

Z Kuşağının Dijital Ortamlarda Gözetim Farkındalığını İncelemeye Yönelik Bir Araştırma



Muhammet Emin
SÖZKESEN*



Yusuf ŞAHİN**



Celalettin VATANDAŞ***

* Doktora Öğrencisi,
Süleyman Demirel Üniversitesi
d1840247014@ogr.sdu.edu.tr
ORCID: 0000-0002-0648-9498

** Doktora Öğrencisi,
Süleyman Demirel Üniversitesi,
d1840247012@ogr.sdu.edu.tr
ORCID: 0000-0002-3903-3366

*** Prof. Dr., Tekirdağ Namık Kemal
Üniversitesi,
cvatandas@nku.edu.tr
ORCID: 0000-0003-1431-3553

Gönderilme/ Received

18.10.2023

Kabul Tarihi/ Accepted

05.01.2024

Yayın Tarihi/Published

31.03.2024

Öz

Tarihsel süreçte siyasal ve ekonomik iktidarlar, varlıklarının devamını sağlamada gözetime büyük önem vermişlerdir. İktidarların büyük önem verdiği gözetim tekniklerinin, toplumları kontrol etme, disipline etme, verimliliği sağlama vb. gibi birtakım amaçlarla kullanıldığı görülmektedir. Günümüzde ise internet teknolojilerindeki gelişmeler ile gözetim, tarihsel süreçteki türlerinden farklılaşarak, bireylerin özel alanları da dahil tüm yaşamlarına şeffaf bir görünüm kazandırmıştır. Söz konusu dijital gözetim, geçmişteki örneklerinden daha yumuşak bir şekilde gerçekleştiğinden bireylerde tamamen özgür olduğu yanlışlaması oluşturmaktadır. Bu noktada, dijital teknolojilerin kullanımı sırasında söz konusu gözetim teknolojileri karşısında farkındalığa sahip olmak, bireyin mahremiyetini koruma konusunda daha hassas olmasını sağlamak açısından önem taşımaktadır. Bu araştırma, dijital ortamlardaki süperpanoptikon gözetim karşısında Z kuşağının farkındalık düzeyini ölçmeyi amaçlamaktadır. Nitel araştırma yöntemlerinden fenomenoloji (olgubilim) modeli kullanılmıştır. Araştırmada Isparta'da ikamet eden 9 Z kuşağı bireye kartopu örneklem ile ulaşılmış ve yarı yapılandırılmış görüşmeler gerçekleştirilmiştir. Elde edilen veriler yorumlayıcı fenomenolojik analiz aracılığıyla çözümlenmiştir.

Anahtar Kelimeler: İnternet, Süperpanoptikon Gözetim, Mahremiyet

* Bu çalışma için Süleyman Demirel Üniversitesi Etik Kurulundan E-87432956-050.99-393147 sayılı ve 16.11.2022 tarihli etik kurul onayı alınmıştır.

Ethics committee approval for this study was obtained from Süleyman Demirel University Ethics Committee with the number E-87432956-050.99-393147 and dated 16.11.2022.

*Bu makale intihal tespit yazılımlarıyla taranmıştır. Benzerlik tespit edilmemiştir.

This article has been scanned by plagiarism detection softwares. No similarity detected.

**Bu çalışmada "Yükseköğretim Kurumları Bilimsel Araştırma ve Yayın Etiği Yönergesi" kapsamında uyulması belirtilen kurallara uyulmuştur.

In this study, the rules stated in the "Higher Education Institutions Scientific Research and Publication Ethics Directive" were followed.

***Yazarların çalışmadaki katkı oranları eşittir.

Authors' contribution rates in the study are equal.

****Çalışma kapsamında herhangi bir kurum veya kişi ile çıkar çatışması bulunmamaktadır.

There is no conflict of interest with any institution or person within the scope of the study.

Kaynak gösterme / To cite this article: Sözkesen, M., E., & Şahin, Y., Vatandaş, C., (2024). Z Kuşağının Dijital Ortamlarda Gözetim Farkındalığını İncelemeye Yönelik Bir Araştırma. *İletişim ve Toplum Araştırmaları Dergisi*, 4(1), 41-66. doi: 10.59534/jcss.1378075



A Study to Examine the Surveillance Awareness of Generation Z in Digital Environments



Muhammet Emin
SÖZKESEN*



Yusuf ŞAHİN**



Celalettin VATANDAŞ***

* PhD Student,
Süleyman Demirel University
d1840247014@ogr.sdu.edu.tr
ORCID: 0000-0002-0648-9498

** PhD Student,
Süleyman Demirel University
d1840247012@ogr.sdu.edu.tr
ORCID: 0000-0002-3903-3366

*** Prof. Dr.,
Tekirdag Namık Kemal University,
cvatandas@nku.edu.tr
ORCID: 0000-0003-1431-3553

Gönderilme/ Received

18.10.2023

Kabul Tarihi/ Accepted

05.01.2024

Yayın Tarihi/Published

31.03.2024

Abstract

In the historical process, political and economic powers have given great importance to surveillance in ensuring the continuity of their existence. In the historical process, surveillance techniques, which the powers have given great importance, have been used to discipline societies, normalize, ensure efficiency, etc. seems to be used for a number of purposes. Today, with the developments in internet technologies, surveillance has differentiated from its types in the historical process and has given a transparent view to all lives of individuals, including their private areas. Since this digital surveillance takes place in a softer way than in the past, it creates the illusion that individuals are completely free. At this point, it is important to be aware of these surveillance technologies during the use of digital technologies, to ensure that the person is more sensitive about protecting their privacy. In this context, this research; it aims to measure the awareness level of Generation Z against Superpanopticon surveillance in digital environments. In this study, the phenomenology model, which is one of the qualitative research methods, was used. In the study, 9 Z generation individuals residing in Isparta were reached with snowball sampling and semi-structured interviews were conducted. The data obtained were analyzed through interpretive phenomenological analysis.

Keywords: Internet, Superpanopticon Surveillance, Privacy

Giriş

Tarihsel süreçte iktidarların “göz”lerini kitlelerin üzerine dikerek onları gözetleme, denetleme ve disipline etme eylemi her zaman bir iktidar pratiği olarak anlam kazanmıştır. Gözetim, temelde bir disiplin sağlama aracıdır. Başka bir deyişle; gözetim, gözetlenene dair bilgi elde etme ve bu yolla onların denetimini ve kontrolünü sağlama amacı taşımaktadır. Gözetim sürecinde, gözetleyen ile gözetlenen arasında iktidar ilişkisi üretilir veya var olan iktidar ilişkilerinin devamlılığı sağlanır (Göker, 2016, s. 973).

İnsanlık tarihinin tüm aşamalarında gözetleyen ile gözetlenen arasındaki iktidar ilişkisini sağlayan gözetim pratikleri ile karşılaşmak mümkündür (Alkan ve Özcan, 2019, s. 270). Bu gözetim pratikleri incelendiğinde; monarşik yönetim anlayışının benimsendiği ve yaygın olduğu dönemlerde, iktidarların bedensel şiddet aracılığı ile disiplini sağlamaya çalıştığı görülmektedir (Foucault, 1992). Aynı zamanda söz konusu dönemlerde ve hatta günümüzde dini kurumların da bireylerin davranışları üzerinde disipline edici bir güce sahip olduğu söylenebilir. Sonraki süreçte ulus devletlerin gelişimi ile gözetim pratiklerinin köklü bir dönüşüme uğradığı görülmektedir. Bu dönem ile, geçmiş dönemlerde bedensel şiddet şeklinde tezahür eden denetleme ve disiplini sağlama yöntemi, psikolojik şiddete evrilmiş; “devletin bürokratik gözetimi, kapitalizmin de teknik gözetim anlayışını benimsemesi” (Giddens, 2008), bireyi birer nesne haline getirmiştir.

Günümüzde ise toplum yapısı, bilgisayar ve internet teknolojilerindeki gelişmeler ile enformasyon toplumuna doğru evrilmiş, bu teknolojiler “gizlilik” ve “şeffaflık” kavramlarını iktidar ilişkileri özelinde tekrar düşünmeyi gerektirmiştir. Bireylerin tercihleri, düşünceleri, hareketleri, diğer bir ifade ile onlara dair her türlü bilgi, giderek “şeffaf bir hale gelirken” ağlar üzerinde yer alan iktidarların varlıkları da söz konusu teknolojiler ile tamamen “gizli” kalmaktadır (Dolgun, 2004, s.62). Dijital iletişim araçlarının gittikçe daha çok yer edindiği post-panoptikon çağda, iktidarlar tarafından söz konusu araçlar kullanılarak gizli bir şekilde gerçekleştirilen gözetim faaliyetlerinin, zaman zaman temel hak ve özgürlükleri de tehdit eder hale geldiği görülmüştür (Özdemir, 2020, s. 81).

Siyasi ve ekonomik iktidarlar tarafından gerçekleştirilen tüm dijital gözetim faaliyetlerini Mark Poster, “Süperpanoptikon” gözetim olarak tanımlamıştır. “Bu gözetim teknolojisi de tarihsel süreçteki diğer gözetim teknikleri ile aynı amaca sahiptir; denetlemek ve verimliliği sağlamak” (Schermer, 2007, s. 42). Süperpanoptikon gözetimde devletler, toplum güvenliğini tehdit eden bir durum olup-olmadığını sürekli olarak sanal devriyeler atarak denetlemektedirler (Bahar, 2020, s. 2763). Olası bir tehdit algılandığında ise IP (internet bağlantı adresi) ile bireyin adresine kolaylıkla ulaşılabilirerek gerekli müdahaleler yapılmaktadır. Bu tür haberler ile gerek geleneksel medyada gerekse sosyal medyada sıklıkla karşılaşmaktadır. Bu haberler bireyin sanal mecralarda hiç de başı boş olmadığını açıkça göstermektedir. Bireyler söz konusu haberler ile gözetlendiği hissini iliklerine kadar hissetmekte ve davranışlarını kontrol etme yoluna gitmektedirler. Siyasal iktidarlar tarafından bu ve benzeri amaçlarla gerçekleştirilen dijital gözetim faaliyetleri bazı gerekçelerle meşrulaştırılabilmektedir. Ancak bu iktidarların sıradan insanların yaşamlarını

içerisine alacak şekilde dijital gözetimi genişletmesi ciddi düzeyde olmak üzere mahremiyet ihlallerini ortaya çıkarabilmektedir. Siyasal iktidarın yanı sıra süperpanoptikon gözetim gerçekleştiren iktidar güçlerinden bir diğeri ekonomik iktidarlardır. “Ekonomik iktidarlar tüketimin disipline edilmesinde Süperpanoptikon gözetimi etkili kullanmaktadırlar. Bu iktidarlar, kullanıcıların internet üzerinde kendilerine dair arkalarında bıraktıkları veri izlerinden beslenerek onlara kişiselleştirilmiş reklamlar sunmaktadırlar.” (Zhu ve Chang, 2016, s. 442; Bauman ve Lyon, 2016, s. 12). Yani bu iktidarlar, bireylerin verilerini alınıp satılabilen bir meta haline getirmektedirler (Drakopoulou, 2017, s. 2). Özetle; gözetleyen konumunda yer alan siyasal ve ekonomik iktidarların (bu çalışmada siyasal iktidarlar tarafından gerçekleştirilen dijital gözetim faaliyetleri sıradan insanların yaşamlarını da içerisine alma ihtimali bağlamında ele alınıyor) gerçekleştirdiği süperpanoptikon gözetim faaliyetleri ile bireylerin kendilerine dair özel alanlarının tamamen ortadan kalkma ihtimali belirmiş, bu faaliyetlerin onların yaşamlarını şeffaf bir hale getirme yolunda hızla ilerlediği görülmektedir. Bu noktada bireylerin süperpanoptikon gözetim teknolojilerinin varlığının farkında olmak, ağlar üzerinde daha bilinçli birer kullanıcı olmaya katkı sağlayacaktır. Bu bağlamda söz konusu araştırmada; küçük yaşlardan itibaren internet teknolojileri ile tanışık olan ve dijital yerliler olarak da adlandırılan Z kuşağının, söz konusu süperpanoptikon gözetim teknolojileri karşısında ne düzeyde farkındalığa sahip olduğunu ortaya çıkarmak, araştırmanın temel problemini oluşturmaktadır. Öte taraftan bu araştırma, Z kuşağının dijital gözetim teknolojileri karşısındaki farkındalık düzeylerini ölçmeye çalışarak onların dijital eleştirel okuryazarlık düzeylerini ortaya çıkarması açısından önem taşımaktadır.

Dijital ağlarda yer almamanın yok sayılmakla eşdeğer olduğu günümüzde, bu ağlardan uzak bir yaşam sürmenin imkânı neredeyse yoktur. Bu teknolojiler insanların yaşamına önemli kolaylıklar sağladığı elbette tartışma kabul etmez bir gerçektir. Ancak söz konusu teknolojiler, bireylerin yaşamlarına bir takım önemli kolaylıklar sağlamakla birlikte birtakım olumsuzlukları da beraberinde getirmektedir. “İktidar mekanizmaları dijital ağlardaki dolaşımı tamamen özgür bırakmamakta, geçmişte toplumların karşılaştığı panoptikonvari gözetim teknikleri kadar katı bir şekilde olmasa da bireylerin tüm yaşamları en ince ayrıntısına kadar şeffaflaştırılabilmekte, denetleyebilmekte ve disipline edebilmektedir” (Önal ve Bendaş, 2017, s. 112). Bu bağlamda söz konusu araştırmanın temel amacı; iktidar mekanizmalarının dijital ağlarda gerçekleştirdiği süperpanoptikon gözetim karşısında Z kuşağının farkındalık düzeyini ortaya çıkarmaktır. Diğer taraftan bu araştırmanın sınırlılıkları arasında; belirli bir zaman diliminde ve tek bir kuşak üzerinden gerçekleştirilmiş olması gösterilebilir. Öte yandan söz konusu kuşağın dijital gözetim teknolojilerine karşı farkındalıklarının incelendiği bu araştırmada, nitel araştırma yöntemlerinden fenomenoloji (olgu) bilim modeli kullanılmıştır. Dolayısıyla güncel araştırmada örneklem gurubuna ulaşmada kartopu örneklem yöntemi kullanılmış ve Isparta’da ikamet eden Z kuşağı dokuz bireye bu şekilde ulaşılmış, yarı yapılandırılmış görüşmeler gerçekleştirilmiştir. Elde edilen veriler ise yorumlayıcı fenomenolojik analiz aracılığıyla çözümlenmiştir. Söz konusu evren/örneklem grubu bütçe kısıtlaması ve ulaşma kolaylığı sağlamasından dolayı Isparta olarak seçilmiştir.

1. Gözetim Kavramı

Fransızcada “bakarak olmak” manasına sahip surveiller fiilinden türetilen “gözetim”, boş bir merakın çok ötesinde, belirli insan davranışlarının dikkatle incelendiği bir sürece işaret eder. Bu kavram ilk olarak Gray T. Marx tarafından “*Gözetim Toplumu: 1984 Tarzı Tekniklerin Tehdidi*” adlı makalesinde kullanılmıştır (Timurturkan, 2010, s. 3). Gray söz konusu makalede gözetim kavramıyla bilgi teknolojilerinin toplumsal denetim önündeki engelleri kaldırdığını ifade etmiştir. David Lyon ise gözetimi, kişisel verileri toplanan ve işlenen bireyleri etkileme veya onları yönlendirme amacıyla girişilen çabalar bütünü olarak tanımlamıştır (Lyon, 2013, s. 30).

Gözetim, tarihsel süreçte, toplumsal ilişkilerin başladığı ilk dönemlerden bu zamana farklı gözetim teknikleri ile toplumlara denetim altında tutmanın bir yolu ve egemen güç olabilmenin önemli bir aracı olarak görülmüştür (Akdağ, 2015, s. 2). Egemen güç olabilmenin önemli bir aracı olarak görülen gözetim, eski dönemlerden bu zamana kadar, devlet kurumlarının nüfus sayımları başta olmak üzere çeşitli yollarla vatandaşları sürekli olarak gözetlemeye çalışmışlardır. Roma imparatorluğu gibi çok eski toplumlarda vergilendirme yapmak ve zorunlu askerlik hizmeti için nüfus sayımları yapıldığı görülmektedir (Lyon, 2013, s. 52). Nüfus sayımı ve benzeri yöntemlerle toplumlara denetlenebilir kılmaya çalışan iktidarlar için beden, disipline edilmesi gerekli olan bir nesneden başka bir şey değildir; egemen güçlerin gözü sürekli bir şekilde bu bedeni gözetlemekte, gözetlenen bedenlerin bilinçlerinde iktidarın bakışı içselleştirilmektedir. Toplumsal yaşamın bireylere tamamen özgür bir alan sunduğu bir yanılsamadan ibarettir. Toplumsal yaşam aslında, hapisane mantığının bir yansımasından başka bir şey değildir. Herkesin belli kurallar ekseninde, davranışlarının nedenini sorgulamadan hareket ettiği bir toplumsal yaşam, bireylerin bir nesne haline getirildiği, diğer bir ifade ile yok edildiği bir duruma göndermede bulunur (Çoban, 2019, s. 119).

Bedenin iktidarın denetimi ile nesneleştirildiği süreci Foucault, tarihsel süreç üzerinden incelemiştir. Foucault’ya göre 18. yüzyıl da dahil olmak üzere bu zamana kadar ki sürede insanların bedeni işkence ve cezalarla disipline edilmeye çalışılmıştır. 19. yüzyıldan itibaren ise egemen güçlerin toplumsal bedene karşı yaklaşımı değişmiştir; Bedenin fiziksel şiddetle disipline edilmesi anlayışından uzaklaşmış, ıslah edilmesi, düzeltilmesi, yetenek kazanması, çalışabilir bir beden olma niteliğinin kazandırılması gereken bir şey olarak görülmüştür (2015, s. 249). Çünkü, sanayileşme ile ekonomik iktidarın varlığının devamlılığını sağlamak için bedeni öldürmek değil, yaşatmak gerekmektedir (Foucault, 2007, s. 102-103). Bından dolayı da bedenin gözetimi ve denetimi kapitalist sermaye sahipleri için olmazsa olmaz bir durum olarak görülmüştür (Foucault, 2014, s. 147). Bahsi geçen kapitalist sermaye sahipleri, gözetim teknikleri aracılığıyla bedenin verimliliğini maksimum düzeyde çıkarmak için Frederick Winslow Taylor’ın bilimsel yönetim ilkesi anlayışını benimsemişlerdir. Taylor’ın bilimsel yönetim ilkesine göre verimlilik için üretim süreci en basit aşamalara ayrılırken, emeğin sahiplerinin kişilikleri yok sayılıyor, sürekli gözetime maruz kalan bir üretim sürecinde, yaratıcılık tamamen ortadan kalkıyordu. Böylelikle disiplini sağlanmış mekanik bir işçi ordusu ortaya çıkarılması amaçlanmıştı (Dolgun, 2015, s. 95).

Diğer taraftan, Karl Marx ise gözetimi, kapitalist işletmelerde gerçekleşen emek ve sermaye çelişkisi üzerinden incelemiştir. Marx'a göre gözetim, fabrikada çalışan işçilerin sermaye adına idari denetimin sürdürülmesinin bir aracı olarak ele alınmalıdır (Lyon, 2012, s. 20). Öte yandan gözetimi sadece fabrikayla sınırlandırmayıp modern örgütleri de kapsayacak bir bütünsellik içerisinde ele alarak dikkatleri üzerine çeken bir diğer kuramcı Max Weber'dir. Weber, kapitalist işletmelerde gözetimin oynadığı rolü tamamen görmezden gelmemekle birlikte, yalnızca sınıf ilişkileri ile sınırlandırılmasına karşı çıkarak, onu çok daha geniş bir alan üzerinden değerlendirmiştir. Bu bağlamda toplum, modern örgütler ile devlet kurumlarındaki yöneticilerin, toplumu fişlemeye yönelik dosyalar oluşturması paralelinde, kişisel verileri saklama tekniklerini ve söz konusu bu verileri çağırma araçlarını geliştirmiş oldukları bir tekniği ifade eden bürokrasi ile çevrilidir. Marx'ın kuramının merkezi konumunda yer bulan kapitalist işletmeler ise bürokrasinin yalnızca bir alt türü olarak düşünülür (Dolgun, 2015, s. 98-99). Diğer bir ifade ile Weber gözetimi, tüm toplumsal yapı üzerinden değerlendirmiştir. Yani, ulus devletler içerisinde yer alan bürokratik örgütler, insanların gündelik yaşamlarında eskiden olduğundan daha fazla yer tutarak, onları dünyaya gözlerini açtıkları andan öldükleri ana kadar sürekli kayıt altına alırlar. Yaşamın her karesi bürokratik örgütlerin gözetimi ile devam eder: Hastanedeki doğum kayıtlarından başlanarak, okullarda davranışların ve ders notlarının kaydedildiği dosyalar, iş yaşamı içerisinde bireye dair tutulan raporlar, vergi dairelerindeki ve sosyal güvenlik kurumlarındaki kayıtlar, sahip olunan mülklerin dokümanları, elektrik-doğalgaz-telefon-su idaresi ve askerlik şubesindeki kayıtlar, iyi bir vatandaş olup olmadığının takibe alınması vs. (Dolgun, 2015, s. 101).

Görüldüğü üzere, günümüze kadar iktidarlar tarafından gerçekleştirilen gözetim faaliyetlerinin panoptikon gözetim tarzında katı bir yapıya sahip olduğu söylenebilir. “Günümüzde ise bilgisayar ve internet teknolojilerinin katı gözetim anlayışını akışkan bir yapıya kavuşturduğu görülmektedir” (Bauman ve Lyon, 2016). “Panoptikon gözetim tekniğinde, gözetlenende gözetleniyor olma hissini oluşturmak esas iken” (Foucault, 1992, s. 253), dijital ağlar üzerinden iktidarlar tarafından gerçekleştirilen gözetim daha yumuşak bir şekilde gerçekleştirildiğinden, birey eğer dijital gözetim teknolojileri konusunda bir farkındalığa sahip değilse gözetlendiğini hissetmemektedir. Bu ağlar, kullanıcılarına özgür bir ortam sunduğu vaadinde bulunur ancak, ekonomik ve siyasal iktidarlar, söz konusu teknolojiler ile bireylerin en özel alanlarını dahi şeffaflaştırabilmektedir. Kullanıcıların dijital ağlar üzerinde kendilerine dair bıraktıkları devasa veri kırıntıları bu ağları kullanmanın en büyük bedelidir.

Bireyler kendilerine dair arkalarında bıraktıkları devasa veri kırıntıları ile internet üzerinde kullandıkları hizmetlerin ücretini ödemektedirler. Yani bu hizmetlerin bedelini bireyler meta haline gelmiş verileri ile ödemektedirler. İnternet üzerinde gerçekleştirilen aramaların özgür bir şekilde gerçekleştiği söylenemez: her internet araması, bireye dair kişisel bilgileri de karşı tarafa aktarmaktadır (Işıklı, 2014). İnternet arama motoru aracılığı ile aranan her kavram bireye dair pek çok şeyi ifşa etmektedir. Bireyin sahip olduğu hastalıklar, satın alma niyetleri, maddi sıkıntıları, boş zaman etkinlikleri, seyahat planlamaları vb. gibi Google arama motoru bireylere dair bu bilgiler ile her yıl

devasa miktarlarda para kazanmaktadır (Aust ve Ammann, 2019, s. 191). Özetle dijital teknolojilerin insan yaşamında vazgeçilmez bir yer edindiği günümüzde özel olarak düşünülen bedenler, birer gözetleme verisi haline gelmiştir (Lyon, 2006, s. 37).

2.Dijital Çağda Gözetimin Değişen Yüzü Olarak Süperpanoptikon Gözetim

Günümüzde dijital iletişim teknolojilerinde yaşanan hızlı gelişmelerle birlikte, gündelik yaşamın dinamikleri de dönüşüm yaşamakta “enformasyon toplumu” olarak ifade edilen halihazırdaki toplum yapısının “gözetim toplumuna” doğru dönüşüm yaşadığı görülmektedir. Sanayi devriminde buharlı makinelerin neden olduğu sosyo-ekonomik dönüşümün benzerine, günümüzde çok daha sarsıcı bir şekilde enformasyon teknolojilerinde yaşanan gelişmeler neden olmakta ve “bilgi parmaklarınızın ucunda” sloganı ile yeni bir dönem başlamaktadır. Bundan böyle gündelik yaşam içerisindeki her şey -ekonomi, eğitim, toplumsal ve idari hizmetler, cemaatleşme, çalışma hayatı vs. gibi- dijital ortamlara taşınmakta, bireyler internete giriş yaptıkları anda ucu bucağı olmayan bir dünyaya yelken açmaktadırlar (Dolgun, 2004, s. 55). Bireylerin ucu bucağı olmayan bir dünyaya yelken açmasını sağlayan internet teknolojileri, iktidarların geleneksel gözetim yöntemlerinin de dönüşüme uğramasına neden olmuştur (Bozkurt, 2000, s. 75-81).

Bu dönüşüm, geleneksel bir gözetim tekniği olan panoptikon gözetimin, iktidarlar tarafından siber mekânlar üzerine uyarlanması şeklinde gerçekleşmektedir. Mark Poster söz konusu bu dijital gözetim tekniğinden elektronik veri tabanları üzerine yazmış olduğu denemede bahseder. Poster denemesinde bireylerin bedenlerinin enformasyon koridorları, veri tabanları içerisine çekildiğinden bahseder ve bireye dair enformasyon depolayan bu yerler, bireye gözetlenmekten kaçabileceği veya etrafına direniş hattı çekebileceği bir sığınak sağlamamaktadır. Bireyin kredi kartı kullanımları ve satın alma eylemleri ile çoğalan devasa miktarlardaki veri, Mark Poster’a göre süperpanoptikon gözetimle sonuçlanır. Süperpanoptikon gözetimin panoptikon gözetimden tek farkı, iktidara veri sağlayan gözetim altındaki bireylerin, gözetimin gönüllüleri olmalarıdır (Bauman, 2010, s. 55). Gözetimin gönüllüleri olan bireyler şeffaf bir hapisane içerisinde olduklarının farkına varmadan özgür bir ortam yanılsaması içerisinde varlıklarını sürdürürler (Çelik, 2014, s. 123). Özgür bir ortam yanılsaması sunan ağlar üzerindeki süperpanoptikon gözetim ile iktidar, toplumsal yaşamın her alanına yayılmıştır. Bu şekilde sınırlı bir alanın gözetiminden çıkarak her yere erişebilen ve bireye dair her veriyi kullanma olanağına sahip olan bir iktidar gözü ortaya çıkmıştır (Hidroğlu, 2019, s. 1415). İktidarın gözüne heryerdelik kazandıran süperpanoptikon gözetim teknolojileri, yalnızca siyasi iktidarlar tarafından yurttaşların denetimini sağlamak için kullanılmamakta, aynı zamanda ticari gözetim amacıyla da ekonomik iktidarlar tarafından kullanılmaktadır. Bireylerin dijital ağlar üzerinde kendilerine dair arkalarında bırakmış olduğu veri kırıntıları ekonomik iktidarlar için meta değeri taşımaktadır. Kullanıcıların ağlar üzerinde bıraktığı bu veriler ekonomik iktidarlar tarafından yine bireyin aleyhine kullanılmakta kişiselleştirilmiş reklamlar ile satın alma davranışları şekillendirilmeye çalışılmaktadır. Lyon’a

göre ekonomik iktidarlar için bu veriler, rakipler ile rekabet avantajı sağlamada önemli olduğundan hırsla ele geçirilmeye çalışılmaktadır (2012, s. 69).

Bu bağlamda, bireylere ait verilerin siyasal ve ekonomik iktidarlar ve istihbarat servisleri tarafından bilgi bankalarında işlenerek gözetim pratiklerine hazır bir şekilde saklanması hız kazanırken, bireylerin özgürlükleri ile mahremiyet alanları tamamıyla ortadan kalkmaya başlamıştır (Dolgun, 2015, s. 16). Bireylerin özgürlükleri ve mahremiyetleri üzerinde önemli bir tehdit olarak görülen gözetim teknolojileri konusunda farkındalık sahibi olmak, bireyin bu konularda daha hassas olmasına katkı sağlayacaktır.

3.Dijital Çağda Süperpanoptikon Gözetim Teknolojileri Karşısında Farkındalık Kazanmanın Önemi

Günümüzde dijital iletişim teknolojilerinde yaşanan gelişmeler bireylerin yaşamlarını tamamen dönüşüme uğratmıştır. Bireyler gündelik yaşamlarının büyük bölümünü dijital ağlar üzerinde sürdürmektedir. Özellikle söz konusu dijital ağları, dijital yerlilerin yaşamlarının her alanında etkili olarak kullandığı görülmektedir. Dijital teknolojileri kullanma konusunda bilgi ve deneyim eksikliği olan dijital göçmenler ise bu teknolojilerden olabildiğinde uzak kalmaktaydı. Ancak geçmiş yıllarda bütün dünyayı etkisi altına alan Covid 19 salgını ile bu teknolojilerin toplumun tüm kesimleri için ne kadar önemli olduğu herkes tarafından anlaşılmıştır. Devletler tarafından salgının önlenmesi için tam kapanmaların yapıldığı dönemlerde bireyler dünya ile iletişimini dijital ağlar üzerinden sürdürmek durumunda kaldılar. Ağlarda yer almayanlar ise yok sayılmakla tehdit edildiler. Kısaca salgın ile tüm toplumların dijital iletişim teknolojilerine adaptasyonu sağlanmış oldu. “Ancak teknolojinin bireylerin yaşamına birtakım kolaylıklar sağladığı inkâr edilmemekle birlikte, bu teknolojilerin ardındaki iktidar mekanizmalarını da gözden kaçırmamak gerekmektedir. Tarihsel süreçte de görüldüğü üzere bütün iletişim araçları ekonomik ve siyasal iktidarların denetimi altında olmuştur. Dijital ağların bu güçlerden bağımsız, bireylere özgür bir alan sunduğu düşünceleri bir yanılısamadan başka bir şey değildir” (Marx, 1996).

Söz konusu egemen güçler “tarihsel süreçte olduğu gibi” (Foucault, 2015, s. 245-246) günümüzde de dijital ağlar üzerinden toplumlara gözetlemekte, denetlemekte ve disipline etmektedir. Ancak ağlardaki gözetim, geçmişteki örneklerinden daha yumuşak bir şekilde gerçekleştirilmektedir. Bireyler doğrudan iktidarın gözü ile karşı karşıya gelmemektedir. Bu da bireyin kendisini ağlar üzerinde rahat hissetmesini sağlamaktadır. Ağlar üzerinde kendini rahat hissetmesi sağlanan bireyler, arkalarında kendilerine dair devasa miktarlarda veri kırıntıları bırakırlar. Bireyin kendisine dair arkasında bıraktığı bu verileri ile dijital bir kimliği oluşturulur. Bu dijital kimlik, bireye dair birçok veriyi barındırır (Alay & Deveciyan, 2023, s. 1446). Söz konusu bu veriler bireyin potansiyel sağlık sorunları, satın alma niyetleri, suça meyletme durumu vb. gibi birtakım bilgileri içerebilir. Bu şekilde ekonomik ve siyasal iktidarlar bireylere dair birtakım profiller oluşturarak toplumlara daha denetlenebilir bir hale getirebilirler.

Elbette potansiyel suçluları tespit ederek bunlara karşı birtakım tedbirler almak, suç eyleminin gerçekleşmeden önlenmesi adına önemli bir durumdur.

Dijital ağlarda güvenliği sağlamak için egemen güçler tarafından alınan buna benzer birtakım önlemler kabul edilebilir olmakla beraber, bu gözetim faaliyetleri amacı dışında kullanıldığında bireysel mahremiyet ihlalleri ile sonuçlanabilmektedir. Bu mahremiyet ihlallerini daha çok ekonomik iktidarlar tarafından gerçekleştirilen gözetim faaliyetlerinde görmek mümkündür. Bireylerin gündelik yaşamlarında sıklıkla kullandıkları Facebook, Instagram vb. dijital platformlar, ekonomik iktidarların ticari işletmelerinden bazılarıdır. Ücretsiz bir şekilde insanlara hizmet sundukları söylemi ile ön plana çıkan bu platformlar, bireylerin verilerini süperpanoptikon gözetime tabii tutarak reklam verenlere birer veri olarak pazarlamaktadırlar (bakınız: Facebook Veri İlkesi). Bireyler bu tür platformlara üye olurken, üyelik sözleşmesinde şirketler bu tür verilerin reklam verenler ile farklı şekillerde paylaşılabilmesine dair birtakım maddelere yer vermektedirler. Ancak çoğu kullanıcı bu platformlara üye olurken genellikle sözleşmeyi okumadan üyeliklerini gerçekleştirmektedirler. Bireylerin “saklayacak bir şeyim yok” söylemi ile sözleşmeleri onaylayarak, verilerini bu platformlarla paylaşmasının ilerleyen zamanlarda ne tür tehditler oluşturacağını kestirmek zor değildir. Bu tehditlerin en zararsızlarından biri bireylerin karşısına kişiselleştirilmiş reklamlar olarak çıkmaktadır. Platformlar bireye dair birtakım verileri toplayarak, onlara kişiselleştirilmiş reklamlar sunarak, satın alma olasılıklarını arttırmaktadır. Facebook vb. platformlar bunu sıklıkla kullanılmaktadır. Facebook görüldüğü üzere “ücretsizdir her zaman da ücretsiz kalacak” vaadi boş bir söylemden ibarettir. Son zamanlarda şirketin adını meta olarak değiştirmesi ise kimsenin dikkatini çekmemiş gibi görünmektedir. Tüm bunlar ise bireyin mahremiyet kaybı ile sonuçlanmaktadır.

Diğer taraftan bireylerin gündelik yaşamının ayrılmaz parçası haline gelen internet bağlantılı akıllı telefonlar, bireysel mahremiyetin en büyük düşmanı olarak değerlendirilebilir. Bireylerin telefonlarına yükledikleri her uygulama risklerle doludur. Bu uygulamalara verilen izinler bireyin kendi elleri ile mahremiyetini yok etmesi ile sonuçlanabilmektedir. Bireyler için faydalı olarak görülen bazı uygulamaların içerisinde ise casus yazılımlar bulunması her zaman için mümkündür. Bu tür uygulamalar verilen izinlere bağlı kalmadan telefonun galerisi ulaşarak en mahrem fotoğraflara ya da kameraya erişerek bireyin özel yaşamını dikizleyebilmektedir. Bu tür veriler birey için bir şantaj olarak kullanılabilir (Cooper, 2015).

Öte yandan birçok işletim sistemi gibi, Android işletim sistemi de mahremiyet konusunda birtakım sorunlar ile gündeme gelmektedir. Örneğin bireyler, kullanmış oldukları Android bir telefonu satmaya kalktıklarında, galerisindeki fotoğrafları ve diğer her türlü kişisel veriyi doğal olarak silmektedir. Ancak bu telefonlardan verileri silmek, tam anlamıyla silindiği anlamına gelmemektedir. Bu veriler silinse bile, küçük byteler halinde telefon hafızasında varlıklarını sürdürmekte ve birçoğu kolaylıkla geri döndürülebilmektedirler (Karaaslan, Demir ve Fetah, 2016). Bir antivirüs yazılımı olan Avast’ın gerçekleştirdiği bir araştırmada, 20 kullanıcının verilerini sildiğini düşünerek sattığı Android telefonlarından, basit programlar ile binlerce mahrem veriye ulaşılması, bu durumu ispatlar niteliktedir (bakınız: Avast). Fotoğraf vb. verileri çağırma programlarına hâkim olan art niyetli kişiler, bireylerin bu mahrem verilerine ulaşarak şantaj vb. amaçlarla kullanabilmektedirler. Diğer taraftan,

Android telefonların risklerini ortaya koyan bir başka araştırma İskoçya'daki Edinburgh ve İrlanda'daki Dublin College Üniversitelerinin ortak çalışması ile gerçekleştirilmiştir. Bu çalışmada Android işletim sistemi ile çalışan akıllı cep telefonlarının kullanıcıların izni olmadan kişisel veri paylaşımı yaptığı ortaya çıkarılmıştır (Leith, Patras ve Liu, 2021). iPhone telefonlarda kullanılan iOS yazılım bireylere bu süperpanoptikon gözetim ve mahremiyet konusunda önemli avantajlar sağlıyor görünmektedir. iPhone telefonlarda silinen fotoğraf ya da videolar hiçbir şekilde geri çağrılmadığı ifade edilmektedir (bakınız: Apple). Aynı zamanda bu telefonlarda, uygulamaların bireylerin ne tür verilerini topladığına dair ayrıca bilgilendirme bölümü vardır. Bireyler bu bölümde hangi uygulamanın ne tür verileri kullanabileceğine kendisi izin vermektedir. Bu bağlamda iPhone telefonlar diğer telefonlara göre bireyin süperpanoptikon gözetimi ve mahremiyeti konusunda daha hassas bir tutuma sahip olduğu izlenimi oluşturmaktadır. Ancak, az önce de bahsedildiği üzere dijital ağlar ve bu ağları kullanmaya olanak sağlayan akıllı cihazların süperpanoptikon gözetim ve mahremiyet kaybı noktasında güvenilirliği sorgulanmalıdır. Bu noktada, dijital ağlardaki süperpanoptikon gözetim teknolojileri konusunda yeterli bilgi donanımına sahip olmak, bireyin mahremiyetini koruma konusunda daha hassas olmasını ve gerekli önlemleri almalarını sağlayacaktır.

4.Yöntem

4.1.Araştırma Modeli

Araştırmada bireylerin Süperpanoptikon gözetim teknolojileri karşısındaki farkındalık düzeylerini ortaya çıkarmak için nitel araştırma yöntemlerinden fenomenoloji (olgubilim) modeli kullanılacaktır. Fenomenoloji, bireylerin belirli bir fenomen ile ilgili bakış açılarını, algılarını ve duygularını ifade etmelerine yardımcı olan ve bu fenomeni ne şekilde deneyimlediklerini anlamak için kullanılan nitel araştırma yöntemlerinden biridir (Rose, Beeby ve Parker, 1995).

4.2.Çalışma Grubu

Katılımcılar belirlenirken kartopu örneklem tekniğinden faydalanılmıştır. Kartopu örneklem tekniğinde araştırmanın konusu ile ilgili bir kişi belirlenmekte ve bu kişi vasıtası ile diğer kişilere ulaşılmaktadır (Biernacki ve Waldorf, 1981). Bu tekniğe uygun bir şekilde Isparta'da ikamet eden ve interneti aktif olarak kullanan Z kuşağı mensubu bir bireye ulaşılmıştır. Katılımcı araştırma konusunda bilgilendirilmiş ve çevresinde aynı kuşağa mensup olan ve interneti aktif olarak kullanan kişileri davet etmesi ricasında bulunulmuştur. Bu şekilde dokuz kişiye ulaşılmıştır. Çalışmaya katılanların 4'ü erkek 5'i kadındır. Katılımcılar ile yarı yapılandırılmış derinlemesine görüşmeler 28-30 Mayıs 2023 tarihleri arasında gerçekleştirilmiştir.

4.3.Veritoplama Aracı ve Süreci

Araştırmada veri toplama aracı olarak yarı yapılandırılmış derinlemesine görüşme formu kullanılmıştır. Görüşme formundaki sorular katılımcıların süperpanoptikon gözetim teknolojileri konusunda farkındalık düzeylerini ortaya çıkarmaya yönelik olarak oluşturulmuştur. Soruların oluşturulması sürecinde konuya dair literatürden ve uzman görüşlerinden faydalanılmıştır. Katılımcılar ile görüşmeler yüzyüze gerçekleştirilmiştir. Katılımcılara araştırmanın amacına

uygun olarak 13 soru yöneltmiştir. Her bir katılımcı ile görüşmeler ortalama 30 dakika sürmüştür. Araştırmanın bulgular bölümünde, katılımcıların sorulara verdikleri yanıtların doğrudan sunumları gerçekleştirilirken, katılımcıların adları kodlanarak verilmiştir.

Bu çalışma için Süleyman Demirel Üniversitesi Etik Kurulundan E-87432956-050.99-393147 sayılı ve 16.11.2022 tarihli etik kurul onayı alınmıştır.

4.4.Verilerin Analizi

Araştırmada elde edilen verilerin analizi yorumlayıcı fenomenolojik analiz yöntemi aracılığı ile çözümlenmiştir. Yorumlayıcı fenomenolojik analiz, bireylerin bir olguyu nasıl algıladıklarına odaklanır (Smith ve Osborn, 2004). Yorumlayıcı fenomenolojik analiz, dil ile insanların düşünce ve duyguları arasında sıkı bir bağlantının olduğu düşüncesinden hareketle onların söylediklerine odaklanır ve yorumlamaya çalışır. Verilerin analizi sürecinde, veriler belirli gruplandırmalar altında temalara ayrılır, daha sonra ise bu veriler, temalar altında tartışılıp yorumlanır (Smith ve Eatough, 2007). Bu bağlamda araştırmanın amacına uygun olarak veriler belirli gruplandırmalar altında temalara ayrılmıştır. Aynı soruya verilen yanıtlar oluşturulan temalar dikkate alınarak tek bir Word dosyasında bir araya getirilmiş ve kapsayıcı, bütünsel bir değerlendirmede bulunulmaya çalışılmıştır. Araştırmada katılımcıların doğrudan ifadelerine yer verilirken kişisel verileri gizli tutulmuş ve K1, K2, K3 şeklinde kodlanmıştır.

5.Bulgular ve Yorum

5.1. Katılımcıların Demografik Bilgileri

Tablo 1. Katılımcıların Cinsiyet ve Yaş Bilgileri

Katılımcıların Kod Adları	Cinsiyet	Yaş
K1	Erkek	22
K2	Erkek	23
K3	Kadın	19
K4	Kadın	19
K5	Kadın	22
K6	Erkek	23
K7	Kadın	23
K8	Erkek	21
K9	Kadın	23

Araştırmaya katılan bireylerin yaş ve cinsiyete dair bilgileri Tablo 1. üzerinden incelendiğinde, katılımcıların 4'ü erkek 5'i kadındır. Katılımcıların yaşlarının ise 19-23 yaş aralığında değiştiği görülmektedir.

Tablo 2. Katılımcıların Eğitim Düzeyleri

Katılımcıların	Eğitim
----------------	--------

Kod Adları	Düzeyi
K1	Lisans
K2	Lisans
K3	Lise
K4	Lise
K5	Lisans
K6	Lisans
K7	Ön Lisans
K8	Lisans
K9	Lisans

Araştırmaya katılan bireylerin eğitim düzeyleri Tablo 2. üzerinden incelendiğinde, katılımcıların 6'sının Lisans, 1'inin Ön Lisans ve 2'sinin Lise eğitim düzeyine sahip olduğu görülmektedir.

5.2. Katılımcıların İnternet Kullanım Sıklığı ve Kullanım Amaçları

Tablo 3. Katılımcıların İnternet Kullanım Sıklıkları

Katılımcıların Kod Adları	İnternet Kullanım Sıklığı
K1	7-8 saat
K2	5-6 saat
K3	5-6 saat
K4	5-6 saat
K5	6-7 saat
K6	4-5 saat
K7	3-4 saat
K8	5-6 saat
K9	7-8 saat

Katılımcıların internet kullanım sıklığı Tablo 3. üzerinden incelendiğinde, katılımcıların büyük bir bölümünün interneti 5 saat üzerinde kullandıkları görülmektedir. Bu verilerden hareketle katılımcıların interneti gündelik yaşamlarında aktif olarak kullandıkları değerlendirilebilir.

Tablo 4. Katılımcıların İnternet Kullanım Amaçları

Katılımcıların Kod Adları	İnternet Kullanım Amaçları
K1	Okul içerisinde genellikle işime odaklı kullanırken yaz ve tatillerde sosyal medya ağırlıklı kullanıyorum

K2	Sosyal medya hesaplarımı kullanmak için ve haberleri takip etmek için
K3	Genellikle sosyal medyaya bakmak, dizi izlemek için kullanırım fakat bir konuda araştırma yapmak, bilgi edinmek için de sık sık kullanırım.
K4	İnterneti genellikle ders çalışmak, dizi film izlemek ve müzik dinlemek için kullanırım. Hayatımın büyük çoğunluğunda internet var.
K5	Bilgi edinme, haberleşme, gelişmeleri takip etme, eğitim, sosyal medya, alışveriş yapmak.
K6	İnterneti bilgi aramak, araştırma yapmak, sosyal medya hesaplarımı takip etmek ve arkadaşlarım ile iletişime geçmek için kullanırım.
K7	Zamanımı verimli geçirmek için, araştırma yapmak için ve bazen eğlenmek için internet kullanıyorum.
K8	Haber ve bilgi almak için.
K9	Araştırma ve iletişim için.

Katılımcıların interneti hangi amaçla kullandığına dair bulgular Tablo 4. üzerinden incelendiğinde, katılımcıların büyük bir bölümünün interneti bilgi aramak ve eğlenmek için kullandığı anlaşılmaktadır.

5.3. Katılımcıların İnternet Üzerinde Kişisel Veri Olarak Gördüğü Bilgileri

Tablo 5. Katılımcıların Kişisel Veri Olarak Gördüğü Bilgiler

Katılımcıların Kod Adları	Katılımcıların Kişisel Veri Olarak Gördüğü Bilgiler
K1	Söylenen tüm bilgileri kişisel veri olarak görüyorum. Bu nedenle gerekmedikçe istenmemesi gerektiğini düşünüyorum. Bazılarının ise hiç istenmemesi gerektiğini düşünüyorum. Bunların başında banka bilgileri ve telefon rehberi fotoğraf kimlik bilgileri vb. geliyor.
K2	Cep telefonu rehberi, banka kartı bilgileri, açık adres, konum, telefon numarası.
K3	Telefon rehberim, banka kartı bilgilerim, açık adres, anlık konum bilgileri, fotoğraflar.
K4	Benim için bu sorunun cevabı kesinlikle telefon numarası, banka kartı bilgileri, açık adres, anlık konum bilgileri, fotoğraflardır. Çünkü bu bilgiler herkese verilebilecek bilgiler değildir. Özel tutulması gerekir ya da çok güvenilir sitelere, kişilere verilebilir.
K5	Kişisel verilerin güvenliği konusunda endişelerim bulunmakla birlikte çok uzun yıllardır internet

	kullanmama rağmen bir sorunla, şüphemi artıracak bir durumla karşılaşmadığımı belirtmek isterim.
K6	Telefon numarası, cep telefonu rehberi, banka kartı bilgileri, açık adres, fotoğraflar, ziyaret edilen siteler, mesajlaşmalar, sosyal medya arkadaş listesi, medeni durum gibi daha birçok şey sayılabilir.
K7	Konum bilgisi ve fotoğraf.
K8	Yaş, telefon numarası, anlık konum bilgileri.
K9	Cep telefonu numarası, banka kart bilgileri, fotoğraflar, açık adres, anlık konum bilgileri.

Katılımcıların internet üzerinde kişisel veri olarak gördüğü bilgiler Tablo 5. üzerinden incelendiğinde katılımcılar için banka kartı bilgileri (6 katılımcı), cep telefonu rehberi (4 katılımcı), telefon numarası (5 katılımcı), anlık konum bilgileri (6 katılımcı), fotoğraflar (6 katılımcı), açık adres (5 katılımcı), gezilen internet siteleri (2 katılımcı), kimlik bilgileri (1 katılımcı), her tür veri (1 katılımcı) vb. bilgiler kişisel veri olarak değerlendirilmektedir.

5.4. Dijital Ortamlarda Gözetim Farkındalığı ve Kullanıcıların Dijital Gözetime Yönelik Olarak Aldığı Tedbirler

5.4.1. Dijital Ağlarda Gözetim Farkındalığı

Gözetim günümüzde tarihteki uygulamalarından çok farklı bir şekilde işlemektedir. İktidarlar geçmişteki doğrudan gözetim uygulamalarını bırakmış, daha yumuşak bir gözetim tekniğine geçiş yapmışlardır. İktidarların bu yeni gözetim tekniği bireyleri eskisi gibi rahatsız etmemektedir. Bireyler bu şekilde internet üzerinde özgür bir ortam yanılması içerisinde varlıklarını sürdürmektedirler. Bireyler bu özgürlük yanılması içerisinde iktidarlar tarafından denetlenmekte ve disipline edilmektedir. Örneğin siyasal iktidarlar bireylerin internet üzerindeki eylemlerini denetime tabii tutarak toplumsal düzeni sağlamaya çalışabilmektedir. Toplumsal düzeni sağlama sürecinde internet üzerinde suç sayılacak eylemlerin kontrol edilip gerekli cezalandırılmaların sağlanması elbette önemlidir. Bu denetim eylemi baskıcı bir tutumda ve sıradan suçsuz insanların mahremiyet alanını ihlâl edecek düzeye gelmediği sürece kabul edilebilirdir. Diğer taraftan internet üzerinde dev şirketler haline gelmiş olan Facebook (yeni adı ile Meta), Google gibi şirketler yalnızca kamusal yarar ilkesini temel alarak ortaya çıkmış kuruluşlar değildir. Bu şirketleri ayakta tutan şey bireyin metalaştırılmış verileridir. Bireyin verileri bireye yönelik olarak kullanılarak onların satın alma eylemleri disipline edilmeye çalışılmaktadır. Öte yandan birey bir de internet üzerinde verilerini hacklere karşı korumak zorundadır. Bireyin internet üzerinde bu ve buna benzer gözetim teknolojilerine karşı farkındalık kazanması mahremiyetini koruması adına önem taşımaktadır. Bu bağlamda araştırma kapsamında Z kuşağı mensubu bireylerin dijital gözetim farkındalık düzeylerini ortaya çıkarmak için yarı yapılandırılmış form eşliğinde olmak üzere görüşme sırasında şu sorular yöneltilmiştir:

1-İnternet üzerinde kişisel verilerinizin güvenliği konusundaki düşünceleriniz nelerdir?

2-İnternet üzerinde bir siteye üye olurken ad, soyad, doğum tarihi, doğum yeri, kredi kartı gibi bilgileri paylaşıırken endişe duyuyor musunuz? Bu endişenizin nedeni nedir?

3-İnternet üzerinde satın almayı düşündüğünüz birşeyin karşınıza reklam olarak çıktığı oluyor mu? Oluyorsa bu durum sizde nasıl bir his oluşturuyor?

4-Sizde bireylerin internet üzerindeki davranışları devletler ve reklam verenler tarafından denetleniyor mu?

İnternet herkes tarafından bilindiği üzere, sıklıkla yapılan bir benzetmeye göre, ucu bucağı olmayan bir deniz gibidir. Birey bu dijital ağlar üzerinde kendine dair paylaştığı kişisel veriler ile birçok tehdit ile karşı karşıya kalabilir. Bu bağlamda katılımcıların süperpanoptikon gözetim teknolojileri karşısında kişisel verilerinin güvenlik düzeyi hakkında farkındalık düzeylerini ortaya çıkarmak için “*İnternet üzerinde kişisel verilerinizin güvenliği konusundaki düşünceleriniz nelerdir?*” şeklinde bir soru yöneltildi. Bu soruya katılımcıların verdikleri yanıtlar şu şekildedir:

K1: “Her ne kadar korunduğunun söylenmesine rağmen yeterince korunduğunu düşünmüyorum ve gereksiz bir çok bilginin istendiğini düşünüyorum. Onları da koruyabildikleri gerçeği şüpheli.”

K2: “Kişisel verilerimi korumak için basit yöntemler kullanıyorum fakat bunların ne kadar işe yaradığı konusunda bilgim yoktur.”

K3: “Kişisel verilerimi elimden geldikçe paylaşmamaya özen gösteriyorum. Bu bilgilerle ne yapılacağını bilmediğim için paylaşmıyorum.”

K4: “Kullandığımız sosyal medyaların hiçbiri güvenli değil bana göre. Çünkü bugün sosyal medya hesaplarına ister istemez bilgilerimizi veriyoruz. Bu durum doğru değil ama bunun karşısında yapacak bir şey olmadığını görüyorum. Mecburen kullanıyoruz. Bütün sosyal medya kuruluşlarının güvenilir olmasını isterdim.”

K5: “Kişisel verilerin güvenliği konusunda endişelerim bulunmakla birlikte çok uzun yıllardır internet kullanmama rağmen bir sorunla, şüphemi artıracak bir durumla karşılaşmadığımı belirtmek isterim.”

K6: “Kişisel verilerimin korunmadığını düşünüyorum. Sadece korunmuş adı altında bilgilerin istenilen kişiler ile paylaşıldığını düşünüyorum. Ashnda bilgilerimiz kişisel bilgi olmaktan çıkıp kamuya açık bilgi haline gelmektedir.”

K7: “Güvende olduğunu düşünmüyorum. Hangi kişisel bilgilerimizin ele geçirildiğini bilmediğim için bu konuda endişe duyuyorum. Telefon no ya da konum bilgisi de olsa başkasının eline geçen veriler beni kaygılandırıyor.”

K8: “Tam anlamıyla bu verilerin korunduğunu düşünmüyorum örneğin alışveriş yapmadığımız markalardan gelen kampanya mesajları gibi.”

K9: “Kişisel verilerimin iznim dışında kullanılmasından çok endişeli değilim, güvenlik haklarımın olduğunu düşünüyorum.”

Araştırmaya dahil olan katılımcılardan biri hariç diğerleri internet üzerinde kişisel verilerinin güvende olmadığını düşünmektedir. Bu bulgulardan hareketle katılımcıların dijital ağlarda verilerinin güvenliği konusunda endişe duyduğu

anlaşılmaktadır. Bu soruya verilen yanıtlardan hareketle katılımcıların dijital ağların riskleri konusunda farkındalık sahibi olduğu değerlendirilebilir.

Diğer taraftan katılımcıların internet üzerinde gözetim teknolojileri karşısında kişisel verilerinin güvenliği konusunda endişe duyup duymadıklarını ortaya çıkararak farkındalık düzeylerini tespit etmek için “*İnternet üzerinde bir siteye üye olurken ad, soyad, doğum tarihi, doğum yeri, kredi kartı gibi bilgileri paylaşıırken endişe duyuyor musunuz? Böyle bir endişeniz varsa bu endişenizin nedeni nedir?*” sorusu yöneltildi. Katılımcıların ilgili soruya verdikleri yanıtlar şu şekildedir:

K1: “Evet duyuyorum. Güvenilir olma konusunda şüphelerim olduğundan verilerin korunmasını iyi yapamadıklarından dolayı istenilen kişisel bilgilerden birçok siteye üye olmaktan vazgeçtiğim oldu. Gerek olmayan kişisel verilen istenmesi de ekstra şüphe uyandırıyor.”

K2: “Özellikle alışveriş sitelelerinde bu bilgileri yazınca tedirgin oluyorum. Bazen kredi kartından alışveriş yapınca telefonuma şifre gelmeden alışverişin tamamlanması beni çok şaşırtıyor. Kart bilgilerinin bir sonraki alışveriş için kaydedilmesinden dolayı oluyor ama bu durum çok sağlıklı değil.”

K3: “Gerekmedikçe sitelere üye olmam ve kişisel bilgilerimi paylaşırken endişe duyarım.”

K4: “Endişe duyduğumu söyleyemem. Çünkü üye olmadan önce sitede araştırmalar yaparım, ondan sonra üye olurum. Örneğin Trendyol sitesine 3 yıldır üyeyim ve bu siteden alışveriş yapıyorum. Kişisel verilerim ile ilgili bir sorun yaşamadım. Burada sitenin güvenilirliği ve bilinirliği benim için önemli kriterdir.”

K5: “Endişe duyuyorum bundan dolayı da bilmediğim ya da güvenmediğim bir siteye üye olmuyorum. Üye olacaksam eğer kısa bir araştırma sonrası üye olmalıyım. Endişemin nedeni bana ait bilgilerle benim adıma birtakım işlemlerin yapılabilir olması.”

K6: “Benim için önemli olan yani kaydolmam gereken yerlere isim soyisim doğum yeri bilgilerimi veriyorum. Kredi kartı bilgilerimi kesinlikle hiçbir site ile paylaşmıyorum. Eğer internet üzerinden alışveriş yapıyorsam kart bilgilerimi kaydetmeden alışveriş yaparım. Bu bilgilerin hepsini vermek beni tedirgin ediyor.”

K7: “Sosyal medya hesaplarımda yer alan bilgiler ile örneğin fotoğrafım ile sahte bir hesabın açılmasından endişe duyuyorum. Ya da vermiş olduğum bilgiler ile adıma bir işlemin yapılması da beni zor durumda bırakır.”

K8: “Evet duyuyorum. Günümüzde siber anlamda her türlü şeyin mümkün olduğu bir çağda yaşadığımızı düşünürsek bu bilgiler ne kadar güvende olsa da sistemin bir açığı olmaktadır.”

K9: “Hayır, endişe duymuyorum, şahsi bilgilerimin iznim dışında kullanılması durumunda hukuksal haklarımı kullanırım.”

Katılımcıların dijital ortamda kişisel verilerinin güvenliği konusundaki endişelerine dair ifadeleri incelendiğinde, katılımcıların büyük çoğunluğunun, genellikle dijital gözetim teknolojilerinin tehditlerine yönelik birtakım önlemler almaya çalıştıkları anlaşılmaktadır. Söz konusu durum, katılımcıların büyük bölümünün (8 katılımcı) dijital ortamın risklerinin farkında olduğunu

göstermektedir. Öte yandan dijital ağlarda ekonomik iktidarların bireylerin kişisel verilerini önemli bir meta olarak gördüğü önceki bölümlerde sıklıkla vurgulanmıştı. Bireylerin verileri internet üzerinde çeşitli şekillerde toplanarak reklam verenlere satılmaktadır. Bu şekilde bireylerin karşısına kişiselleştirilmiş reklamlar çıkmaktadır. Bireylerin bu konuda farkındalık düzeylerini ölçmek için “*İnternet üzerinde bazen satın almayı düşündüğünüz birşeyin karşınıza reklam olarak çıktığı oluyor mu? Oluyorsa bu durum sizde nasıl bir his oluşturuyor?*” sorusu yöneltildi. İlgili soruya alınan yanıtlar şöyledir:

K1: “Evet oluyor. Gün içerisinde dinlenme algoritmasından dolayı günümüzde bilindik bir şey artık. Herhangi bir ürünü arattığımda veya konuştuğumda sürekli karşıma artık o üründen çıkmaya başlıyor ve bu da bir hayli ürkütüyor. Ne kadar alışmış olsakta özeline dinlenilmesi ve karşısına onların çıkması özel hayatı ciddi tehdit ediyor.”

K2: “Bu durumu sıklıkla yaşıyorum. Sosyal medya hesaplarından aradığım bir ürünü girdiğim sitelerde reklam olarak görebiliyorum. Arama geçmişini sürekli temizlesem dahi bu durum ile sıklıkla karşılaşıyorum. Bu durum izlendiğimi, heran takip edildiğimi hissettiriyor.”

K3: “Oluyor fakat artık normal buluyorum. Bunu etrafımdaki insanlar da söylüyorlar. Buna artık şaşırıyorum”

K4: “Çoğu zaman daha önceden beğendiğim gönderilerde yer alan ürünler karşıma reklam olarak çıkmaktadır. Çok şaşırtıcı.”

K5: “Evet çok sık oluyor. İnternet üzerinden yaptığımız aramaların ya da sohbet programlarında geçen konuşmaların karşıma çıkması aslında bize ait şeylerin bize ait olmadığını düşündürüyor.”

K6: “Telefonlar aracılığıyla hepimizin dinlenebildiği bir dönemde yaşıyoruz. İlk kez bu durum ile karşılaşıncaya şaşırmıştım ama şu an çok şaşırmıyorum. Yine de bu durum pek olumlu şeyler hissettirmiyor.”

K7: “Ben bu durumu sıklıkla yaşamaya başladım. Telefonların dinlendiğini düşünmeye başladım, çünkü bazen arkadaşlarım ile konuştuğum bazı şeyler hemen sonraki gün karşıma çıkıyor. Bunları görünce tedirginliğim daha çok artıyor.”

K8: “Evet oluyor. Telefonlar aracılığıyla izleme, dinleme gibi şeyler var ki bizim o an konuştuğumuz şeyin reklamı karşımıza çıkıyor ve endişe verici bir duruma dönüşüyor.”

K9: “Evet, Instagram arayüzünde zihnimde geçirdiğim şeylerin akışa düştüğüne çok defa şahit oldum. İnternet aracılığıyla yaptığım aramalarda buna şahit oldum.”

Bu bulgulardan hareketle, katılımcıların kişiselleştirilmiş reklamlar için gözetletlendiği konusunda tüm katılımcıların farkındalık düzeyine sahip olduğu anlaşılmaktadır. Özetle katılımcılar, kendilerine dair verilerin yine kendilerine yönelik olarak kullanıldığının farkındadırlar.

Tarihsel süreçte devletlerin varlıklarının devamını sağlamak için vatandaşlarını gözetime tabi tuttukları bilinmektedir. Toplumsal düzeni bozan ve devletin varlığını riske atan insan eylemlerinin gözetlenerek disipline edilmesi devletler için her zaman önemli olmuştur. Ancak bu gözetim tekniklerinin sıradan insanları da içine alarak baskı unsuruna dönüşmesi ise istenmeyen bir durumdur. Günümüzde ise internetin anonimliği devletleri de birtakım önlemler

almaya itmiştir. Bu önlemler ile devletin güvenliğini tehdit edecek unsurların denetlenebilirliği sağlanmaya çalışılmaktadır. Ancak daha önceki satırlarda da ifade edildiği üzere bu dijital gözetim faaliyetlerinin sıradan insanların eylemlerini de içine alacak şekilde genişletilmesi bireysel mahremiyet ihlalleri ile sonuçlanabilir. Öte yandan daha önce de birçok kez vurgulandığı üzere dijital ağların gözetim kulesinde yer alan ve mahremiyet ihlallerine sebep olan bir diğer iktidar sahibi ekonomik iktidarlardır. Çoğu kişisel verinin bu iktidarlar tarafından bireyin kendisine bir silah olarak kullanıldığı artık herkes tarafından derinden hissedilmektedir. Tüm bunlar ise dijital ağlarda bireylerin mahremiyetine vurulan önemli darbelerdir. Bu bağlamda katılımcıların devletlerin ve reklamverenlerin dijital gözetim faaliyetlerden haberdar olup olmadığını öğrenmek için “*Sizce bireylerin internet üzerindeki davranışları devletler ve reklam verenler tarafından denetleniyor mu?*” sorusu yöneltildi. İlgili soruya alınan yanıtlar şu şekildedir:

K1: “Hayır asla düşünmüyorum çok nadir ses getiren davranışlar kontrol altına alınıyor diğer türlü ses duyulmamış davranış ve reklamlar rahatlıkla yapılıyor.”

K2: “Devlet tarafından denetlendiğini düşünüyorum ve bunun gerekli olduğunu düşünüyorum. Çünkü herkes sosyal medyayı farklı amaçlar ile kullanmaktadır. Zararlı içerikler ve yanlış bilgileri empoze eden hesapların control edilmesi gerekmektedir.”

K3: “Denetleniyordur bence. Mail adresine gelen reklamlar başka şekilde ulaştırılmaz. Bizim verilerin para karşılığında reklam şirketlerine satıldığını biliyorum ama nasıl yapıldığını anlamıyorum.”

K4: “Bu konuda malesef bilgim yok.”

K5: “Evet denetlendiği için bütün bilgilerimi vermeyi tercih etmiyorum.”

K6: “Devlet tarafından denetlendiğini düşünüyorum. Ama devlet bunu bazı sebeplerden dolayı yapmaktadır. Reklam verenler reklamlarını ulaştıracakları kitleyi daha iyi tanımak için denetliyor olabilirler.”

K7: “Öncelikle internet ve sosyal medya uygulamalarının denetlenmesi gerektiğini düşünüyorum ama sıkı bir denetim olmadığını düşünüyorum.”

K8: “Hayır denetlenmiyor bence. Denetlenseydi kişisel verilerimiz satılmaz ve bu bilgilere devlet dışındaki kurumlar sahip olmazdı.”

K9: “Evet, devlet değil ama reklam veren şirketler tarafından denetlendiğini ve ona göre algoritma oluşturulduğunu düşünüyorum. Satın alma davranışlarının altyapısında bu bilgilerin kullanıldığını düşünüyorum.”

Katılımcıların bir kısmı (2 katılımcı) yalnızca devletlerin dijital gözetim faaliyetlerine ifadelerinde yer verirken, katılımcıların bir diğer kısmı (3 katılımcı) ise yalnızca reklam verenlerin gözetim faaliyetlerine ifadelerinde yer vermektedir. Öte yandan katılımcıların bir kısmı (2 katılımcı) ise hem devletlerin hem de reklam verenlerin dijital gözetim faaliyetlerine ifadelerinde yer vermişlerdir. Bununla birlikte 2 katılımcının ise ifadelerinden söz konusu denetim faaliyetlerinden haberdar olmadığı anlaşılmaktadır. Özetle katılımcıların büyük bir bölümü internetin tamamen denetimden uzak bir ortam olmadığını farkındadırlar.

5.4.2.Dijital Ağlarda Katılımcıların Gözetime Karşı Aldıkları Tedbirler

İnternetin bireylerin yaşamlarına büyük kolaylıklar getirdiği kimse tarafından inkâr edilemez. Ancak internetin olumlu yanlarının yanı sıra, olumsuz taraflarını da gözden kaçırmamak gerekir. Özellikle konuya “dijital gözetim bağlamında bakıldığında birey bu ağlarda geçmiş dönemlere kıyasla ciddi mahremiyet ihlalleri ile karşılaşabilir. “Bu ihlaller bazen, sosyal ağlar gibi platformlar vasıtası ile bireyin gönüllü olarak gerçekleştirdiği ifşaatların sonucunda gerçekleşebilirken” (Tiryaki, Balcı ve Karakuş, 2021, s. 61-62), bazen de bireylerin dijital ağları kullanırken, farkına bile varmadan arkalarında bıraktıkları kişisel veri kırıntıları ile yaşanabilir. Bu noktada eleştirel bir bilince sahip olmak, internetin ardındaki iktidar mekanizmalarına karşı birtakım tedbirler alınmasını sağlayacağı için önem taşımaktadır. Bu bağlamda araştırmaya dahil olan Z kuşağına mensubu katılımcıların, dijital gözetim teknolojileri karşısında eleştirel bir bilince sahip olup olmadığını tespit etmek ve bu konuda birtakım tedbirler alıp almadıklarını değerlendirmek için, katılımcılara yarı yapılandırılmış görüşme sırasında şu sorular sorulmuştur:

- 1-Bir siteye üye olurken üyelik sözleşmesini okuyor musunuz?
- 2-İnternet üzerinde aramaktan sakındığınız şeyler oluyor mu?
- 3-Sosyal ağların konum, fotoğraf galerisi vb. gibi verilerinize erişim iznini sınırlandırıyor musunuz?
- 4-Mailinize gelen herhangi bir linke tıklamadan önce, linkin güvenilir bir kişiden gelip gelmediğine bakıyor musunuz?

İnternet üzerinde bütün siteler üye olacak abonelerine bir üyelik sözleşmesi sunarlar. Bu sözleşmeler genellikle çok uzun olduğundan bireyler tarafından okunmazlar. Ancak sonraki süreçte bu sözleşmelerin bireylere ne getireceği belirsizdir. Üye olurken verilen ad, soyad, iletişim bilgileri vb. üçüncü taraf işletmeler ile farklı amaçlarla paylaşılabilir. Bundan dolayı bu tür sözleşmelerin detaylıca okunması, bireyin farkında olmadan kendi eli ile mahremiyetini yıkmaması adına önem teşkil etmektedir. Bu noktadan hareketle araştırmaya dahil olan katılımcılara “*Bir siteye üye olurken üyelik sözleşmesini okuyor musunuz?*” sorusu yöneltildi. Katılımcıların ilgili soruya verdikleri yanıtlar şu şekildedir:

- K1: “Çok önemli sitelerde okurum ama önemsiz gördüğüm yerlerde pek dikkate almıyorum.”
- K2: “Genellikle okumuyorum. Bunun sebebi üyelik sözleşmesinin çok uzun olması. Orada yazan haklar ve hukuki terimleri anlamadığım için okumuyorum.”
- K3: “Okuyorum ama genellikle bu sözleşmeyi kabul ediyorum. Bazı haklarım olduğunu bu sözleşmelerde görüyorum.”
- K4: “Ben sitelere üye olmadan önce mutlaka bunları okuytorum. Sitelerin güvenilirliği konusunda endişelerim olduğu için bu sözleşmeleri mutlaka okuyup, incelerim.”
- K5: “Endişe duyduğum bir site ise bakıyorum ancak bir şüphem yoksa okuma gereği duymuyorum.”

K6: “Üyelik sözleşmelerinde üyeliği sonlandırma kısımlarını okuyorum. Her bölümü okumak çok güç olduğu için en önemli olan alanları okumaya çalışıyorum.”

K7: “Evet genellikle okumaya çalışıyorum.”

K8: “Hayır okumuyorum. Bu sözleşmeleri okumam gerekiyor ama sözleşmeler o kadar uzun ve karmaşık ki neredeyse okunmasın diye yazılmış metinler gibi geliyor bana. Herhangi bir sorun ile karşılaşıncı mecburen okuyorum.”

K9: “Evet, okuyorum ama detaylı bir şekilde incelemiyorum.”

Katılımcıların ilgili soruya verdikleri yanıtlar incelendiğinde, katılımcıların küçük bir kısmı (2 katılımcı) üyelik sözleşmesini uzun olduğu gerekçesi ile okumadığını ifade etmiştir. Katılımcıların önemli kısmı (7 katılımcı) ise bu sözleşmeleri okumanın gerekli olduğunu belirtmişlerdir. Özetle katılımcıların büyük bir bölümü üye olacakları sitenin kendilerine oluşturabileceği tehditleri önceden öngörebilmek için üyelik sözleşmelerini okumanın önemini kavramış durumdadırlar. Katılımcıların küçük bir kısmı ise uzun olması gerekçesi ile okumadıkları sözleşmelerin ilerleyen zamanlarda kendilerine neler getireceği konusunda belirsiz içindedir.

Bireyler internetin anonim bir ortam olmadığını, internet üzerinde arama yaptıktan sonra karşısına çıkan kişiselleştirilmiş reklamlar ile anlayabilir. Bireyin arama geçmişi Google tarafından analiz edilerek kullanıcılara kişiselleştirilmiş reklamlar sunulabilir. Bu yalnızca ekonomik gözetimin bir boyutudur. Aynı şekilde söz konusu bu dijital ağlar siyasal iktidarların da gözetim altındadır. Bu bağlamda eleştirel dijital medya okuryazarlığına sahip olmak, bireyin internet üzerinde hem mahremiyet kaybını ortadan kaldıracaktır, hem de suç oluşturacak eylemlerde bulunmasına karşı tedbirli olmasına katkı sağlayacaktır. Bu noktada katılımcıların bu tür dijital gözetim teknolojileri karşısında ne tür savunma mekanizmaları geliştirdiğini değerlendirmek için katılımcılara “*İnternet üzerinde aramaktan sakındığınız şeyler oluyor mu?*” sorusu yöneltildi. İlgili soruya alınan yanıtlar ise şu şekildedir:

K1: “Evet oluyor. Bu durumlarda aramaları kendi hesabımdan yapmıyorum yedek hesaplarım olunca aramaları oradan yapıyorum.”

K2: “Bazen sakındığım için gizli sekmeden aramalar yapıyorum ya da aramayı yaptıktan sonra geçmişi temizliyorum.”

K3: “Bazen bazı şeyleri aramaktan çekiniyorum ama bu çok olmuyor.”

K4: “Hayır, genellikle olmuyor.”

K5: “Hayır. Çünkü internet üzerinde aradığım şeyler genellikle herkesin aradığı şeyler oluyor. Bundan dolayı endişe duymuyorum.”

K6: “Sadece aramak değil bazen konuşmaktan da çekindiğim şeyler oluyor. Herşeyi WhatsApp üzerinden konuşmayı uygun görmüyorum. Bunun gibi aklıma gelen her şeyi aramak da pek uygun değil.”

K7: “Hayır, genellikle aradığım şeyler sakınca gerektirmeyen şeyler oluyor.”

K8: “Evet oluyor. İzlediğimi düşündüğüm zaman neredeyse çoğu şeyi aramaktan korkar hale geliyorum. Tabi arama yapınca birşey olmaz ama bir işe başvuru yaparken bile bu aramalar, beğeniler karşımıza çıkacak diye düşünüyorum.”

K9: “Hayır, şimdiye kadar olmadı.”

Katılımcıların ilgili soruya verdikleri yanıtlar incelendiğinde, katılımcıların tamamına yakını (8 katılımcı) internet üzerinde zaman zaman aramaktan sakındığı şeyler olduğunu ifade etmişlerdir. Yani dijital gözetim teknolojilerine karşı kendilerine göre bir savunma mekanizması geliştirmişlerdir. 1 katılımcı ise internet üzerinde aramaktan sakındığı birşey olmadığını ifade etmiş, bu ortamın ona özgür bir ortam sağladığını belirtmiştir.

Herkes tarafından dile getirildiği üzere internet bağlantılı akıllı telefonlar bireylerin yaşamlarının vazgeçilmez bir parçası durumundadır. Bireyler bu akıllı cihazlarına sohbet, eğlence vb. içeriklere sahip olan birçok uygulama yükleyebilmektedirler. Bireyler bu uygulamaları cihazlarına yükledikten sonra, söz konusu uygulamalar kullanıcılarından birçok erişim izni (fotoğraf galerisine erişim, konum izni vb.) istemektedir. Bu izinler aracılığı ile bireyler dijital gözetimin birer nesnesi haline gelebilmektedir. Bu bağlamda katılımcıların söz konusu uygulamaları kullanırken hangi kişisel verilerini uygulama ile paylaşımını sınırlandırdıklarını değerlendirmek için “*Sosyal ağların konum, fotoğraf galerisi vb. gibi verilerinize erişim iznini sınırlandırıyor musunuz?*” sorusu yöneltildi. İlgili soruya alınan yanıtlar şu şekildedir:

K1: “Evet bu tarz erişimin gerek olmadığını düşündüğümden izin vermediğim için çok fazla kullanmaktan kaçınıyorum öyle yerleri.”

K2: “Bazı sosyal medya hesaplarında sınırlandırmak malesef mümkün olmamaktadır. Sınırlandırma yetkimin olduğu sosyal medya uygulamalarında sınırlandırıyorum. Günümüzde konum için Google ve WhatsApp kullandığım için sürekli konum açık kalmaktadır.”

K3: “Evet kişisel verilerimize ulaşmalarını istemiyorum.”

K4: “Bazı sosyal medya hesaplarında sınırlandırma yapıyorum. Örneğin snapchat. Bu uygulama benden sürekli konum istemekte ama ben konumumu paylaşmak istemiyorum.”

K5: “Evet. Telefon galerisinde bulunan fotoğraflar ve diğer şeylerin hepsi bana ait, özel olduğu için izin vermiyorum.”

K6: “Erişim izinlerini sınırlandırabildiğim kadar sınırlandırıyorum. Özellikle konum izni isteyen uygulamalarda tedirgin oluyorum.”

K7: “Bazı sınırlandırmalar yapmaya çalışıyorum fakat bu sınırlamaları getirdikten sonra sitelerin ya da uygulamaların bazı özelliklerini kullanamıyorum. Bundan dolayı tekrar sınırlamaları kaldırmak zorunda kalıyorum.”

K8: “Evet sınırlandırıyorum. Bu sınırlandırmaların devlet tarafından zorunlu hale getirilmesi gerekiyor. Çünkü özel bilgilerimi verme karşılığında uygulamayı kullanmama izin vermesini etik görmüyorum.”

K9: “Evet, sınırlandırıyorum çünkü bu bilgilerin nasıl kullanılacağı konusunda endişelerim var.”

Katılımcıların tamamının yükledikleri uygulamaların erişebilecekleri kişisel verileri sınırlandırma konusunda bir çabaya sahip olduğu görülmektedir. Diğer bir ifade ile katılımcılar dijital gözetimin farkındalar ve bu konuda birtakım önlemler almaya çalışmaktadırlar. Akıllı telefonların bireye dair birçok mahrem bilgiyi içerdiği düşünüldüğünde, yüklenen her uygulamanın bireyin mahrem bilgilerini dijital gözetime tabi tutarak yıkıma uğratacağı unutulmamalıdır.

Dijitalleşme, bireylerin yaşamına büyük kolaylıklar sağlamakla birlikte, bir taraftan da yine aynı teknoloji vasıtası ile büyük tehditlerle kolay bir şekilde karşı karşıya kalabilmesine de sebep olabilmektedir. Örneğin, teknolojinin bu kadar gelişkin olmadığı zamanlarda bir mektubun alıcısına ulaşması belki ayları bulabilirken, günümüzde saniyeler içerisinde dünyanın bir ucundan diğer ucuna kolaylıkla mail gönderilebilmektedir. Ancak bazen bilinmeyen kaynaklardan gelerek mail kutusunu dolduran tehlikeli yönlendirici mailler, kullanıcının akıllı cihazının kötü niyetli insanlar tarafından kolaylıkla ele geçilmesini sağlayabilir. Bu konuda farkındalık sahibi olmak önem teşkil etmektedir. Bu bağlamda, araştırmada, katılımcıların söz konusu bilinmeyen kaynaklardan gelen maillere yönelik aldıkları önlemleri değerlendirmek ve bu konudaki farkındalık düzeyini ölçmek için *“Mailinize gelen herhangi bir linke tıklamadan önce, linkin güvenilir bir kişiden gelip gelmediğine bakıyor musunuz?”* sorusu yöneltildi. İlgili soruya alınan yanıtlar şu şekildedir:

K1: “Evet tanımadığım kişilerden gelen link veya mesajları dikkate almıyor ve bakmıyorum.”

K2: “Ben hiçbir linke tıklamak istemiyorum çünkü gerçekten güvenim kalmadı. Sahte linkler ve siteler üretmek kolay olduğu için herkes tarafından bilinen siteler dışında sitelere girmemeye çalışıyorum.”

K3: “Evet, gelen maillerin çoğunluğu reklam mailleri oluyor. Bir tane linke tıklayınca ardından başka linkler geliyor bu durum hiç bitmiyor.”

K4: “Mutlaka bakarım. Bu zamanda güvenilir çok az kişi ve kurum var. Gelen mail güvenilir ve tanınır bir yerden gelmiyorsa bu mailleri açmadan silmeyi tercih ediyorum.”

K5: “Evet bakıyorum. Çünkü bir tane linke tıklamak bile her şeye izin vermek anlamına gelmektedir. Bundan dolayı dikkat etmeye çalışırım.”

K6: “Spam kutusuna düşen maillerde bu durumu göz önüne alıyorum. Bu mailleri açmadan siliyorum. Çünkü çoğu mail reklam verenler tarafından gönderiliyor.”

K7: “Tanımadığım ya da bilmediğim yerlerden gelen mailleri siliyorum. Bu mailer ya reklam mailleri oluyor ya da spam mailer oluyor. Bilgisayara zarar vereceğini düşündüğüm için bu linklere tıklamıyorum.”

K8: “Tabiki bakıyorum.”

K9: “Evet, link konusunda dikkat ediyorum. Linklerin içerikleri çoğu zaman reklam olabiliyor ya da zararlı bazı içerikler sunulabiliyor.”

Görüşme yapılan katılımcıların tamamı (9 katılımcı) bilinmeyen kaynaklı maillere karşı dikkatli davrandıklarını ifade etmişlerdir. Diğer bir ifade ile katılımcılar, dijital ortamın riskleri konusunda farkındalığa sahiptirler.

Sonuç

Tarihsel süreçte gözetim aracılığıyla disiplini sağlama iktidarlar tarafından tercih edilen bir yöntem olmuştur. Günümüzde de aynı şekilde gözetim aracılığı ile disiplini sağlama iktidarlar için önemli bir yöntemdir. Ancak günümüzde iktidarların kullanmış olduğu gözetim teknikleri ve uygulama şekilleri geçmişteki tekniklerden çok büyük farklılıklara sahiptir. Günümüzdeki gözetim teknikleri, internet teknolojilerinde yaşanan gelişmeler ile daha yumuşak bir şekilde gerçekleştirilme imkanına sahip olmuştur. Bireyler, internet ortamında özgür bir ortam yanılması içerisinde varlıklarını sürdürürken, iktidarların

gözetimine tabi tutulmakta, farklı şekillerde gözetimin nesnesi haline getirilmektedirler. Bu noktada, bireylerin internet üzerinde, söz konusu dijital gözetim teknolojileri karşısında farkındalığa sahip olması, mahremiyetini koruması açısından önem taşımaktadır. Bu bağlamda söz konusu araştırmada; küçük yaşlardan itibaren internet teknolojileri ile tanışık olan ve dijital yerliler olarak da adlandırılan Z kuşağının, söz konusu süperpanoptikon gözetim teknolojileri karşısında ne düzeyde farkındalığa sahip olduğunu ortaya çıkarmak, araştırmanın temel problemini oluşturmaktadır. Öte yandan bu araştırma, Z kuşağının dijital gözetim teknolojileri karşısındaki farkındalık düzeylerini ölçmeye çalışarak, onların dijital eleştirel okuryazarlık düzeylerini ortaya çıkarması açısından önem taşımaktadır. Diğer taraftan söz konusu araştırmanın temel amacı, iktidar mekanizmalarının dijital ağlarda gerçekleştirdiği süperpanoptikon gözetim karşısında, Z kuşağının farkındalık düzeyini ortaya çıkarmaktır.

Araştırmanın bulgularına göre, katılımcıların internet kullanım süresi 5 saat üzerinde değişkenlik göstermektedir. Diğer taraftan katılımcıların interneti kullanma amaçlarına bakıldığında, katılımcıların büyük bir bölümünün interneti bilgi aramak ve eğlenmek için kullandığı anlaşılmaktadır. Katılımcılar banka kartı bilgileri (6 katılımcı), cep telefonu rehberi (4 katılımcı), telefon numarası (5 katılımcı), anlık konum bilgileri (6 katılımcı), fotoğraflar (6 katılımcı), açık adres (5 katılımcı), gezilen internet siteleri (2 katılımcı), kimlik bilgileri (1 katılımcı), her tür veri (1 katılımcı) vb. bilgileri kişisel veri olarak değerlendirmektedir.

Diğer taraftan araştırmanın amacına uygun olarak Z kuşağının dijital gözetim farkındalığını ve dijital gözetime yönelik aldıkları tedbirlere yönelik katılımcılara bir takım sorular yöneltilmiştir. Katılımcıların dijital gözetim farkındalığını ölçmek için yöneltilen sorular ve alınan cevaplar şöyledir: **1-** İnternet üzerinde kişisel verilerinizin güvenliği konusundaki düşünceleriniz nelerdir? (güvende olduğunu düşünmüyorum (8 katılımcı), güvende olduğunu düşünüyorum (1 katılımcı)), **2-** İnternet üzerinde bir siteye üye olurken ad, soyad, doğum tarihi, doğum yeri, kredi kartı gibi bilgileri paylaşırken endişe duyuyor musunuz? Bu endişenizin nedeni nedir? (8 katılımcı evet, 1 katılımcı hayır), **3-** İnternet üzerinde satın almayı düşündüğünüz birşeyin karşınıza reklam olarak çıktığı oluyor mu? Oluyorsa bu durum sizde birileri tarafından gözetlendiğiniz hissini oluşturuyor mu? (9 katılımcı evet), **4-** Sizce bireylerin internet üzerindeki davranışları devletler ve reklamverenler tarafından denetleniyor mu? (2 katılımcı evet ama yalnızca devletler tarafından değerlendiriliyor, 3 katılımcı evet ama yalnızca reklam verenler tarafından denetleniyor, 2 katılımcı hem devletler hem de reklamverenler tarafından denetleniyor, 2 katılımcı böyle bir denetim faaliyetinden haberim yok) soruları yöneltilti. Bu sorulara alınan yanıtlar değerlendirildiğinde katılımcıların büyük oranda dijital gözetim teknolojilerine karşı farkındalığa sahip olduğu değerlendirilebilir.

Öte yandan katılımcıların dijital gözetim teknolojilerine karşı ne tür tedbirler aldığını öğrenmek için yöneltilen sorular ve alınan cevaplar şöyledir: **1-** Bir siteye üye olurken üyelik sözleşmesini okuyor musunuz? (7 katılımcı evet okuyorum, 2 katılımcı hayır okumuyorum), **2-** İnternet üzerinde aramaktan sakındığınız şeyler oluyor mu? (8 katılımcı evet aramaktan sakındığım şeyler oluyor, 1 katılımcı hayır olmuyor), **3-** Sosyal ağların konum, fotoğraf galerisi vb. gibi

verilerinize erişim iznini sınırlandırıyor musunuz? (9 katılımcı evet verilerime erişimi sınırlandırıyorum), 4- Mailinize gelen herhangi bir linke tıklamadan önce, linkin güvenilir bir kişiden gelip gelmediğine bakıyor musunuz? (9 katılımcı evet linkin güvenilirliğini sorguluyorum) gibi sorular yöneltildi. Genel olarak katılımcıların sorulara verdikleri yanıtlar incelendiğinde katılımcıların dijital gözetim teknolojileri karşısında birtakım önlemler almaya çalıştığı görülmektedir.

Araştırma sonucunda elde edilen bulguların genel bir değerlendirmesi yapıldığında, Z kuşağı mensubu katılımcıların büyük bir bölümü dijital gözetim teknolojilerinin varlığından haberdar durumda ve bu gözetim teknikleri karşısında birtakım önlemler almaya çalıştıkları anlaşılmaktadır.

Dijital ağları kullanmanın bireysel mahremiyet ihlalleri ile sonuçlandığı günümüzde, bu kaybı en aza indirmek için dijital gözetim teknolojilerinin varlığına dair farkındalık kazanmak önem taşımaktadır. Eleştirel bir bilince sahip olmak, bu teknolojilerin ardındaki iktidar mekanizmalarını görmeyi sağlayacak, bireyi mahremiyetini korumaya yönelik önlemler alması yönünde adımlar atması için harekete geçirecektir.

Kaynakça

- Akdağ, G. (2015). *"Gözetim toplumu" teorilerinin tarihsel ve teorik bir incelemesi.* (Yayımlanmamış yüksek lisans tezi). Adnan Menderes Üniversitesi, Aydın.
- Alay, H.K. ve Deveciyan, M.T. (2023). *Digital footprint management: Digital burial- dijital ayak izi yönetimi: Dijital defin.* *Nevşehir Hacı Bektaş Veli Üniversitesi Sosyal Bilimler Dergisi*, 13(3), 1446-1456.
- Alkan, F. ve Özcan, A. (2019). Üniversite öğrencilerinin gözetime, güvenlik ve mahremiyet bağlamında yaklaşımı üzerine bir araştırma. *Gümüşhane Üniversitesi İletişim Fakültesi Elektronik Dergisi*, 7(1), 270-292.
- Apple. (2023). <https://support.apple.com/tr-tr/guide/icloud/mmae56ea1ca5/icloud#:~:text=Ancak%20kal%C4%B1c%C4%B1%20olarak%20sildi%C4%9Finiz%20dosyalar%C4%B1%20kurtaramaz%20ve%20geri%20y%C3%BCkleyemezsiniz.> (Erişim Tarihi: 01.10.2023).
- Aust, S. ve Ammann, T. (2019). *Dijital diktatörlük.* (E. Yücel ve H. Yılmaz, Çev.) (3. bs.). Ankara: Hece Yayınları.
- Avast. (2023). <https://blog.avast.com/2014/07/08/tens-of-thousands-of-americans-sell-themselves-online-every-day/>. (Erişim Tarihi: 01.10.2023).
- Bahar, A. (2020). Polislik perspektifinden dijital misenformasyon ve dezenformasyon: Covid-19 örnek olayı bağlamında bir analiz. *OPUS International Journal of Society Researches*, 16(30), 2760-2794.
- Bauman, Z. (2010). *Küreselleşme: toplumsal sonuçları.* (A. Yılmaz, Çev.) (3. bs.). İstanbul: Ayrıntı Yayınları
- Bauman, Z. ve Lyon, D. (2016). *Akışkan gözetim.* (E. Yılmaz, Çev.) (2. bs.). İstanbul: Ayrıntı Yayınları.

- Biernacki, P. ve Waldorf, D. (1981). Snowball sampling: Problems and techniques of chain referral sampling. *Sociological Methods & Research*, 10(2), 141-163.
- Bozkurt, V. (2000). Gözetim ve internet: özel yaşamın sonu mu?, *Birikim Dergisi*, 75-81.
- Cooper, C. (2015). *You've been googled: What employers don't want to see in your online profile*. <https://www.theguardian.com/careers/careers-blog/google-online-searches>. (Erişim Tarihi: 01.10.2023).
- Çelik, R. (2014). *Gözetim toplumu ve internet: Yeni iletişim ortamlarında gözetimin dönüşümü*. (Yayımlanmamış doktora tezi). Marmara Üniversitesi, İstanbul.
- Çoban, B. (2019). *Panoptikon: Gözün İktidarı Üzerine*. B. Çoban ve Z. Özarslan (Ed.), *Panoptikon: Gözün İktidarı içinde* (s. 111-138). İstanbul: Su Yayınları.
- Dolgun, U. (2004). Gözetim toplumunun yükselişi: enformasyon toplumundan gözetim toplumuna. *Yönetim Bilimleri Dergisi*, 2(1), 55-74.
- Dolgun, U. (2015). *Şeffaf hapisane yahut gözetim toplumu*. İstanbul: Ötüken Yayıncılık.
- Drakopoulou, S. (2017). “We can remember it for you”: Location, memory, and commodification in social networking sites. *Sage Open*, 7(3), 1-13.
- Facebook, (2023). <https://www.facebook.com/privacy/policy>. (Erişim Tarihi: 01.10.2023).
- Foucault, M. (1992). *Hapishanenin Doğuşu*. (M. A. Kılıçbay, Çev.) (5. bs.). Ankara: İmge Kitapevi Yayınları.
- Foucault, M. (2007). *Cinselliğin Tarihi*. (H.U. Tanrıöver, Çev.) (2.bs.). İstanbul: Ayrıntı Yayınları.
- Foucault, M. (2014). *Özne ve İktidar*. (I. Ergüden ve O. Akınhay, Çev.) (4. bs.). İstanbul: Ayrıntı Yayınları.
- Foucault, M. (2015). *Büyük Kapatılma*. (I. Ergüden ve F. Keskin, Çev.) (4. bs.). İstanbul: Ayrıntı Yayınları.
- Giddens, A. (2008). *Ulus-Devlet ve Şiddet*. (C. Atay, Çev.) (2. bs.). Kalkedon Yayınları.
- Göker, G. (2016). Bir gözetim aracı olarak Periscope. *Çankırı Karatekin Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, 7(1), 969-992.
- Hıdıroğlu, İ. (2019). Ana-akım filmlerde gözetim olgusunun temsili. *Atatürk Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, 23(3), 1407-1426.
- Işıklı, Ş. (2014). Büyük veri, epistemoloji ve etik tartışmalar. *AJIT-e: Bilişim Teknolojileri Online Dergisi*, 5(17), 89-122.
- Karaarslan, E., Demir, M. ve Fetah, V. (2016). *Akıllı telefonlarda gizlilik ve mahremiyet: durum saptaması ve öneriler*. 18. Akademik Bilişim Konferansı. Aydın.

- Leith, D., Patras, P. ve Liu, H. (2021). *Android Destekli Cep Telefonları Kullanıcıların Onayı Olmadan Veri Paylaşımı Yapıyor*. <https://tr.euronews.com/2021/10/15/android-destekli-cep-telefonlar-kullan-c-lar-n-onay-olmadan-veri-paylas-m-yap-yor-arast-rm>. (Erişim Tarihi: 15.09.2022).
- Lyon, D. (2006). *Gözetlenen Toplum*. (G. Soykan, Çev.). (1. bs.). İstanbul: Kalkedon Yayıncılık.
- Lyon, D. (2012). *Vesikalı Yurttaş: Gözetim Aracı Olarak Kimlik Kartları*. (B. Baysal, Çev.). (1. bs.). İstanbul: Kalkedon Yayıncılık.
- Lyon, D. (2013). *Gözetim Çalışmaları*. (A. Toprak, Çev.). (1. bs.). İstanbul: Kalkedon Yayıncılık.
- Marx, Gray T. (1996). *Privacy and technology*, telektronik, <http://web.mit.edu/gtmarx/www/privantt.htm>. (Erişim Tarihi: 25.09.2023).
- Önal, İ. ve Bendaş, K. (2017). Sinoptik Çağda Gözetimin Morfolojisi: Takip Edilmek ve İnternet Reklamcılığı. *Anasay 3 Aylık Ulusal Hakemli Dergi*, (2), 109-117.
- Özdemir, Ş. (2020). Post-panoptikon Çağı: Gözetimin Dijitalleşmesi ve Çevrimiçi Kimliğin Gizliliği Üzerine Bir Analiz. *Anadolu Üniversitesi Sosyal Bilimler Dergisi*, 20(3), 81- 108.
- Rose, P., Beeby, J. ve Parker, D. (1995). Academic rigour in the lived experience of researchers using phenomenological methods in nursing. *Journal of Advanced Nursing*. 21(6), 1123-1129. <https://doi.org/10.1046/j.1365-2648.1995.21061123.x>
- Schermer, B. W. (2007). *Software agents, surveillance, and the right to privacy: a legislative framework for agent-enabled surveillance*. (Doctoral Thesis). Leiden University Press, Leiden
- Smith, J. A. ve Eatough, V. (2007). Interpretative Phenomenological Analysis. In E. Lyons ve A. Coyle (Ed.). *Analysing Qualitative Data in Psychology*. (s. 35-50). Los Angeles: SAGE Publications.
- Smith, J. A. ve Osborn, M. (2004). Interpretative Phenomenological Analysis. In G. M. Breakwell (Ed.), *Doing Social Psychology Research* (s. 229–254). Leicester, England: British Psychological Society. <https://doi.org/10.1002/9780470776278.ch10>
- Timurturkan, M. (2010). Gündelik hayatın gözetimi: “Panoptikon toplumu”. *ETHOS: Felsefe ve Toplumsal Bilimlerde Diyaloglar Dergisi*, 3(2), 1-19.
- Tiryaki, S., Balcı, E.V. ve Karakuş, M. (2021). Gözetim, Mahremiyet ve Sosyal Medya. İletişimde Güncel Çalışmalar II. içinde (s.61-84). (Ed. S. Tiryaki ve E.V. Balcı). Konya: Palet Yayınları.
- Zhu, Y. Q. ve Chang, J. H. (2016). The key role of relevance in personalized advertisement: examining its impact on perceptions of privacy invasion, self-awareness, and continuous use intentions. *Computers in Human Behavior*, 65, 442-447.