 12'si verilerinin çevrimiçi ortamda güvenli olduğunu düşünürken, 47'si ise güvenlik konusunda endişeli olduklarını belirtmiştir. Bu bağlamda, katılımcılara *"İnternet ortamında kişisel verilerinizi korumak ve başkalarının erişimini engellemek için herhangi bir önlem alıyor musunuz? Eğer alıyorsanız, ne tür önlemler alıyorsunuz?"* sorusu yöneltilmiştir. Bu soruya 20'den fazla katılımcı çeşitli önlemler aldıklarını ifade etmiştir.

"Kişisel verilerimi başkalarının elektronik cihazlarında kullanmıyorum, şüpheli internet bağlantılara geçmiyorum." (Katılımcı 8)

"Öncelikle phishing sitelerine girmemek lazım, bunun için domain adresi kontrol edilmeli. Sadece bankacılık ve diğer egov.kz web sitesinde kişisel bilgiler girilmeli. Şifre ve PIN kodlar kimseyle paylaşılmamalı, Kazakistan Elektronik Dijital İmzasını (ЭЦП) düzenli olarak güncellemek lazım ve onu kimseye vermemeli." (Katılımcı 33)

"Önlem amaçlı iki adımlı doğrulamayı kullanıyorum, ardından ek bir e-posta ve numara kurtarma fonksiyonunu kullanıyorum." (Katılımcı 48)

"İnternet ortamında kişisel bilgilerimi, telefon numaramı göstermemeye çalışıyorum." (Katılımcı 38)

"Evet, ilk önce kişisel telefonuma kimsenin erişememesi için şifre ve Face ID belirledim. Aynı şey tüm kişisel ve iş e-postalarım için de geçerli, şifremi kimseyle paylaşmıyorum. Üçüncü şahıslar, kişisel sosyal medya sayfalarımda yalnızca benim iznimle içerik paylaşabilirler. Bunu yapmak için sosyal ağ ayarlarınızda ilgili komutu etkinleştirmeniz gerekiyor." (Katılımcı 68)

"İnternet ortamında kişisel 'internet hijyenimi' uyguluyorum." (Katılımcı 9)

"Evet, özellikle verilerimi kullanma izni isterlerse hemen reddediyorum. Ayrıca YouTube'u bana hiçbir video göstermeyecek ve yalnızca abone olduğum videoları gösterecek şekilde ayarladım." (Katılımcı 55)

"Sadece sosyal ağların kendileri tarafından önerilen önlemleri alıyorum." (Katılımcı 23)

"İnternet ortamında kişisel banka belgelerimi veya kimlik kartlarımı sunmuyorum." (Katılımcı 36)

"Kişisel bilgilerimi paylaşmıyorum, bütün sosyal medya hesaplarımda güçlü bir parola kullanıyorum ve iki faktörlü kimlik doğrulamayı da ihmal etmiyorum." (Katılımcı 50)

"Evet, internet ortamında hakkımdaki bazı bilgileri siliyorum ve gizliyorum." (Katılımcı 2)

"Google'nun 2 adımlı kimlik doğrulamasını kullanıyorum." (Katılımcı 54)

"Sitelerdeki geçmişimi mutlaka temizleyeceğim, e-postalarımdan ve hesaplarımdan çıkış yapacağım. Hiçbir siteye kişisel verilerimi girmiyorum." (Katılımcı 60)

"Evet, önlem alıyorum. Kişisel veritabanımı ve şifremi sık sık değiştiriyorum." (Katılımcı 62)

"Gerekli olmadıkça Elektronik Dijital İmzayı, şifrelerimi ve kullanıcı bilgilerimi başkalarıyla paylaşmamaya gayret gösteriyorum." (Katılımcı 67)

"Evet. Sahte hesaplar kullanarak ve kişisel bilgileri vermeyerek önlem almak lazım diye düşünüyorum." (Katılımcı 47)

"Ara sıra önlem alıyorum. Son zamanlarda internet dolandırıcılığı çoğalınca çok fazla paylaşım yapmamaya çalışıyorum." (Katılımcı 65)

"Önlem amaçlı iki aşamalı doğrulamayı kullanıyorum, ardından ek bir e-posta ve numara kurtarma fonksiyonu daha var. Aslında bu önlemlerin tam koruma sağlayamayacağını fark ettim." (Katılımcı 27)

"Evet, güçlü bir parola belirlemek ve parolayı sık sık değiştirmek, şifrelemeyi etkinleştirmek ve iki faktörlü kimlik doğrulamayı kullanmak çok önemlidir. Bilmediğiniz websiteleri girmemek lazım." (Katılımcı 37)

"Sosyal medyada çoğunlukla 'gizlilik' ilkesini kullanmaya çalışıyorum." (Katılımcı 1)

"Evet, internet ortamında kendim hakkında az bilgi veririm." (Katılımcı 59)

Katılımcıların 14'ü önlem almadıklarını ve şüpheli web sitelere girmeyip, çerezleri kabul etmediklerini de ifade etmiştir.

"Hayır, önlem almıyorum. Çünkü nasıl kullanacağını bilmiyorum." (Katılımcı 19)

"Önlem alıyorum diyemiyorum. Fakat, bu düşünülmesi gereken bir konudur." (Katılımcı 34)

"Şüpheli web sitelere ziyaret etmiyorum" (Katılımcı 53)

"Hayır, hiçbir önlem almıyorum." (Katılımcı 28)

"Maalesef önlemler almıyorum. Özel evraklarım ve bilgilerimi her zaman kendim ulaşabilmem için internet ortamında (ICloud, Drive) tuttuğumdan da endişeleniyorum." (Katılımcı 35)

"Açıkçası, pek fazla önlem almıyorum." (Katılımcı 58)

"Herhangi bir önlem almıyorum, sadece şüpheli internet bağlantılarını açmıyorum." (Katılımcı 44)

"Hayır, maalesef. Fakat web siteleri ziyaret ettiğimde çerezleri kabul etmiyorum." (Katılımcı 51)

"Parolamı sürekli güncellemediğim sürece çok fazla önlem almıyorum." (Katılımcı 29)

Katılımcılardan 3'ü kişisel verileri hakkında bilgi sahip olmadıklarını da dile getirmiştir.

"İnternet ortamında kişisel verilerin güvenliğinin sağlanmasını bilmiyordum." (Katılımcı 16)

"...kişisel verilerimi hiç düşünmemişim..." (Katılımcı 31)

"İnternet ortamında verilerimin başkalarının eline geçmemek için önlemler almayı deneyeceğim." (Katılımcı 17)

Katılımcıların çoğu internet ortamında şifrelerini değiştirip, onu güçlendirdiklerini ve kod veya FaceID ile doğrulama yaptıklarını da belirtmiştir.

"En güçlü şifre, iki adımlı doğrulama ve düzenli aralıklarla kod veya Face ID ile doğrulama yapıyorum." (Katılımcı 42)

"Evet, güçlü bir şifre belirleyeceğim, bildirim ayarlarını zaten devre dışı bıraktım." (Katılımcı 52)

"Sosyal medya hesaplarımda şifremi sık sık değiştiriyorum." (Katılımcı 64)

"Çok sayıda şifre koyuyorum ve bilgi göndermeden önce alıcıyla iletişime geçiyorum." (Katılımcı 22)

"Güvenlik açısından parolamı zor ve karmaşık hale getirmeye çalışıyorum." (Katılımcı 15)

"İnternet ortamında şifrelerimi her yıl değiştiriyorum..." (Katılımcı 21)

Verilen cevaplarda genellikle katılımcıların internete çok fazla kişisel veri girmedikleri, iki adımlı doğrulama kullandıkları veya kişisel bilgileri paylaşmaktan kaçındıkları görülmektedir. Buradan yola çıkarak, araştırmaya katılan Kazakistanlı katılımcıların sosyal medya ve dijital platformlardaki gözetim ve denetim faaliyetlerinden bir ölçüde haberdar oldukları söylenebilir. Çoğu kişi iki adımlı doğrulama veya Elektronik Dijital İmza (örneğin e-Devlet gibi) yöntemleriyle verilerini koruduğunu düşünürken, bazıları ise Face ID veya kod belirleme gibi yöntemlerle güvenlik sağladığını düşünmektedir. Ancak burada asıl korunması gereken, bu ağları elinde bulunduran büyük platformlar ve yöneticileridir.

Buna karşın bazı katılımcılar pek fazla önlem almadıklarını ve yalnızca içerik paylaşırken daha dikkatli davrandıklarını belirtmişlerdir. Bunun gerekçesi olarak ise, ne kadar önlem alınsa da kişisel bilgilere ulaşılabileceği inancını dile getirmişlerdir.

> *"Daha az içerik oluşturmak ve bilgileri önceden dikkatlice kontrol etmek lazım."* (Katılımcı 24)

> *"Veriler çok önemli değil, önemlisi şifreyi kimseye söylememek..."* (Katılımcı 49)

> *"Gelen mesajları dikkatlice okumak, şüpheli bağlantılara tıklamamak, gereksiz durumlarda kişisel bilgileri websitelerde doldurmamak, vb."* (Katılımcı 40)

The Guardian gazetesine göre, birçok ticari şirket ve istihbarat teşkilatı, milyonlarca kullanıcının hesaplarına şifrelerle bile ulaşabilmektedir ve aslında bu şifreleme sistemleri, hesapların ele geçirilmesini kolaylaştırmaktadır. İnsanlar verilerini şifreleyerek korunduğunu düşünseler de, bu şifreler aslında hesaplarının başkalarının eline geçmesine kapı aralamaktadır.

"Önlem almayı deneyeceğim ama bunun tam bir garanti sağlamadığını biliyorum. Bu nedenle kişisel verileri ifşa etmemek, kimlik doğrulama ve şifreleri güçlendirmek gibi önlemler alıyorum." (Katılımcı 45)

Sonuç olarak, şifre koyarak verilerimizi teslim etmiş oluyoruz (James vd., 2013). Yukarıdaki katılımcı bu durumu benzer şekilde açıklamıştır.

3.3.9. Sosyal Medya: Gözetimin Yeniden İnşa Edildiği Bir Zemin

Günümüzde, özellikle sosyal medya platformlarında gerçekleştirdiğimiz tüm etkinliklerimiz ve paylaşımlarımız (kişisel bilgilerimiz, fotoğraflarımız, düşüncelerimiz vb.) kayıt altına alınmakta ve izlenmektedir.

Shenk'e göre, 11 Eylül saldırılarının ardından özellikle Amerika Birleşik Devletleri'nde istihbarat birimlerinin teröristleri izleme konusundaki başarısızlığına dair fikirler yükselirken, toplumda güvenlik endişeleri ve korkuların artmasıyla birlikte bireylerin gözetlenmekten rahatsız olmadıkları ve panoptik devlet modelinin ortaya çıktığı görülmektedir (Shenk, 2003: s. 71). Bu bağlamda, araştırmada katılımcılara *"İnternette yaptığımız araştırmaların ve paylaştığımız tüm verilerin (kişisel bilgiler, fotoğraflar, görüşler vb.) saklanmasının, gözetlenme algısı üzerindeki etkisini nasıl yorumlarsınız?"* sorusu yöneltilmiştir.

> *"Bunun normal olduğunu düşünüyorum. Bilgiler çok uluslu şirketlerin sunucularında saklanıyor ve hiç kimse hiçbir şekilde buna müdahale edemiyor."* (Katılımcı 33)

> *"İnternet araştırmalarının devlet tarafından sıkı bir şekilde kontrol edilmesi gerektiğini düşünüyorum."* (Katılımcı 1)

> *"Genelleme amacıyla yapılan bilimsel ve analitik araştırmalar, anonimliğin korunması şartıyla bireyler için güvenlidir; bu, genel eğilimler, insanların çıkarları ve toplumun bir bütün olarak gelişimi açısından önemlidir. Ve kişisel veriler tehlikeye girdiğinde, bu doğrudan kişisel güvenliği etkiler."* (Katılımcı 45)

> *"Reklam yapmamızın kolay olacağını düşünüyorum."* (Katılımcı 29)

> *"Bir insanın "gözetlenmesi gereken insan" kategorisine katıldığı andan bu tür faaliyetlerin zor olacağını düşünmüyorum. Gözetlenmesi gereken kişi hem ev ortamında hem toplumda ve dışarıda kolayca gözetlenebilir."* (Katılımcı 35)

> *"İnternette paylaştığımız her türlü bilginin saklanmasının, insanları gözetlenme üzerindeki etkisi oldukça büyüktür."* (Katılımcı 2)

> *"Temel olarak bilgiler kontrol altında olmalıdır."* (Katılımcı 30)

> *"Bunu tek bir bağlamda tanımlamak zordur. Çeşitli olabilir. Soru şu ki, bu kontrolü kimin uyguladığına bağlıdır."* (Katılımcı 34)

"50/50 olarak düşünüyorum. Kamuoyuna açık olduğunu düşündüğüm tüm bilgilerin kullanılmasına karşı değilim. Ve bu şekilde işaretlenmemiş tüm bilgilerin kategorize edilmesini istemem." (Katılımcı 37)

Katılımcılardan birçoğu, kişisel verilerin saklanmasının insanları gözetlenme üzerindeki etkisini olumsuz yönde ve tehlikeli olabileceğini dile getirmiştir.

"Bazen sosyal medya sayfalarımda bilgi saldırısı hissediyorum. Tanımadığım insanlar gelip bana zorbalık yapıyor ve olumsuz yorumlar bırakıyor." (Katılımcı 27)

"Bazı İnstagram fenomenleri yurtdışına çıkmışken, onların evleri soyulmuştu..." (Katılımcı 24)

"Paylaştığımız bilgilerin veya kişisel verilerin bir kısmı çalınabilir ve siber zorbalık, etnik ve dinsel nefret gibi zararlı eylemlere yol açabilir. Yani tamamen güvenli olduğunu söyleyemem." (Katılımcı 32)

"Herhangi bir bilgi olumsuz yönde kullanılabilir." (Katılımcı 6)

"Önceden aradığınız şey karşınıza çıkacaksa, şimdi ise düşündüğünüz her şey gerçek olacaktır. Bu benim için korkutucudur." (Katılımcı 23)

"İnternet ortamında paylaşılan kişisel verilerin depolanması, kişilerde sürekli gözetlenme hissi yaratabiliyor. Bu durum derin psikolojik ve özgürlükçü etkilere yol açabilir, insanların mahremiyetini ve özgürlüklerini tehlikeye atabilir ve çevrimiçi ortamda daha temkinli, güvensiz ve kısıtlı davranmalarına neden olabilir." (Katılımcı 58)

"Elbette ki karşıyım. Böyle bir durum kişinin mahremiyetine saldırıdır. Eğer birisi bizim görüşümüzü kullanıyorsa, telif hakkımızı ihlal etmeden bir bağlantı vermeniz tavsiye edilir. Kişisel ve aile fotoğraflarınızı uygunsuz şekilde kullanmamak da iyi bir fikirdir. Mümkünse üçüncü şahısların kişisel bilgileri ve görselleri için izin almayı tercih ederim." (Katılımcı 68)

"Kişisel bilgilerimin çevrimiçi olarak toplanması ve depolanmasının, uygun hizmetler sunarken, gizlilik ihlali ve manipülasyon riskini artırdığına inanıyorum." (Katılımcı 50)

"Bunun çok tehlikeli olduğunu düşünüyorum çünkü hiç kimse hata yapmaktan muaf değil ve yaptıkları hatalar gelecekte kişinin kariyerini sekteye uğratabilecek, nesiller boyu unutulmayacak olumsuz bir izlenim bırakabilecek, hatta iftira atılsa bile kurtulması zor sonuçlar doğurabilir." (Katılımcı 55)

"Bunu bir kişinin mahremiyetine müdahale olarak görüyorum." (Katılımcı 26)

"Ben genel olarak bilgilerin tamamının çevrimiçi kaynaklarda saklanmasına karşıyım. Gerektiğinde herkes orijinal ve noter tasdikli belge kullanabilir." (Katılımcı 67)

"Bence bu korkunç. Bu bir nevi özgürlüğün kısıtlanmasıdır. Kendini özgür hissediyorsun ama görünmez, soyut bir güç senin hakkında her şeyi biliyor." (Katılımcı 51)

"Pek mümkün. Ama böyle bir hukuksuzluğun caiz olduğunu düşünmüyorum." (Katılımcı 31)

"Çok büyük etkisi var. İnternetteki bilgiler bir kişinin günlük yaşamını tahmin edebilir." (Katılımcı 47)

Bazıları ise, bunun için bir şey söylemek zor olduğunu ve hiçbir şey farketmediğini belirtmiştir.

"Ben pek bir şey paylaşmadığım için böyle bir şey farketmedim." (Katılımcı 48)

"Etkisinin ne olacağını tam olarak söyleyemem. Kullanıcılara bilgilerin nasıl toplandığı ve hangi amaçla kullanıldığı konusunda tam bir anlayış sağlamanın önemli olduğunu düşünüyorum." (Katılımcı 39)

"Herkes onu farklı düzeylerde algılasa da, bilgi de herkes için farklı şekilde çalışır." (Katılımcı 18)

*"Hangi bağlamda bakıldığına bağlı olarak bunu söylemek zor." (*Katılımcı 8)

Genel olarak katılımcılar, sosyal medyanın gözetleme amaçlı tasarlandığını ve yaşamlarını etkilediğini belirtmiş; internete yüklenen fotoğrafların gizli olmadığını ve bilimsel veya analitik araştırmalar için verilerin toplandığını ifade etmişlerdir. Örneğin, katılımcıların büyük çoğunluğu sosyal medyanın ve burada yürütülen faaliyetlerin birer izleme mekanizması olduğunu dile getirmiştir. Ancak, bir katılımcı, günümüzde interneti kullanmaktan kaçınmanın mümkün olmadığını savunmaktadır.

"Doğrudan bir etkisi olduğunu düşünüyorum. Ancak şu an için interneti onsuz kullanmak imkansız gibi görünüyor, dolayısıyla onunla idare etmekten başka çaremiz yok:)*"* (Katılımcı 61)

Katılımcıların 8'i ise, bu konuyu internet ortamında başkaları tarafından gözetlenme (Dikizleme Kültürü) şeklinde değerlendirmektedir.

"İnternette yaptığımız her eylemin, gözetim altında olan insanların kişisel sınırlarının ihlali olduğunu düşünüyorum." (Katılımcı 54)

"Öte yandan, güvenliği, terörizmi, pedofiliyi, zorbalığı, bilgi tehditlerini, mali dolandırıcılığı, cinsel tacizi, uyuşturucu bağımlılığını ve çeşitli toplumsal sorunları teşvik eden yayın ve mesajları sınırlamak ve önlemek için de kontrol ve izlemenin gerekli olduğu belirtiliyor. Özellikle çocukları ve bilgi okuryazarlığı düşük olan kişileri tehlikelerden korumak için bu gereklidir. Ama insanlar siyasi, dini vb. görüşlerinden dolayı kısıtlanmamalı." (Katılımcı 60)

"...insanları etkileme, baskı ve yönetim olanaklarını genişletir." (Katılımcı 38)

"Aslında bu tür eylemlerin bazı organlar tarafından yapılmasında bir kayırmacılık olduğunu düşünmüyorum. Çok farklı insanlar olduğu için kimisi dürüstçe yaşarken, kimisi de aşağılık eylemlerde (cinayet, şiddet) bulunuyor. Bu bilginin, suçluların kişisel bilgileri sızdırılmadığı sürece gerektiğinde suçun failinin bulunmasına ve kim olduğunun tespit edilmesine yardımcı olacağını düşünüyorum." (Katılımcı 53)

"Bazı medya kuruluşları yazımızı ve paylaşımlarımızı kullandıklarını bildiriyor ve fotoğraf ve telefon numaramızı bu sosyal ağlardan aldıklarını da iddia ediyorlar." (Katılımcı 65)

"Günümüzün gelişmiş bilgi teknolojileri ve yapay zeka çağında, internette kendimiz hakkında edinilen bilgilerin bizi incelemek, bilgi toplamak ve gerektiğinde bizi izlemek için kullanılabileceğine inanıyorum." (Katılımcı 40)

"Artık hiçbir şey gizli kalmıyor. Kullanmazsanız bir daha olmaz. Evet maalesef her şey kontrol altında." (Katılımcı 64)

"İnsanları gözetliyor, pazarlama ve diğer amaçlar için kullanıldığını düşünüyorum." (Katılımcı 52)

Diğer 2 katılımcı ise, sosyal medyayı bir gözetim aracı olarak görmediklerini ifade etmiş ve internette paylaştıkları fotoğraf anılarının kendilerini rahatsız etmediğini de eklemiştir.

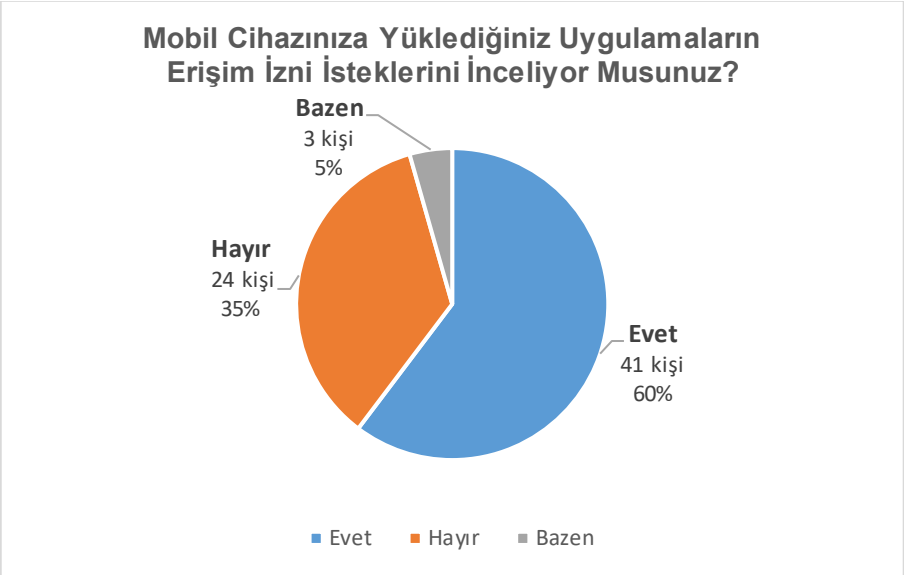
> *"Öncelikle insan sosyal medyada kendini kontrol eder, internet üzerinden resim paylaşarak anılarını da bir şekilde depoluyor. İzlemesi gereken kişi izliyorsa izlesin, bir şey değişmeyecek ki..."* (Katılımcı 44)

> *"Sosyal medyada fotoğraflarımı yükler ve yorumlarımı kendim yazarım. O yüzden bunu bir sır olarak görmüyorum."* (Katılımcı 15)

3.3.10. Onay Süreci ve Kişisel Verilere Erişim

Günümüzde, bildirimler, onaylar ve kişisel bilgilere erişim izinleri, mahremiyeti korumada en yaygın yöntemlerden biridir. Yeni bir uygulama indiren ya da bir çevrimiçi hizmet için hesap oluşturan kullanıcı, o uygulama ya da hizmeti kullanmadan önce onay vermek zorundadır. Kullanıcı genellikle bu bilgilendirme metinlerini okuyarak, mahremiyet haklarını koruyacak koşulları öğrenir ve ardından onay kutusuna tıklayarak kabul eder. Fakat Apple, Google ve Microsoft gibi büyük teknoloji şirketlerinin sunduğu bu şartların asıl hedefi farklıdır. Facebook, kullanıcıların tüm verilerini ticari olarak kullanabilme hakkını elinde tutarken, Instagram ve Snapchat gibi sosyal medya platformları da kullanıcıların yüklediği fotoğrafları telif olmadan kullanabilmektedir (Lokke, 2018: s. 74).

Bu kapsamda, araştırmada katılımcılara mobil cihazlarına yükledikleri uygulamaların fotoğraf, kamera, konum, ses gibi verilere erişim istediğinde; bu talepleri onaylayıp onaylamadıkları sorulmuştur. Katılımcılardan 41'i, uygulamaların erişim izinlerini kontrol ettiğini belirtmiştir. Ancak, 24 katılımcı gizlilik veya mahremiyet metinlerini okumayı zaman kaybı olarak görüp, genellikle doğrudan onayladığını ifade etmiştir. Ayrıca, 3 katılımcı ise bazen bu tür erişim izinlerine onay verdiklerini dile getirmiştir (Şekil 19).



Şekil 19. *Katılımcıların Mobil Uygulamaların Erişim İzni İsteklerini İnceleyip İncelemediğine Dair Görüşleri*

"Evet, elbette inceliyorum. Hangi ayarlarda olduğunu kontrol edeceğim. Fotoğraf izinleri görebiliyor mu, konumu alabiliyor mu diye bir bakacağım. Daha sonra cihazıma kuracağım." (Katılımcı 9)

"Hayır, okumaya üşeniyorum bile. Uygulamaları indirirken hiç kontrol etmemişim." (Katılımcı 23)

"Kontrol etmem gerektiğini bilmeme rağmen kontrol etmekten çekiniyorum." (Katılımcı 55)

"Gerçekten önemsemiyorum, genelde onaylıyorum." (Katılımcı 6)

"Evet, ama bazen okumayı unutuyorum." (Katılımcı 56)

"Maalesef dikkat etmem bu konuda, incelemeden yüklüyorum." (Katılımcı 35)

"Genelde bugünlerde sadece onaylıyoruz. Çok nadiren okuyoruz. Tam olarak incelemiyorum." (Katılımcı 2)

"Hayır, maalesef. Hiç dikkat etmiyorum bu konulara. Çoğunlukla onay verip geçiyorum. Gizlilik politikasını okumak zaman alıyor ve ilgilenmiyorum." (Katılımcı 51)

"Evet. Telefonun hangi fonksiyonlarına izin verildiğine sürekli bakıyor ve değiştiriyorum (kamera, mikrofon vb.)." (Katılımcı 37)

"İzin veriyorum, zorunlu. Eğer fotoğrafları online düzeltmem gerekiyorsa fotoğraflarda erişime izin vermem gerekiyor." (Katılımcı 12)

"Evet, kesinlikle önemsiyorum ve mobil uygulamaların erişim iznini inceliyorum." (Katılımcı 68)

Diğer katılımcılar ise bazı durumlarda, uygulamaları yükleyebilmek için bu izinleri vermek zorunda kaldıklarını ifade etmişlerdir.

"Evet, uygulamaları indirmek için bazen izin veriyorum..." (Katılımcı 22)

"Tabii ki, erişimi her zaman sınırlamaya veya en aza indirmeye çalışırım." (Katılımcı 8)

"Elbette önemsiyorum, ama her zaman değil." (Katılımcı 1)

"Evet, bazen uygulamaları indirmek için erişim izinleri incelemeyi deniyorum." (Katılımcı 32)

"Uygulamalara çok dikkat ediyorum ve bazen izin veriyorum." (Katılımcı 29)

"Muhtemelen izin veriyorum. Vermediğimde uygulama yüklenmiyor. Dolayısıyla onaylamak zorunda kalıyorsun." (Katılımcı 25)

Araştırmaya katılan birçok kişi, mobil uygulamaların onay ve erişim izinleri konusunda dikkatli davrandıklarını, bu nedenle bazen istedikleri uygulamalardan vazgeçtiklerini söylemiştir.

"Çoğu zaman hayır, tüm bilgileri görmesine izin veriyorum. Ama anlamadığım programları yüklemem." (Katılımcı 50)

"Evet, önemsiyorum. Ama sadece tanıdığım ve saygı duyduğum kişilerin önerdiği uygulamaları yüklüyorum." (Katılımcı 60)

"Kesinlikle okuyup inceliyorum ve işime ters gelecekse izin vermiyorum." (Katılımcı 67)

"Evet, yüklediğim uygulamaların erişim izni isteklerini inceliyorum." (Katılımcı 62)

"Hayır kontrol etmiyorum ve uygulamalara onay vermiyorum." (Katılımcı 44)

"Aslında çok önemli bir konu, ama takip etmesi zor." (Katılımcı 24)

"Elbette önemsiyorum ve bu konu hakkında yazılan yazıları inceliyorum." (Katılımcı 42)

Katılımcılardan 4'ü ise hangi uygulamalara izin verip vermeyeceklerini uygulamanın içeriğine göre değerlendirdiklerini aktarmıştır.

"İyi korunan ve kesinlikle güvenli olan mobil uygulamaları kontrol ederek, onlara izin veriyorum ve yüklüyorum." (Katılımcı 65)

"Evet, izinleri her zaman kontrol ediyorum, bazen de kısıtlıyorum." (Katılımcı 45)

"Hayır, önce içeriğine bakarım ve uygun değilse, o zaman o uygulamayı yüklemem." (Katılımcı 19)

"Kesinlikle, her hafta ayarları kontrol ediyorum ve uygulamaları indirirken çok dikkatli olurum." (Katılımcı 33)

3.4. Gözetim ve Mahremiyete İlişkin Analiz Sonuçlarının Değerlendirilmesi

Kazakistan Cumhuriyeti, Doğu Avrupa ile Orta Asya'nın kesişiminde yer alan bir devlettir. Ülkenin batı sınırları Volga Nehri'nin aşağı kısımlarından başlar ve doğuda Altay Dağları'na kadar yaklaşık 3.000 kilometre boyunca uzanır. Kuzeyde Batı Sibirya Ovası'ndan başlayıp, güneyde Tanrı Dağları ile Kızılkum Çölü'ne kadar 1.600 kilometrelik bir mesafeyi kapsar. Kazakistan, Hazar Denizi aracılığıyla Azerbaycan ve İran'a; Volga Nehri ile Volga-Don Kanalı vasıtasıyla ise Azak ve Karadeniz'e ulaşım sağlayabilir. Denizlere doğrudan kıyısı bulunmayan ülkeler arasında yüzölçümü bakımından en büyük ülke konumundadır.

Dünyanın en uzun kara sınırına sahip ülkelerinden biri olan Kazakistan, toplamda beş ülkeyle sınır komşuluğu bulunmaktadır. Bu komşular; kuzey ve batı yönünde Rusya, güneyde Türkmenistan, Özbekistan ve Kırgızistan, doğuda Çin'e bağlı Uygur Özerk Bölgesi (Doğu Türkistan) bulunmaktadır. Ülkenin kara sınırlarının toplam uzunluğu 13.394 kilometreyi bulmaktadır. Ayrıca batısında yaklaşık 2.000 kilometre uzunluğunda Hazar Denizi'ne, güneybatı yönünde ise Aral Denizi'ne kıyısı vardır.

Kazakistan, köklü tarihi ve sunduğu çeşitli fırsatlarla, küresel ölçekte rekabetçi ülkeler arasına katılmayı hedefleyen bir devlettir. Üniter yapıya sahip olan Kazakistan Cumhuriyeti, başkanlık sistemiyle yönetilmektedir. 16 Aralık 1991 tarihinde

bağımsızlığını ilan eden ülkenin başkenti günümüzde Astana'dır. Resmi dili Kazakça olup, Rusça ise farklı etnik gruplar arasında iletişim dili olarak kabul edilmektedir. Ülkenin para birimi Tenge'dir. İdari yapılanması 17 eyaletin yanı sıra, cumhuriyet için özel statüye sahip üç büyük şehirden oluşmaktadır: Astana, Almatı ve Şımkent.

Bu çalışma kapsamında, Kazakistan'da yükseköğretim mezun ve öğrenci olan bireylere; sosyal medya aracılığıyla gözetlenip gözetlenmediklerine ilişkin farkındalık düzeyleri, çevrimiçi ortamlarda kişisel verilerin güvenliğine dair algıları, mahremiyet kavramına atfettikleri önem, zaman içerisinde mahremiyet algılarında meydana gelen değişim ve sosyal medyanın bir gözetim mecrası olarak konumlanıp konumlanmadığına yönelik çeşitli alt temalarda sorular yöneltilmiştir. Yarı yapılandırılmış mülakat tekniği ile elde edilen veriler, belirlenen tematik çerçeveler doğrultusunda sistematik olarak analiz edilmiştir. Bu bölümde, katılımcı görüşlerinden elde edilen bulgular bütüncül bir bakış açısıyla değerlendirilmekte ve ilgili değerlendirmelere ilişkin analitik yorumlara yer verilmektedir.

Görüşmeler, Kazakistan'ın çeşitli bölgelerinde yükseköğretim mezun ve öğrenci olan bireylerin katılımıyla gerçekleştirilmiştir. Araştırma kapsamında katılımcıların belirlenmesinde kartopu örnekleme yöntemi tercih edilmiştir. Katılımcıların demografik dağılımı incelendiğinde, 19'unun lisans, 29'unun yüksek lisans ve 20'sinin doktora düzeyinde eğitim aldığı; cinsiyet açısından ise 45'inin erkek, 23'ünün kadın olduğu görülmektedir.

Kadın katılımcıların sosyal medyada geçirdiği günlük ortalama süre 3,13 saat iken, erkek katılımcılar için bu süre ortalama 3,02 saattir. En yoğun biçimde kullanılan sosyal medya platformları sırasıyla Instagram, Facebook ve WhatsApp olarak belirtilmiştir. Katılımcıların ifadelerine göre sosyal medya en çok bilgi edinme ve güncel gelişmeleri takip etme amacıyla kullanılmaktadır. Katılımcıların 12'si ise "Boş vakit geçirmek" ve 11 katılımcının "Eğlence" amaçlı kullandıkları tespit edilmiştir. Sosyal medyayı "Diğer" amaçlı kullanan 10 katılımcılar ise; kendi işi, mesleği, ticaret, eğitim ve yakınları ile iletişim kurmak için kullandıklarını belirtmiştir.

Araştırmaya dâhil edilen ve Kazakistan'da yükseköğretim mezun ve öğrenci olan katılımcıların, mahremiyet kavramına ilişkin temel bir bilgi birikimine sahip oldukları görülmektedir. Katılımcılar, mahremiyeti başkalarının erişimine kapalı tutulması gereken, bireye ait özel bilgi ve veriler olarak tanımlamaktadır. Bu çerçevede,

mahremiyet kapsamında değerlendirilen veriler arasında kimlik kartı bilgileri, ikamet adresi, özel mesaj içerikleri ve anlık konum bilgileri öne çıkmaktadır. Ayrıca, sosyal medya mecralarının yaygın kullanımıyla birlikte bireylerin mahremiyet algılarında belirgin bir dönüşüm yaşandığı, sanal ortamda mahremiyetin sınırlarının silikleştiği ifade edilmiştir. Cinsiyet temelinde gerçekleştirilen analizlerde, kadın katılımcıların mahremiyeti daha çok ailevi bilgiler, kişisel sağlık durumu ve bireysel verilerin yabancılardan gizlenmesi gerekliliği üzerinden tanımladığı; erkek katılımcıların ise kimlik, lokasyon, iletişim içerikleri ve sağlık bilgileri gibi öğelerin gizliliği, korunması ve üçüncü şahıslara ifşa edilmemesi gerektiği yönünde bir mahremiyet anlayışına sahip oldukları gözlemlenmiştir.

Katılımcıların 47'si internette bilgilerin güvende olmadığını ve 12'si ise güvende olduğunu ifade etmektedir. Katılmcıların cevaplarında genel olarak internette kişisel verilerini girmediklerini ve iki faktörlü kimlik doğrulamayı veya çok fazla kişisel veriler paylaşmamaya özen göstermeye çalıştıklarını belirtmektedir. Bununla beraber araştırmada katılımcılara *"İnternet ortamında kişisel verilerinizin güvenliğini sağlamak ve başkalarının eline geçmesini önlemek için önlemler alıyor musunuz? Eğer alıyorsanız, hangi tür önlemler alıyorsunuz?"* şeklinde sorulmuştur. 20'den fazla katılımcının önlem aldıklarını ve katılımcıların 14'ü önlem almadıklarını ve şüpheli web sitelere girmeyip, çerezleri kabul etmediklerini ifade etmiştir. Bazı katılımcılar, kişisel verilerin korunması noktasında kapsamlı önlemler almadıklarını, bunun yerine sosyal medya paylaşımlarında daha temkinli davrandıklarını ifade etmişlerdir. Bu tutumlarını, alınan önlemlerin yetersiz kalabileceği ve kişisel verilere erişimin her koşulda mümkün olabileceği yönündeki inançlarıyla gerekçelendirmişlerdir. Öte yandan, katılımcıların büyük bir kısmı çevrim içi güvenliği sağlamak adına şifrelerini belirli aralıklarla yenilediklerini, bu şifreleri daha karmaşık hale getirdiklerini ve ek olarak iki faktörlü kimlik doğrulama yöntemleri (örneğin, doğrulama kodları veya yüz tanıma sistemi/FaceID) kullandıklarını belirtmişlerdir.

Bu araştırmada sırasında, *"Size göre kişisel verilerin paylaşımı kişisel mahremiyeti ihlal ediyor mu, ediyorsa niçin?"* diye sorulduğunda, katılımcıların çoğu mahremiyeti ihlal ettiklerini, çünkü kişisel veriler ile ilgili kişinin izni/rızası olmadan paylaşılıyorsa, bu kişisel mahremiyetin ihlali anlamına geldiğini, internet dolandırıcılarının kişisel bilgileri kendi yararına kullandığını ve Kimlik kartı ve sağlık bilgilerinin paylaşılmaması

gerektiği görülmektedir. Katılımcıların 7'si kişisel verilerin paylaşımı kişisel mahremiyeti ihlal etmediğini düşünürken, bazı katılımcılar ise, Kimlik ve banka kartı kartı bilgilerinin paylaşılması kişisel mahremiyetin ihlal edildiğini belirtmişlerdir. Bazıları ise, kendi rızasıyla kişisel verilerin paylaşılmasının kendi tercihi olduğunu ve kimilerine göre bunun için çok fazla ihlal etmediklerini yalnızca günümüzde artık bunu normal olarak karşıladığını öne sürmüştür. Bunun yanı sıra diğer katılımcılar, teknolojinin gelişiminin ve mobil uygulamaların mahremiyetin kaybolmasına sebep olduğunu da düşünmektedirler.

Araştırma kapsamında katılımcılara, *"Sosyal medya platformlarında en sık hangi tür içerikleri paylaşıyorsunuz ve hangi içeriklere "Beğen" veya "Paylaş" butonunu basıyorsunuz?"* sorusu yöneltilmiştir. Katılımcıların büyük bir bölümü, sıklıkla "Beğen" ve "Paylaş" butonunu bastıklarını ifade etmiştir. Buna karşılık, 7 katılımcı herhangi bir içeriğe "Beğen"i ya da "Paylaş'ı Tıklamıyorum" yanıtını vermiştir. Katılımcılardan 10'u siyaset, iş, ekonomi içerikli bilgileri beğendiğini ve paylaştıklarını araştırılırken, katılımcılardan 9'u ülke ve toplum için faydalı olan içerikleri beğendiğini ve paylaştıklarını ifade etmiştir. Fakat katılımcılardan 7'si sosyal medyayı takip etmediğini ve içerikleri beğenmeyip paylaşım yapmadıklarını ifade etmektedirler. Ayrıca katılımcılardan birçoğu sosyal medyada eğlenceli içeriklere "Beğen" ve/veya "Paylaş" yaptığını ve katılımcılardan çoğu sosyal medya hesaplarında bilim, eğitim, bilişsel, spor vb. alanlardaki içeriklere "Beğen" butonunu bastıklarını ifade etmektedirler. Katılımcılardan 7'si manevi ve psikoloji konularında içerikleri beğendiğini ve paylaştığını belirtmişse; kendi mesleği, kişisel ve aile hayatı ile ilgili içerikli "Paylaş"ımlarda bulunduğu tespit edilmiştir.

Yarı yapılandırılmış görüşmeler kapsamında katılımcılara, sosyal medya kullanımında gözetlendiklerinin farkında olup olmadıkları ve sosyal medyayı bir gözetim mekanizması olarak algılayıp algılamadıkları sorulmuştur. Bu bağlamda, 45 katılımcı sosyal medya üzerinden izlendiğinin bilincinde olduğunu ifade ederken, 2 katılımcı zaman zaman böyle bir izlenim edindiğini, 3 katılımcı ise bu konuda bilgi sahibi olmadığını belirtmiştir. Katılımcıların 11'i sosyal medyada gözetlenmediğini ve bunu sorun olarak görmediklerini düşünmektedirler. Endişe verici bir cevap veren katılımcılardan 1'si gözetimden dolayı sosyal medyayı bırakmak istediği tespit edilmiştir.

Araştırma kapsamında katılımcılara internetin, özellikle de sosyal medya platformlarının, gözetimin yeniden üretildiği bir alan olup olmadığı sorulmuş; pek çok katılımcı sosyal medyanın gözetleme amacıyla tasarlandığı ve bireylerin yaşamlarını çeşitli şekillerde etkilediği görüşünü ifade etmiştir. Paylaşılan içeriklerin gizlilik niteliğini yitirdiği, bu verilerin ise sıklıkla bilimsel ve analitik çalışmalarda kullanılmak üzere talep edildiği belirtilmiştir. Katılımcıların çoğunluğu, sosyal medya kullanımını bir tür dijital denetim aracı olarak değerlendirmiş ve bu durumun potansiyel riskler barındırdığını vurgulamıştır. Öte yandan, yalnızca 2 katılımcı sosyal medyayı bir gözetim aygıtı olarak görmediğini ifade etmiş; paylaştıkları fotoğrafların herhangi bir mahremiyet problemi yaratmadığını savunmuştur. Ayrıca katılımcılardan birisi, şu an interneti kullanmamak imkansız olduğunu savunmuştur.

Katılımcıların 41'i, mobil uygulamaların erişim izinlerini incelediklerini belirtmiştir. Ancak bu katılımcıların bir kısmı, ilgili uygulamaların gizlilik politikalarını okumadan onay verdiklerini kabul ederken; diğer bir kısmı ise bu konuda daha dikkatli davrandıklarını ve gerekli görmedikleri takdirde erişim izni vermediklerini ifade etmiştir. Bunun yanında, bazı katılımcılar ise yalnızca uygulamayı kullanabilmek adına, zaman zaman zorunlu olarak bu erişim izinlerini kabul ettiklerini dile getirmiştir.

Bu araştırma; dijital mahremiyetin yalnızca teknik değil, aynı zamanda kültürel ve bireysel farkındalıkla da şekillenen bir olgu olduğunu göstermektedir. Katılımcıların sosyal medya kullanımlarındaki mahremiyet algısı, veri güvenliği davranışları ve gözetim farkındalıkları arasında dikkat çekici ilişkiler saptanmıştır. Bu durum, Kazakistan'daki genç nüfusun dijital dünyaya dair gelişen farkındalığını ve buna bağlı tutumlarını anlamak açısından önemli bir içgörü sunmaktadır. Araştırmanın sonuçları, dijital haklar, mahremiyet eğitimi ve sosyal medya politikalarının yeniden değerlendirilmesi açısından da yol gösterici niteliktedir.

SONUÇ VE ÖNERİLER

Teknolojide yaşanan gelişmeler toplumun özgürlük ve haklarını kısıtlayıcı olmaması, tersine özgürlük ve hakları genişletici mahiyette olması gerekmektedir. Bu amaçla söz konusu her ülkedeki düzenlemeler ve yönetmelikler, teknolojideki gelişmelerden satın alıcıların azami düzeyde emniyetli bir ortamda yararlanabilmeleri amacı ile çıkartılmıştır.

Günümüz dijital çağında, web merkezli bir yaşam ortamında yetişen çocuklar ve gençlerin yaşam öyküleri, teknolojinin bireysel kimlik oluşumu ve yaşam algısı üzerindeki dönüştürücü etkisini ortaya koyan önemli ampirik veriler sunmaktadır. Sosyal medya platformlarında bireylerin özel yaşamlarına ilişkin içerikleri sürekli olarak paylaşmaları, bu paylaşımlara yönelik toplumsal tepkileri beklemeleri ve bu doğrultuda diğer kullanıcıları izleyip değerlendirme eğiliminde olmaları, mahremiyet algısında derin bir dönüşüme işaret etmektedir.

Sosyal medya kullanımının hızla artması ve yaygınlaşması, mahremiyet kavramını gözetim ve güvenlik gibi diğer konularla birlikte ele alınmasına yol açmıştır. Mahremiyetin hem bireysel hem de teknolojiye odaklı bir yönü olduğu için, herhangi bir kişisel bilgi kolayca hassas bir hale gelebilmektedir. Zira sosyal ağlar yalnızca iletişim aracı olarak kullanılmamakta; aynı zamanda kişisel profillerin oluşturulması, bilgi paylaşımı, uygulama paylaşım havuzları ve kullanıcılar arasında sosyal bağ kurulması gibi çeşitli amaçlarla da kullanılmaktadır.

Bu araştırma, yarı yapılandırılmış görüşmeler aracılığıyla gerçekleştirilmiş ve Kazakistan'daki yükseköğretim öğrencileri ile mezunlarının mahremiyet kavramına dair bilgi düzeylerinin bulunduğunu, kavrama yönelik genel bir farkındalığa sahip olduklarını ve sosyal medyanın ortaya çıkışıyla birlikte mahremiyetin anlamının dönüşüme uğradığının farkında olduklarını ortaya koymuştur. Teknolojik gelişmelerin beraberinde getirdiği çeşitli (mobil) uygulamalar sayesinde bireylerin özel bilgilerine erişim izni sağlanabilir hale gelmiş; böylece geçmişte mahrem olarak değerlendirilen pek çok unsur, artık bu şekilde algılanmamaya başlamıştır. Ayrıca Kazakistan'da yapılan araştırmada bireylerin, sosyal medya aracılığıyla bazı kişisel bilgileri gönüllü olarak paylaştığı ve bunun toplumsal uyum için olağanlaştığı gözlemlenmiştir. Araştırmada katılımcıların sosyal medya platformları aracılığıyla izlendiği ve denetlendiği konusunda bilinçli oldukları; ancak bu dijital ağların gözetim mekanizmalarının nasıl işlediğinden her zaman

haberdar olmadıkları anlaşılmıştır. Bununla birlikte, internet ortamında paylaşılan bilgilerin tam anlamıyla güvenli olmadığı, alınan çeşitli önlemlere rağmen uygulama sahiplerinin kişisel verileri ellerinde tuttukları ve bu bilgileri farklı amaçlarla kullanabilecekleri sonucuna ulaşılmıştır. Kişisel verilere erişim sağlanmadan önce gizlilik politikalarının okunması ve onay verilmesi istenmekteyse de, araştırma bulguları, katılımcıların bir kısmı bu uzun metinleri zaman kaybı olarak gördüğünü, bu nedenle okumaktan kaçındıklarını ve çoğunlukla önemsemediklerini göstermiştir.

Belirli mekânlarda ve durumlarda gözetimin yoğunlaştığını kabul edilmektedir. Örneğin, bir havaalanı kontrolünden geçerken bedeniniz ve eşyalarınız özel cihazlarla taranmakta; bazı ülkelere girişte parmak izi verilmesi ve retina taramasına tabi tutulma zorunluluğu doğmaktadır. İşsiz kaldığınızda ve sosyal yardıma başvurduğunuzda ise daha farklı bir denetim süreci işlemeye başlar; bu süreçte çabalarınız, niyetleriniz ve gelişim durumunuz sistematik biçimde kayıt altına alınır. Devlet kurumları, hastaneler ve eğitim kurumları gibi yapılar, her biri kendi denetim mekanizmaları ve veri sistemlerine sahiptir. Ancak tüm bu denetimler yalnızca özel mekânlarda değil, gündelik yaşamın olağan anlarında da karşımıza çıkar. Sokakta yürürken dahi büyük olasılıkla birçok güvenlik kamerası tarafından izlenmektesiniz; kredi kartı harcamalarınız, çevrimiçi arama geçmişiniz ve telefon görüşmeleriniz kolayca takip edilebilir durumdadır. Güvenlik teknolojileri, yakın dönemde kaydettiği gelişimle birlikte yalnızca toplum yapısına değil, bireysel yaşamlarımıza ve hatta bedenlerimizin mahrem katmanlarına kadar nüfuz etmeye başlamıştır.

Çağımızda gözetim olgusu yalnızca belirli alanlarla sınırlı kalmayıp, toplumsal yaşamın bütününü kuşatan bir norm halini almaktadır. Foucault'nun da belirttiği üzere, "hapishane" yalnızca fiziksel bir mekân değil, bireyin evinden dışarı adım attığı anda başlayan bir denetim alanıdır; hatta bu süreç daha da önce başlayabilir. Bu durumu, bireyin gözetlendiğinin farkında olmadan içselleştirmesiyle mi kabullendiği, yoksa başka bir alternatifin bulunmaması nedeniyle mi mecburen benimsediği tartışmaya açıktır. Her iki olasılık da geçerli olabilir; ancak her ikisinin temelinde korkunun yattığı görülmektedir. Birey, hapishane toplumunun koşullarını kabullenir çünkü onun dışındaki belirsizlik daha büyük bir tehdit olarak algılanmaktadır. İnsan, sadece güvenliğin nesnesi değil, aynı zamanda bu güvenlik rejiminin öznesidir de. Toplumsal bir sorumluluk duygusuyla çevresine karşı sürekli tetikte olur; örneğin metroda şüpheli davranışları

izlemeye yönelir. Bu bağlamda korku, bireyin kendi iradesiyle güvenlik mekanizmalarına katkı sunmasını meşrulaştıran temel bir güdü haline gelmiştir.

Tüm bu değerlendirmeler ışığında, dijital çağda gözetimin yeniden inşa edildiği bir zeminin varlığından söz edilebilir. Özellikle sosyal medya, bu gözetim biçiminin yeniden üretildiği temel alanlardan biri olarak öne çıkmaktadır. Kişisel verilere güvenlik amacıyla erişim sağlanırken dahi bireylerin gözetim altında oldukları gerçeği göz ardı edilmemelidir. Mahremiyet bağlamında ise, Kazakistan'daki bireylerin bu kavrama dair bilgi sahibi oldukları ve mahremiyet algılarının zaman içinde değişim geçirdiğine inandıkları görülmektedir. Araştırma sonuçları, bireylerin kişisel verilerini paylaşma konusunda temkinli davranmaya çalıştıklarını ortaya koymaktadır. Bunun nedeni olarak, bazı kişilerin gözetimin yalnızca tanınmış ya da önemli figürler için değil, sıradan insanlar için de uygulandığının farkında olmaları gösterilebilir. Kişisel bilgiler, korunması gereken hassas verilerdir. Bu nedenle, bireylerin mahremiyet hakları ve kişisel veri güvenliği konularında bilgilendirilmesi ve farkındalıklarının artırılması gerekmektedir. Bu amaçla seminerler, projeler ve konferanslar düzenlenebilir. Bu tür çalışmalar, bireylerin dijital dünyada daha bilinçli hareket etmelerini ve mahremiyet haklarını koruyabilmelerini sağlayacaktır.

Katılımcıların büyük çoğunluğu, çeşitli sosyal medya ve mobil uygulamalar yoluyla kişisel bilgilerinin izlenebilir ve kullanılabilir hale geldiğinin farkındadır. Ancak bu platformların gizlilik politikalarını çoğunlukla okumadıkları gözlemlenmiştir. Bununla birlikte, sosyal medya gibi dijital ağların yalnızca güvenlik gerekçeleriyle değil, aynı zamanda ticari çıkarlarla da kullanıcıların verilerini izlediği ve bu durumun sıradan bireyler için de ciddi mahremiyet tehditleri yarattığı anlaşılmıştır.

Sosyal medyada her geçen gün daha da azalan ve anlamını yitiren mahremiyet, dikkate alınması gereken önemli bir mesele olarak öne çıkmaktadır. Bu nedenle, yapılan literatür incelemeleri ve anket verileri ışığında Kazakistan'da yükseköğretim mezun ve öğrencilerinin dijital çağda gözetim ve sosyal medya mahremiyeti ile ilgili olarak dikkat edilmesi ve uygulayabilinmesi gereken bazı önerileri aşağıdaki başlıklar altında ifade etmek mümkündür.

İlk olarak "genel farkındalık ve bilinçlenme" başlığı altında mahremiyet ve gözetim konularında bilinçli olmak, sosyal medyada yaptığımız paylaşımların uzun vadede nasıl kullanılabileceğini ve üçüncü taraflara nasıl aktarılabileceğini öğrenmek gerektiğinin

altını çizilmelidir. Aynı şekilde dijital ayak izini azaltmak için sosyal medya gizlilik ayarlarının düzenli olarak kontrol etmek ve güncellemek de önemlidir.

"Kişisel verilerin korunması" başlığında ise gerçekten gerekli olmadıkça kişisel verileri paylaşmaktan kaçınmanın önemli olduğudur. Özellikle kimlik, adres, finansal bilgi gibi hassas verileri sınırlı paylaşmak gerekmektedir. Bunun yanı sıra güçlü parolalar kullanmak ve iki aşamalı kimlik doğrulamayı aktif etmek de mahremiyetin korunmasına yardımcı olacaktır.

"Mobil uygulamalar ve erişim izinleri" de bir başka önemli başlıktır. Bunun için yeni bir uygulama yüklerken erişim izinleri mutlaka gözden geçirilmelidir. Uygulamanın neden bu bilgilere ihtiyaç duyduğunu anlamak ve gerekirse kısıtlamaktan kaçınılmamalıdır. Gereksiz uygulamaları cihazlardan kaldırmak da önemlidir. Çünkü, kullanılmayan uygulamalar bile arka planda veri toplayabilir.

"Sosyal medya kullanımında iletişim dili ve paylaşımlar" konusunda ise, ne paylaşıldığına dikkat etmek, her paylaşımın sosyal medyada kalıcı izler bırakabileceğini ve farklı şekillerde kullanılabileceğini unutmamak gerekmektedir. Yine çevrim içi ortamlarda yanlış anlaşılmalara ve özel bilgilerin ifşasına yol açabilecek paylaşımlardan da kaçınmak gerekmektedir.

"Eğitim ve ileri seviye güvenlik" bağlamında da mahremiyet ve gözetim konularında çevrim içi eğitimlere katılmak, kurslar ve seminerler aracılığıyla bilginin artırılmasına çaba gösterilmelidir. Dijital vatandaşlık, sosyal medya etiği gibi ders veya atölye çalışmalarına katılmak, dijital becerilerin geliştirilmesine destek olacaktır.

Son olarak da "toplumsal ve hukuki haklar" başlığı altında kullanıcıların kendi ülkelerindeki veri koruma yasalarını ve sosyal medya platformlarının kullanıcı haklarını öğrenmelerinin önemli olduğunun altını çizmek gerekir. Buna paralel olarak da dijital ortamda yaşanabilecek mahremiyet ihlallerine karşı nasıl hukuki adımlar atılabileceğini araştırmak ve bu konuyla ilgili bilgi edinmek de günümüz sosyal medya alanında mahremiyetin korunması açısından zorunluluk halini almaktadır.

Altı çizilen önerilerin hayata geçirilmesi ve sivil bilinçlenmenin arttırılması bağımsızlık sonrası dönemde hızlı bir dijitalleşme çabası içinde olan Kazakistan'da mahremiyetin ve kişisel verilerin korunması açısından daha da önemlidir. Bu nedenle gerek kamu yetkilileri gerekse sivil toplum örgütleri Kazakistan halkının, dijital çağda mahremiyetin önemi ve korunması hakkında bilinçlendirme için önlemler almalı ve gerekli çabaları yoğunlaştırmalıdır.

KAYNAKÇA

Adilet.zan.kz. (2023, Kasım 25). *2005-2007 yıllarında Kazakistan Cumhuriyeti'nde "E-devlet" oluşumunun devlet programı hakkında (Қазақстан Республикасында "электрондық үкімет" қалыптастырудың 2005–2007 жылдарға арналған мемлекеттік бағдарламасы туралы).* https://adilet.zan.kz/kaz/docs/U040001471_ (Erişim tarihi: 25.11.2023)

Aktaş, C., & Çaycı, B. (2013). Yeni enformasyon ve iletişim teknolojilerinin sosyal hayattaki rolü / *The role of new information and communication technologies in social life*. In *Proceedings of the 1st International Symposium on Media Studies* (ss. 621-629).

Anık, M. (2019). Sosyal Medyada Mahremiyetin İfşası: Georg Simmel Ekseninde Eleştirel Bir Değerlendirme. İçinde Nafize Şişman (Ed.), *Mahremiyet: Hayatın Sırları ve Sınırları* (1.). İstanbul: İnsan Yayınları.

Arık, E. (2018). *Dijital Mahremiyet.* Yeni Medya ve Gözetim Toplumu. Konya: LİTERATÜRK Academia.

Assange, J., Appelbaum, J., Müller-Maguhn, A. & Zimmermann, J. (2013). *Şifrepunk.* Özgürlük ve İnternetin Geleceği Üzerine Bir Tartışma. İstanbul: Metis Yayınları.

Baban, E. (2012). Mc Luhan ve Baudrillard'ın Penceresinden Sosyal Medyanın Etkisi: İfadenin Esareti, Gözetlenen Toplum ve Kayıp Kimlik Sendromu. Tolga Kara ve Ebru Özgen (Ed.), *Sosyal Medya Akademi* içinde (s. 57-82). İstanbul: Beta Yayınları.

Baltacı, A. (2018). Nitel Araştırmalarda Örnekleme Yöntemleri ve Örnek Hacmi Sorunsalı Üzerine Kavramsal Bir İnceleme. *Bitlis Eren Üniversitesi Sosyal Bilimler Enstitüsü Dergisi,* 7(1), 231-274.

Barbarosoğlu, F. (2015). *Şov ve Mahrem.* İstanbul: Profil.

Bauman, Z. (2001). *Bireyselleşmiş Toplum* (Çev. Yavuz Alogan). İstanbul: Ayrıntı Yayınları.

Bauman, Z., ve Lyon, D. (2013). *Akışkan Gözetim* (Çev. E. Yılmaz), İstanbul: Ayrıntı Yayınları.

Bayraktutan, G., Binark, M., Çomu, T., Doğu, B., İslamoğlu, G. & Aydemir, A. T. (2012). Sosyal Medyada 2011 Genel Seçimleri: Nicel-Nitel Arayüzey İncelemesi. *Selçuk İletişim Dergisi,* 7, 3, 15-16.

Begen, R. (2024). "Dijital Gözetim Çağındf Panoptikon: Kazakistan Cumhuriyeti Elektronik Hükümeti Portalı (Egov.Kz)", *"Communicata" Dergisi,* Atatürk Üniversitesi Yayınları, Yıl 2024, Sayı: 28, 8-17, 17.09.2024 https://dergipark.org.tr/tr/pub/communicata/issue/87235/1423901

Bennett, C. (1992). *Regulating Privacy: Data Protection and Public Policy in Europe and The United States.* Ithaca, MI: Cornell University Press.

Bentham, J. (2016). Panoptikon. Gözün İktidarı (Çev. Z. Özarslan, ve B. Çoban), İstanbul: Su Yayınları.

Bıyıkbeyi, T. (2019). *Benimsenmiş Ulusal Kültürel Değerler Sınıflandırması Bağlamında Panoptikon, Psikolojik Güçlendirme ve İş Tatmini Arasındaki İlişki: Bir Alan Araştırması.* Kahramanmaraş Sütçü İmam Üniversitesi Sosyal Bilimler Enstitüsü, Doktora Tezi. Kahramanmaraş.

Bitirim Okmeydan, S. (2017). "Postmodern Kültürde Gözetim Toplumunun Dönüşümü: 'Panoptikon'dan 'Sinoptikon' ve 'Omniptikon'a". *AJIT-e: Online Academic Journal of Information Technology,* 8 (30), 45-69.

Boyd, D. (2006). "Friends, Friendsters, and Top 8: Writing Community Into Being on Social Network sites". 11, 12. https://firstmonday.org/ojs/index.php/fm/article/view/1418/1336 (Accessed: 21.10.2024)

Boyd, D.M., & Ellison, N.B. (2007). Social Network Sites: Definition, History, and Scholarship. *Journal of Computer: Mediated Communication*, 13(1), 210-230.

Bruns, A. & Moe, H. (2016). "Twitter'da İletişimin Katmanları". (Der. Katrin Weller vd.). *Twitter ve Toplum* (s. 62-78). İstanbul: Kafka.

Burgess, J. & Green, J. (2009). YouTube Online Video and Participatory Culture. Cambridge, UK: Polity Press.

Castells, M. (2006). *Enformasyon Çağı: Ekonomi, Toplum ve Kültür. -Kimliğin Gücü-* 2.Cilt. İstanbul: İstanbul Bilgi Üniversitesi.

Castells, M. (2008). *Enformasyon Çağı: Ekonomi, Toplum ve Kültür. -Ağ Toplumunun Yükselişi-* 1.Cilt. İstanbul: İstanbul Bilgi Üniversitesi.

Cılızoğlu, G. Y. & Çetinkaya, A. (2016). "Sivil Toplum Örgütlerinin Instagram Kullanımı". *Asos Journal,* 4, 27, 161-181.

Çaycı, A. E., ve Çaycı, B. (2017). Dijital İletişim Çağında Teknolojinin Açığa Çıkardıkları: Gözetim ve Mahremiyet. *The Turkish Online Journal of Design,* 7(1), 36-46.

Çoban, B. (2014). *"Yeni Panoptikon Gözün İktidarı ve Facebook"* (Ed. Barış Çoban). Sosyal Medya Devrimi (s. 303-318). İstanbul: Su Yayınları.

Deborah, G. J. (2001). *Computers Ethics.* Prentice-Hall, Inc.

Deleuze, G. (1992). *"Postscript on the Societies of Control".* October, Vol. 59: 3-7.

Demir, A. (2017). "Panopticon ve Synopticon Geriliminde Özgürlük Paradoksu". *KAYGI Uludağ Üniversitesi Fen Edebiyat Fakültesi Felsefe Dergisi,* 28, 55-67.

Digital Kazakhstan. (2024, Mayıs 28). *"Цифрлық Қазақстан" мемлекеттік бағдарламасы.* https://egov.kz/cms/en/digital-kazakhstan (Erişim tarihi: 28.05.2024)

DLA Piper. (2025, Mayıs 25). *Data protection laws in Kazakhstan.* https://www.dlapiperdataprotection.com/index.html?t=world-map&c=KZ (Erişim tarihi: 25.05.2025)

DLA Piper. (2025, Mayıs 25). *Online privacy in Kazakhstan.* https://www.dlapiperdataprotection.com/?t=online-privacy&c=KZ#insight (Erişim tarihi: 25.05.2025)

Dolgun, U. (2015). Şeffaf Hapishane Yahut Gözetim Toplumu- Küresselesen Dünyada Gözetim, Toplumsal Denetim ve İktidar İlişkileri. İstanbul: Ötüken.

Dolgun, U. (2005). *Enformasyon Toplumundan Gözetim Toplumuna.* 21. Yüzyılda Gözetim, Toplumsal Denetim ve İktidar İlişkileri. Bursa: Ekin Kitabevi.

Draper, R. (2018). "Biri Bizi Gözetliyor". *National Geographic Türkiye.* 202, Şubat, s. 54-89.

EGov.kz Portalı. (2024, Mayıs 27). *Kazakistan Cumhuriyeti'nin Elektronik Hükümeti (Қазақстан Республикасының электрондық үкіметі).* https://egov.kz/cms/kk/information/about/help-elektronnoe-pravitelstvo (Erişim tarihi: 27.05.2024)

E-Hükümetin Başarıları. (2024, Mayıs 29). *Электрондық үкіметтің жетістіктері.* https://egov.kz/cms/kk/information/help/help-elektronnoe-pravitelstvo (Erişim tarihi: 29.05.2024)

Elias, N. (1973 [1939]). *La Civilisation des moeurs.* Paris: Calmann-Levy, s. 271; İngilizce baskısı: The Civilizing process: *The History of Manners and State Formation and Civilization* (Çev. E. Jephcott), Oxford: Blackwell, 1994.

Ercan, S. (2019). *Dijitalizm.* 1. Baskı. İstanbul: Motto Yayınları.

Erdoğan, G. ve Ş. Bahtiyar (2014). "Sosyal Ağlarda Güvenlik". *(XVI. Akademik Bilişim Konferansı Bildirileri).* Akademik Bilişim'14, s. 267-272.

Ernout, A., & Meillet, A. (2001). *Dictionnaire étymologique de la langue latine.* Paris: Klinckseick.

Evans, R. (1971). "Bentham's Panopticon. An Incident in the Social History of Architecture", Architectural Association Quarterly, 3/2: 21-37.

Facebook. (2024, Kasım 14). *Gizlilik İlkesi.* https://tr-tr.facebook.com/privacy/explanation (Erişim tarihi: 12.05.2025)

Flaherty, D.H. (1989). *Protecting Privacy in Surveillance Societies.* Chapel Hill, NC: University of North Carolina Press.

Foucault, M. (2017). *Hapishanenin Doğuşu.* (7. Baskı). (Çev. Mehmet Ali Kılıçbay). Ankara: İmge Kitabevi.

Foucault, M. (1995). *Discipline and Punish: The British of the Prison*. New-York: Random House.

Fuchs, Ch. (2014). *Sosyal Medya: Eleştirel Bir Bakış.* (Çev. D. Saracoğlu ve İ. Kalaycı). Ankara: NotaBene Yayınları.

Gandy, O.H. (1993). Panoptik Çeşit: Kişisel Bilginin Politik Ekonomisi *(The Panoptic Sort: A Political Economy of Personal Information),* Boulder, Colorado: Westview Press.

Gardner, H. & Davis, K. (2013). *APP Kuşağı.* Dijital Dünyada Kimlik, Mahremiyet ve Hayal Gücü. İstanbul: Optimist Yayınları.

Giddens, A. (1992). *Modernity and Self-Identity,* Cambridge: Polity Press.

Giddens, A. (2014). *Modernite ve Bireysel Kimlik.* Geç Modern Çağda Benlik ve Toplum. İstanbul: Say Yayınları.

Gündoğan, A.O. (2019). "Başlangıç"tan Günümüze Mahremiyetin İdrak Edilişi. İçinde N. Şişman (Ed.), *Mahremiyet. Hayatın Sırları ve Sınırları* (ss. 35-50). İstanbul: İnsan Yayınları.

Güven, O.Ö. (2014). "Gözetim Tekniklerinin Güç İlişkileri Bağlamında Dönüşümü ve Toplumsal Denetim". *Atatürk İletişim Dergisi,* 7, 79-112.

Habermas, J. (1989). *The Structural Transformation of the Public Sphere: An Inquiry into a Category of Bourgeois Society.* Cambridge: MIT Press.

Hazır, M. (2019). Siber Toplumda Mahremiyetin Dönüşümü. In. N. Şişman (Ed.), *Mahremiyet. Hayatın Sırları ve Sınırları* (1., pp. 145-161). İstanbul: İnsan Yayınları.

Holtzman, D. H. (2006). Privacy Lost. How Technology Is Endangering Your Privacy. United States of America: Jossey Bass. https://fictionbook.ru/download/david_holtzman_h/privacy_lost_how_technology_is_endangeri/?formats=pdf

Hu, Y., Manikonda, L. & Kambhampati, S. (2014). "What We Instagram: A First Analysis of Instagram Photo Content and User Types". *Proceedings of the Eighth International AAAI Conference on Weblogs and Social Media.* ICWSM.

Instagram. (2022, Ocak 4). *Instagram Veri İlkesi.* https://help.instagram.com/155833707900388 (Erişim tarihi: 12.05.2025)

James, B., Borger, J., & Greenwald, G. (2013). How US and UK Spy Agencies Defeat Internet Privacy and Security.

https://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security (Erişim tarihi: 19.05.2025)

Kabir, S. (2014). "Sanal Röntgencilik ve Facebook'ta Bireyselliğin Kullanımı" (Ed. Barış Çoban). Sosyal Medya Devrimi (s. 290-302). İstanbul: Su Yayınları.

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

Karagülle, A. E. (2015). *Günümüze Değişen Mahremiyet Algısının Sosyal Ağlar Bağlamında İncelenmesi.* İstanbul Ticaret Üniversitesi. Yüksek Lisans Tezi. İstanbul.

Karakaya, B. (2019). Osmanlı Toplumunda Mahremiyetin Sınırlarını "Pencere" Üzerinden Okumak. İçinde Nafize Şişman (Ed.), *Mahremiyet. Hayatın Sırları ve Sınırları* (1.). İstanbul: İnsan Yayınları.

Karakartal, M. (2013, Ağustos 21). Sosyal medya perhizi. *Hürriyet, Kelebek*, s. 5.

Kavut, S. (2023). Dijital Dönüşüm Çağında Gözetimin Elektronikleşmesi: Panoptikon'dan Süperpanoptikon'a Gözetim Toplumu. *Atatürk Üniversitesi Yayınları.* DOI: 10.5152/communicata.2023.23029

Kazakistan Cumhuriyeti E-Devlet Projeleri. (2024, Mayıs 30). *Қазақстан Республикасының электрондық үкіметінің жобалары.* https://egov.kz/cms/kk/information/about/projects (Erişim tarihi: 30.05.2024)

Köse, H. (2011). "Synoptikon" Evresindeki İletişim ya da Küresel Gözetim Toplumunda "İktidar Görünmezliği"nin Sonu. Hüseyin Köse (Ed.). *Medya Mahrem* içinde (ss. 199-225). İstanbul: Ayrıntı Yayınları.

Kuran, N.H. (2005). *Devlet Baba'dan E-Devlet'e: Türkiye için E-Devlet Modeli.* Analiz ve Model Önerisi. 1. Baskı. İstanbul: İstanbul Bilgi Üniversitesi Yayınları.

Kütükoğlu, E. (2021). *Kuşaklar Bağlamında Sosyal Medya ve Mahremiyet.* Konya: Eğitim Yayınevi.

Leavitt, A. (2016). "#FollowFriday'den YOLO'ya". (Der. Katrin Weller vd.). Twitter ve Toplum (s. 205-225). İstanbul: Kafka.

Lee, E., Lee, J., Moon, J. H. & Sung, Y. (2015). "Pictures Speak Louder than Words: Motivations for Using Instagram". *Cyberpsychology, Behavior and Social Networking*, 18, 9, 552-556.

Lewis, T. (2006). 'Critical Surveillance Literacy', Cultural Studies, 6 (2): s. 263-81.

LinkedIn, Gizlilik Politikaları, https://www.linkedin.com/legal/privacy-policy?trk=uno-reg-guest-home-privacy-policy (Erişim tarihi: 12.05.2025)

LinkedIn, LinkedIn Ofisi, https://www.linkedin.com/company/linkedin (Erişim tarihi: 12.05.2025)

Lister, M., Dovey, J., Giddens, S., Grant, I. & Kelly, K. (2009). New Media: A Critical Introduction. New York: Routledge.

Livberber, T. (2018). *Sosyal Medyada Mahremiyet. Gözetim.* Teşhir ve Dikizleme Kültürü. Konya: Literatürk academia.

Lokke, E. (2018). *Mahremiyet: Dijital Toplumda Özel Hayat* (1.). İstanbul: Koç Üniversitesi Yayınları.

Lokke, E. (2018). NOU 1999: 27, "İfade Özgürlüğü Gerçekleşmelidir"; Anayasanın yeni 100. Maddesi için Öneriler. İçinde *Mahremiyet: Dijital Toplumda Özel Hayat* (1.). İstanbul: Koç Üniversitesi Yayınları.

Lyon, D. (1994a). *he Electronic Eye-The Rise of Surveillance Society.* Minneapolis: University of Minnesota Press.

Lyon, D. (1994b). *Elektronik Göz: Gözetlenen Toplumun Yükselişi.* Cambridge: Polity Press.

Lyon, D. (2006). *Gözetlenen Toplum* (Çev. Gözde Soylan). İstanbul: Kalkedon Yayıncılık.

Lyon, D. (2013). *Gözetim Çalışmaları: Genel Bir Bakış* (Çev. Ali Toprak). İstanbul: Kalkedon Yayınları.

Marx, G.T. (1985). "Surveillance Society: The Threat of 1984-style Techniques", *The Futurist,* June: 21-6.

Mattelart, A. (2012). *Gözetimin Küreselleşmesi. Güvenlileştirme Düzeninin Kökeni* (Çev. Onur Gayretli – Su Elif Karacan). İstanbul: Kalkedon Yayınları.

Meyrowitz. J. (1986). *No Sense of Place: The Impact of Electronic Media on Social Behavior.* New York: Oxford University Press.

Nakıboğlu, G. (2015). "Ütopyadan Doğmak, Ütopya Doğurmak: Heterotopya Kavramı ve Heterotopya Bağlamında Balık İzlerinin Sesi". *FSM İlmî Araştırmalar İnsan ve Toplum Bilimleri Dergisi,* 5, 381-407.

Niedzviecki, H. (2010). *Dikizleme Günlüğü: Kendimizi ve Komşularımızı Gözetlemeyi Niçin Bu Kadar Sevdik?* (1.). İstanbul: Ayrıntı Yayınları.

Niedzviecki, H. (2009). *Dikizleme Günlüğü.* (Çev. G. Gündüç). İstanbul: Ayrıntı Yayınları.

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

Oğurlu, Y. (2010). *İdare Hukukunda "E-Devlet" Dönüşümü ve Dijitalleşen Kamu Hizmeti.* 1. Baskı. İstanbul: On İki Levha Yayıncılık.

Özbay, C., Terzioğlu, A., ve Yasin, Y. (2011). *Neoliberalizm ve Mahremiyet: Türkiye'de Beden, Sağlık ve Cinsellik.* İstanbul: Metis Yayınları.

Öztürk, S. (2013). "Filmlerle Görünürlüğün Dönüşümü: Panoptikon, Süperpanoptikon, Sinoptikon". *İletişim Kuram ve Araştırma Dergisi*, 36, 132-151.

Packard, V. (1964). *The Naked Society.* Brooklyn, New York: Ig Publishing.

Patton, M.Q. (1987). *How to Use Qualitative Methods in Evaluation*. Newbury Park: Sage Publications.

Poster, M. (1995). *The Second Media Age,* Cambridge: Polity Press.

Poster, M. (1996). *Computers, Surveillance, and Privacy.* "Söylem Olarak Veri Tabanları", D. Lyon ve E. Zureik (eds). Minneapolis MN: University of Minnesota Press.

Postman, N. (1994). *Televizyon: Öldüren Eğlence.* İstanbul: Ayrıntı Yayınları.

Rizanaj, F.H. (2020). *Yeni Medyada Gözetim ve Mahremiyetin Dönüşümü.* Gözetimin Yeniden Üretildiği Bir Alan Olarak Yeni Medya ve Mahremiyet Algısındaki Değişim. Birinci Basım. Ankara: Gece Kitaplığı.

Rogers, R. (2016). "Twitter'ı Sıradanlıktan Kurtarmak". (Der. Katrin Weller vd.). *Twitter ve Toplum* (s. 9-31). İstanbul: Kafka.

Salomon, D. (2013). "Moving on from Facebook: Using Instagram to Connect with Undergraduates and Engage in Teaching and Learning". *College and Research Libraries,* 74, 8, 408-412.

Schmidt, J.H. (2016). "Twitter ve Kişisel Kamuların Doğuşu". (Der. Katrin Weller vd.). *Twitter ve Toplum* (s. 47-61). İstanbul: Kafka.

Shcherbina, J. (2017). "Reading in the Age of Web 2.0". *Russian Social Science Review*, 58, 1, 86-108.

Shenk, D. (2003). Elektronik Göz: İleri Teknoloji Sizi İzliyor. *National Geographic* (31), 71, 72, 86.

Snowden, Edward (2018). "Facebook Bir İstihbarat Şirketi", Bianet, 20 Mart 2018. https://bianet.org/haber/snowden-facebook-bir-istihbarat-sirketi-195348

Solove, D.J. (2008). *Understanding Privacy*. Harvard University Press.

Statista (2017). Number of Monthly Active Instagram Users from January 2013 to Decdember 2016 (in millions). https://www.statista.com/statistics/253577/number-ofmonthly-active-instagram-users/ (Mart, 2017)

Stefanick, L. (2011). Controlling Knowledge: Freedom of Information and Privacy Protection in a Networked World. Canada: Athabasca University Press.

Strangelove, M. (2010). *Watching YouTube.* London: University of Toronto Press.

Şişman, N. (2019). Sunuş. İçinde *Mahremiyet. Hayatın Sırları ve Sınırları* (1., ss. 7-20). İstanbul: İnsan Yayınları.

Timisi, N. (2003). *Yeni İletişim Teknolojileri ve Demokrasi*. Ankara: Dost Kitabevi.

Toprak, A., Yıldırım A., Aygül E., Binark M., Börekçi S. & Çomu T. (2014). *Toplumsal Paylaşım Ağı Facebook: "Görülüyorum Öyleyse Varım!".* İstanbul: Kalkedon Yayınları.

Towner, T. L. & Muñoz, C. L. (2017). "Picture Perfect? The Role of Instagram in Issue Agenda Setting During the 2016 Presidential Primary Campaign". *Social Science Computer Review,* 1-16.

Twenge, Jean M. ve W. Keith Campell (2010). *Asrın Vebası: Narsizm İlleti.* Çev.: Özlem Yüksel, İstanbul: Kaknüs Yayıncılık.

Uluç, G. ve Yarcı, A. (2017). "Sosyal Medya Kültürü". *Dumlupınar Üniversitesi Sosyal Bilimler Dergisi.* 52, 88-102.

Van Dijk, J. (2016). *Ağ Toplumu.* İstanbul: Kafka.

Vincent, D. (2017). *Mahremiyet: Kısa Bir Tarih* (Birinci Baskı). Ankara: Epos Yayınları.

Warren, S.D. & Brandeis, L.D. (1984). "The Right to Privacy. The Implict Made Explicit". (Ed. FD Shoeman). *Philosophical Dimensions of Privacy: An Anthology* (pp. 75-103). Cambridge: Cambridge University Press.

We Are Social (2025). *"Digital 2025: Kazakhstan"*. The Essential Guide to Digital Trends. https://datareportal.com/reports/digital-2025-kazakhstan

Weller, K. vd. (2016). "Twitter ve Toplum: Giriş". (Der. Katrin Weller vd.). *Twitter ve Toplum*. (s. 33-44). İstanbul: Kafka.

Wikipedia.org. Etnik Gruplar *(Ұлттық құрамы)* https://kk.wikipedia.org/wiki/%D2%9A%D0%B0%D0%B7%D0%B0%D2%9B%D1%81%D1%82%D0%B0%D0%BD_%D0%B4%D0%B5%D0%BC%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%8F%D1%81%D1%8B (Erişim tarihi: 24.05.2025)

Wikipedia. (t.y.). Kazakistan Demografisi *(Қазақстан демографиясы)* https://kk.wikipedia.org/wiki/%D2%9A%D0%B0%D0%B7%D0%B0%D2%9B%D1%81%D1%82%D0%B0%D0%BD_%D0%B4%D0%B5%D0%BC%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%8F%D1%81%D1%8B (Erişim tarihi: 24.05.2025)

Wikipedia. (t.y.). Kazakistan'da Din *(Қазақстандағы дін)* https://kk.wikipedia.org/wiki/%D2%9A%D0%B0%D0%B7%D0%B0%D2%9B%D1%81%D1%82%D0%B0%D0%BD_%D0%B4%D0%B5%D0%BC%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%8F%D1%81%D1%8B (Erişim tarihi: 24.05.2025)

Wikipedia. (t.y.). Okuryazarlık *(Сауаттылық)* https://kk.wikipedia.org/wiki/%D2%9A%D0%B0%D0%B7%D0%B0%D2%9B%

D1%81%D1%82%D0%B0%D0%BD_%D0%B4%D0%B5%D0%BC%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%8F%D1%81%D1%8B (Erişim tarihi: 24.05.2025)

Yavanoğlu, U., Ş. Sarıoğlu ve İ. Çolak (2012). "Sosyal Ağlarda Bilgi Güvenliği Tehditleri ve Alınması Gereken Önlemler". *Politeknik Dergisi*, 15(1), 15-27.

Yıldırım, A., ve Şimşek, H. (2011). *Sosyal Bilimlerde Nitel Araştırma Yöntemleri* (8. Baskı). Ankara: Seçkin Yayıncılık.

Yıldırım, H., Kaplan V., Çakmak T., Üstün C. (2006). *E-Devlet Başa.* (Haz. Ö. Fatih Akpınar) Ankara: Macar Yayıncılık.

YouTube, Politikalar ve Gizlilik, https://www.youtube.com/intl/tr/yt/about/policies/#community-guidelines (Erişim tarihi: 12.05.2025)

YouTube, YouTube hakkında, https://youtube.com/intl/tr/yt/about (Erişim tarihi: 12.05.2025)

Yüksel, M.E., Yüksel, A.S. ve Zaim, A.H. (2013). "A Reputation-Based Privacy Management System for Social Networking Sites". *Turkish Journal of Electrical Engineering and Computer Scienes.* 21, 766-784.

Zappavigna, M. (2016). "Social Media Photography: Construing Subjectivity in Instagram Images". *Visual Communication*, 15, 3, 271-292.

Zimmer, M. & Proferes, N. (2016). "Twitter'da Mahremiyet, Mahremiyet Üzerine Twitter". (Der. Katrin Weller vd.). *Twitter ve Toplum*. (s. 243-258). İstanbul: Kafka.

Zureik, E. (2003). 'Teorizing Surveillance: The Case of the Workplace', içinde D. Lyon (ed.), *Surveillance as Social Sorting,* London and New York: Routledge.

EK 1

Tarih:31/12/2024 08:19
Sayı: E-65836846-044-341674
REKTÖRLÜK

341674

İSTANBUL TİCARET ÜNİVERSİTESİ

T.C.
İSTANBUL TİCARET ÜNİVERSİTESİ REKTÖRLÜĞÜ

TÜRKİYE CUMHURİYETİ'NİN YÜZÜNCÜ YILI

Sayı : E-65836846-044-341674 31.12.2024
Konu : Etik Onayı

Sayın Ruslan BEGEN

İlgi : 24.12.2024 tarihli dilekçeniz.

İlgi yazınız ile "Dijital Çağda Gözetim ve Sosyal Medya Mahremiyeti: Kazakistan Örneği" isimli çalışmanın yarı yapılandırılmış görüşme sorularına Etik Kurul onayı talep edilmektedir.

Adı geçen ve ekte yer alan yarı yapılandırılmış görüşme soruları, Üniversitemiz Etik Kurulunca incelenerek etik tanım, değer ve ilkelere aykırı bir düzenleme tespit edilmediği, önerilen yarı yapılandırılmış görüşme sorularının etik kurallara uygun olduğu ve etik onayının verildiği ifade edilmiştir.

Konuya ilişkin bilgilerinizi rica ederim.

Prof. Dr. Hanifi PARLAR
Rektör a.
Rektör Yardımcısı

Ek: Etik Onaylı Yarı Yapılandırılmış Görüşme Soruları

Bu belge güvenli elektronik imza ile imzalanmıştır.

Belge Doğrulama Kodu:
9A2812B1-B692-44BC-A27A-E624799EA483

Belge Doğrulama Adresi:

Adres: Örnektepe Mah. İmrahor Cad. No: 88/2 Beyoğlu/İstanbul
Telefon No: 444 04 13 / 4583 Faks No: 0212 320 70 11
E-Posta: İnternet Adresi:
KEP Adresi:

Ayrıntılı Bilgi İçin:
Büro Personeli
Telefon No:

EK 2

BİLGİLENDİRİLMİŞ ONAM FORMU

Değerli Katılımcı,

Bu çalışma, ... Prof. Dr. Abdulhamit AVŞAR ..... danışmanlığında İstanbul Ticaret Üniversitesi, ... Lisansüstü Eğitim ~~Fakültesi~~/Enstitüsü, ... Medya ve İletişim Çalışmaları .....

Lisans/Yüksek Lisans/Doktora programı öğrencisi (Adı-Soyadı) ..... Ruslan Begen ..... tarafından yürütülen ..... Dijital Çağda Gözetim ve Sosyal Medya Mahremiyeti: Kazakistan Örneği ..... isimli bir (tez) / makale çalışmasıdır.

Araştırmaya katılımınız tamamen gönüllülük esasına dayanmaktadır. Bu çalışma 18 yaş ve üzeri katılımcıları kapsamaktadır. Araştırma sırasında sizden alınan bilgiler grup halinde değerlendirileceğinden, sizden kimlik belirleyici bilgiler istenmeyecektir. Cevaplarınız gizli tutulacak ve sadece araştırmacı tarafından bilimsel çalışmalarda kullanılacaktır. Bu anlamda, araştırma sonuçlarından sağlıklı bilgiler edinilebilmesi için soruların samimi bir şekilde doldurulması ve soruların boş bırakılmaması oldukça önemlidir. Yarı Yapılandırılmış Görüşme Soruları genel olarak kişisel rahatsızlık teşkil edecek sorular içermemektedir. Araştırmaya katılmayı kabul ettiğiniz takdirde sizinle yaklaşık ..... 20 ..... dakika sürmesi planlanan bir görüşme yapılacak ve görüşmede izninizle ses kaydınız alınacaktır. Ancak görüşme sırasında veya sonrasında herhangi bir nedenden dolayı rahatsızlık hissederseniz, katılımınızı sonlandırabilir ve ses kaydınızın imha edilmesini talep edebilirsiniz. Bu durumda ses kaydınız, ses kayıt deşifreniz silinecek ve basılı herhangi bir veriniz var ise kâğıt öğütücüden geçirilerek imha edilecektir. Çalışma hakkında daha fazla bilgi almak için (Adı Soyadı) ..... Ruslan Begen ..... (e-posta ılaşabilirsiniz. Katılımınız için şimdiden teşekkür ederiz.

Bu çalışmaya tamamen gönüllü olarak katılıyorum (ses kaydımın alınmasına rıza gösteriyorum) ve istediğim zaman katılımımı sonlandırabileceğimi biliyorum. Verdiğim bilgilerin bilimsel amaçlı kullanımını kabul ediyorum (Ses kaydında kişisel bilgilerin yer almamasına özen gösterilmesi gerekmektedir).

Evet ( ) Hayır ( )

Araştırmacının Adı Soyadı

Ruslan Begen

İSTANBUL TİCARET ÜNİVERSİTESİ
ETİK KURUL ONAYI ALMIŞTIR
Kurul Tarihi: 27.12.2024
Kurul Karar No: 12-12

Demografik Bilgi Formu

1. **Yaşınız**
   18-24 ( ) 25-34 ( ) 35-44 ( ) 45-54 ( ) 55-64 ( ) 65 ve üstü ( )

2. **Cinsiyetiniz?**
   Kadın ( ) Erkek ( )

3. **Medeni durumunuz?**
   Bekar ( ) Evli ( ) Boşanmış ( )

4. **Eğitim durumunuz?**
   Lisans ( )
   Yüksek Lisans ( )
   Doktora ( )

5. **Yaşadığınız şehir/eyalet?**
   …….

6. **Hangi sektörde çalışmaktasınız?**
   Özel sektör ( ) Kamu sektörü ( ) Çalışmıyorum ( )

7. **Sosyal medya kullanıyor musunuz?**
   Evet ( ) Hayır ( )

8. **Sosyal medyayı ne zamandan beri kullanıyorsunuz?**
   1yıl ( ) 2 yıl ( ) 3 yıl ( ) 4 yıl ve üzeri ( )

9. **Aşağıdaki sosyal medya araçlarından hangilerini aktif olarak kullanıyorsunuz?** *(Birden fazla seçeneği işaretleyebilirsiniz)*
   Instagram ( )
   Facebook ( )
   X (Twitter) ( )
   WhatsApp ( )
   Telegram ( )
   TikTok ( )
   Mail.ru ( )
   LinkedIn ( )
   Diğer ( ) (lütfen adını yazın): ……

10. **Aktif olarak kullandığınız sosyal medya araçlarını, en çok kullandığınızdan en aza sıralama yaparsanız, en çok kullandığınız hangisidir?**
    Cevap: ……...

12. **Sosyal medyayı en çok hangi amaçla kullanıyorsunuz?**
    Gelişmelerden haberdar olma ( )
    Bilgi edinme ( )
    Eğlence ( )
    Boş vakit geçirme ( )
    Diğer ( ) (lütfen belirtin) …….

İSTANBUL TİCARET ÜNİVERSİTESİ
ETİK KURUL ONAYI ALMIŞTIR
Kurul Tarihi: 27.12.2024
Kurul Karar No: 12-12

13. **Aşağıdakilerden hangisini / hangilerini kişisel veri olarak görüyorsunuz?** *(Birden fazla seçeneği işaretleyebilirsiniz)*
    Kişisel kimlik bilgileri( )
    Açık adres ( )
    Kişisel fotoğraflar ( )
    Cep telefonu rehberi ( )
    Telefon numarası ( )
    Anlık konum bilgileri ( )
    İnternet alışveriş bilgileri ( )
    Gezinti yapılan web sitesi adresleri ( )
    Kişisel mesajlar ( )
    Diğer ( ) (lütfen belirtin): …….

14. **Günde internete bağlı olduğunuz zaman ortalama kaç saattir?**
    1 saat ( ) 2 saat ( ) 3saat ( ) 4 saat ve üzeri ( )

15. **İnternet ortamında kişisel verilerinizin güvende olduğunu düşünüyor musunuz?**
    ( ) Evet ( ) Hayır ( ) Fikrim yok

İSTANBUL TİCARET ÜNİVERSİTESİ
ETİK KURUL ONAYI ALMIŞTIR
Kurul Tarihi: 27.12.2024
Kurul Karar No: 12-12

GÖRÜŞME SORULARI

1. Size göre, mahremiyet ve sosyal medyada mahremiyet kavramı neyi ifade ediyor?
2. Size göre kişisel verilerin paylaşımı kişisel mahremiyeti ihlal ediyor mu, ediyorsa niçin?
3. Sosyal medya hesaplarında en çok ne tür içerikler paylaşıyorsunuz ve ne tür içeriklerle ilgili "Beğen" ve/veya "Paylaş" yapıyorsunuz?
4. Sosyal medyada gözetlendiğinizi düşünüyor musunuz?
5. Webte yaptığımız araştırmaların, paylaştığımız her türlü bilginin (kişisel bilgilerimiz, fotoğraf, görüşlerimiz vb.) depolanıp saklanmasının, insanlarının gözetlenmesine etkini nasıl değerlendirirsiniz?
6. İnternet ortamında kişisel verilerinin güvenliği ve başkalarının eline geçmemesi için önlem alıyor musunuz? Alıyorsanız bunlar ne tarz önlemlerdir?
7. Mobil cihazlara yüklediğiniz uygulamaların erişim izni isteklerini inceliyor musunuz?

İSTANBUL TİCARET ÜNİVERSİTESİ
ETİK KURUL ONAYI ALMIŞTIR
Kurul Tarihi: 27.12.2024
Kurul Karar No: 12-12

EK 3. Katılımcıların Kişisel Bilgilerinin Sınıflandırılması

Katılımcı No.	Kişisel Kimlik Bilgileri	Açık adres	Kişisel fotoğraflar	Cep telefonu rehberi	Telefon numarası	Anlık konum bilgileri	İnternet alışveriş bilgileri	Gezinti yapılan web sitesi adresleri	Kişisel mesajlar	Diğer
Katılımcı 1	✓				✓	✓		✓	✓	
Katılımcı 2	✓	✓			✓					
Katılımcı 3	✓		✓			✓			✓	
Katılımcı 4	✓	✓				✓	✓		✓	
Katılımcı 5									✓	
Katılımcı 6	✓	✓	✓	✓	✓	✓	✓	✓	✓	
Katılımcı 7	✓	✓	✓	✓		✓		✓	✓	
Katılımcı 8	✓	✓	✓			✓	✓			
Katılımcı 9	✓	✓			✓			✓	✓	
Katılımcı 10	✓				✓	✓				
Katılımcı 11	✓			✓						
Katılımcı 12	✓					✓			✓	
Katılımcı 13	✓	✓								
Katılımcı 14	✓	✓	✓			✓				
Katılımcı 15	✓								✓	
Katılımcı 16	✓					✓			✓	
Katılımcı 17			✓							
Katılımcı 18	✓	✓								
Katılımcı 19	✓			✓					✓	
Katılımcı 20	✓		✓	✓	✓	✓	✓	✓	✓	
Katılımcı 21	✓	✓	✓		✓	✓			✓	
Katılımcı 22	✓				✓		✓		✓	
Katılımcı 23	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Katılımcı 24	✓			✓	✓	✓				
Katılımcı 25	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Katılımcı 26	✓	✓	✓	✓	✓	✓	✓	✓	✓	
Katılımcı 27	✓						✓			
Katılımcı 28	✓	✓		✓	✓			✓	✓	
Katılımcı 29						✓	✓	✓	✓	
Katılımcı 30	✓					✓	✓	✓	✓	
Katılımcı 31	✓	✓				✓	✓		✓	
Katılımcı 32	✓	✓	✓	✓	✓	✓			✓	
Katılımcı 33	✓	✓	✓			✓	✓	✓	✓	
Katılımcı 34	✓	✓	✓	✓	✓			✓	✓	
Katılımcı 35	✓			✓					✓	
Katılımcı 36	✓									
Katılımcı 37	✓		✓		✓	✓		✓	✓	
Katılımcı 38	✓			✓	✓	✓	✓	✓	✓	✓
Katılımcı 39	✓	✓		✓	✓	✓				
Katılımcı 40	✓	✓	✓	✓	✓		✓		✓	
Katılımcı 41	✓	✓	✓	✓	✓	✓				
Katılımcı 42	✓	✓		✓					✓	
Katılımcı 43	✓	✓		✓		✓		✓	✓	
Katılımcı 44		✓		✓						
Katılımcı 45	✓	✓	✓	✓	✓	✓			✓	
Katılımcı 46	✓	✓	✓	✓	✓	✓	✓	✓	✓	
Katılımcı 47	✓	✓	✓	✓	✓	✓	✓	✓	✓	
Katılımcı 48	✓						✓			✓
Katılımcı 49	✓			✓						
Katılımcı 50	✓	✓				✓				
Katılımcı 51	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Katılımcı 52	✓	✓		✓	✓	✓			✓	
Katılımcı 53	✓	✓	✓							
Katılımcı 54	✓									
Katılımcı 55	✓	✓						✓	✓	

Katılımcı 56	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Katılımcı 57	✓	✓	✓		✓					
Katılımcı 58	✓	✓								
Katılımcı 59	✓	✓	✓	✓	✓	✓		✓	✓	
Katılımcı 60	✓	✓			✓	✓	✓		✓	
Katılımcı 61	✓	✓	✓	✓	✓	✓	✓	✓	✓	
Katılımcı 62	✓	✓	✓							
Katılımcı 63	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Katılımcı 64	✓	✓	✓	✓		✓				
Katılımcı 65	✓	✓	✓		✓	✓				
Katılımcı 66	✓	✓	✓			✓		✓	✓	
Katılımcı 67	✓									
Katılımcı 68	✓	✓	✓	✓	✓	✓	✓	✓	✓	