Anadolu Üniversitesi Sosyal Bilimler Dergisi AÜSBD
Anadolu University Journal of Social Sciences AUJSS

Post- Panoptikon Çağı: Gözetimin Dijitalleşmesi ve Çevrimiçi Kimliğin Gizliliği Üzerine Bir Analiz

Post-Panopticon Age: An Analysis on the Digitalization of Surveillance, and the Privacy of Online Identity

Dr. Öğr. Üyesi Şebnem Özdemir[1]

Başvuru Tarihi: 22.11.2019
Kabul Tarihi: 22.06.2020
Makale Türü: Derleme

Öz

Gözetim, insanlık tarihi boyunca bir güç ve iktidar aracı olmuştur. Ağırlıklı olarak Bentham ve Foucault ile anılan Panoptikon, gözetim olgusu ile en çok anılan tasarım olup pek çok teorisyenin ilgisini çekmiş ve çekmektedir. Panoptikon'dan yola çıkarak zaman içerinde Süper-panoptikon, Sinoptikon, Omniptikon, Katoptikon gibi pek çok terim de yazına girmiş, gözetim çalışmaları yıllar içinde çok daha fazla zenginlik kazanmıştır.

Dijital iletişim araçlarının gün geçtikçe insan hayatına daha çok girdiği post-panoptikon çağında bu araçların kullanımı vasıtası ile yapılan gözetim zaman zaman temel hak ve özgürlükleri de tehdit eder duruma gelmiştir. Çoğu insanın zaman zaman bilinçsizce ve çoğu zaman gönüllü olarak gözetleyenlere teslim ettiği veriler insanların sadece kendi mahremiyetlerini ve güvenliklerini değil içinde bulundukları toplumları da tehdit edebilmektedir. Bu tehditlerin başında ayrımcılık, dışlama, zorlama, edilgenleştirme ve korku ve güvensizliğin gittikçe artması sayılabilir. Gerek politika yapıcılar gerekse işletmeler tarafından yapılan gözetim yeni bir tür gelir aracı yaratmıştır ki o da "veri"dir. Gözetleme kapitalizminde veri artık yeni bir para birimidir. Veri, alınabilir, satılabilir, değer kazanabilir ya da kaybedebilir, yatırım ve ticareti yapılabilir bir varlık haline gelmiştir.

Bu çalışma, Panoptikon analojisi üzerinden, dijital iletişim araçları vasıtası ile hangi verinin ne şekilde elde edildiği ve hangi amaçlarla kullanıldığı, dijital gözetlemenin sıradan insanlar ve genel olarak toplumsal yapı için nasıl tehdit oluşturabildiğini farklı örnekler ve vakalar ile destekleyerek incelemeyi amaçlamaktadır.

Anahtar Kelimeler: *Panoptikon, Gözetleme, Gözetim, Sürveyans*

[1] Sivas Cumhuriyet Üniversitesi İİBF İşletme Bölümü, **SebnemOzdemirTR@gmail.com**, ORCID: 0000-0003-0421-0833

Abstract

Surveillance has been a mean for gaining power throughout human history. Panoptikon, which is mainly referred to Bentham and Foucault, is the most mentioned design with the surveillance phenomenon and attracts the attention of many theorists. Over time, many terms such as Super-panopticon, Synopticon, Omnipticon, Catopicon have entered the literature, and surveillance studies have gained much importance over the years.

In the post-panopticon era, where digital communication tools are increasingly used, surveillance through the use of these tools has sometimes threatened fundamental human rights and freedoms. The data that most people sometimes hand over to the observers unconsciously and often voluntarily may threaten not only their own privacy and security, but also the communities which they live in. Among these threats are discrimination, exclusion, coercion, passivisation, and increasing fear and insecurity. Surveillance by both policy makers and businesses has created a new type of revenue instrument, which is "data". In surveillance capitalism, data is a new type of currency. Data has become an asset that can be bought, sold, raised or decreased in value, invested, and traded.

The aim of this study is to examine which data is obtained through digital communication tools for what purposes, and how digital surveillance may threaten ordinary people and societies in general by using different examples and cases through the Panopticon analogy.

Keywords: *Panopticon, Surveillance*

"Bene qui latuit bene vixit"
(Gizlilik içinde yaşayan güzel yaşar)
Ovidius, Tristia, 3.4.25.

Giriş

Dünya Bankası verilerine göre hâlihazırda dünyada 1 milyar insanın resmi kimlik belgesi bulunmamaktadır (Identification For Development - World Bank, 2019). Resmi kimlik belgesi sahibi olmayan bu insanlar, oy verme, banka hesabı açma, pasaport alma, sosyal güvenlikten faydalanma, eğitim kurumlarına kayıt olma, işe girme ya da iş kurma, hatta telefon hattı alma vb. pek çok temel haktan faydalanamamaktadır. Bu durum bireyler kadar devletler açısından da büyük bir sorundur, zira devletler de bu sebeple vergi kaybına uğramakta, sağlık, hukuk, eğitim gibi hizmetleri etkili şekilde planlayamamakta, sınır güvenliğini ve iç güvenliği yeterince sağlayamamaktadır. Yaklaşık 1 milyar kişinin resmi kimlik belgesinin olmadığı dünyada, bir yandan da dijital teknolojinin geldiği nokta sorgulanmakta, dijital araçların nimetleri ve külfetleri tartışılmakta, dijital araçlar ile ilgili yeni kanunlar, düzenlemeler ve uygulamalar yürürlüğe girmektedir. Türkçeye "dijital eşitsizlikler" ya da "sayısal uçurum" olarak çevrilen "digital divide" kavramı bir anlamda bu durumu betimleyen bir kavramdır: bir tarafta resmi

kimlik belgesi olmadığı için temel haklardan bile yararlanamayan insanlar diğer taraftan ise teknolojinin nimetlerinin onlar için külfet haline geldiği insanlar.

Günümüzde dijital iletişim araçlarının yanı sıra biyometri, şeylerin interneti, akıllı kartlar, blok zinciri, bulut bilişim ve benzeri pek çok yeni dijital teknoloji kullanımdadır- ki bu araçlar zaman zaman bir nev'i post-panoptik gözetim aygıtı haline de gelebilirler. Bu araç ve teknolojiler, sayısallaştırmada kesinlik ve tasarruf başta olmak üzere pek çok avantaj sağlamakta, bununla beraber bu teknolojilerden kaynaklı riskler de insanlar ve hükümetler için endişe kaynağı olabilmektedir. Verinin gittikçe daha fazla değer kazandığı dünyada dijital gözetim (sürveyans) de gittikçe yükselen bir endişe haline gelmektedir.

Bu çalışma "post-panoptikon" olarak da nitelendirilen panoptikon sonrası gözetim kavramını ayrıntılı olarak değerlendirmeyi amaçlamaktadır. Çalışma kapsamında, özellikle 21. Yüzyıl'ın başlangıcından itibaren günümüz insanının gündemine giren ve gittikçe artan şekilde endişelere neden olan dijital gözetimin, sıradan insanların neredeyse fark edemeyecekleri bir hız ve farklı yöntemlerle insanların hayatına sızması ve dijital gözetim vasıtası ile elde edilen verinin güç ve iktidar kazanma amacıyla nasıl kullanıldığı incelenecektir.

Gözetleme ve Panoptikon

"Halka şeklinde bir bina ve ortasında bir kule ve kuleden halkanın iç cephesine bakan geniş pencereler… Kuleye bakan bina hücrelere ayrılmıştır. Hücrenin her biri bina boyunca derinlemesine uzanır. Bu hücrelerin iki penceresi vardır. Biri içeriye doğru açıktır, kulenin pencerelerine denk diğer, diğeri dışarıya bakarak, ışığın bir baştan bir başa hücreyi kat etmesini sağlar. Bu durumda merkezi kuleye bir gözlemci yerleştirmek ve her bir hücreye bir deli, bir hasta, bir mahkûm, bir işçi ya da bir öğrenci kapatmak yeterlidir." (Foucault, 2007, s. 86).

Panoptikon, genellikle Foucault ile anılan bir kavram olsa da aslen Jeremy Bentham tarafından ortaya atılmıştır[2]. Bentham, panoptikonu bir ıslah merkezi, bir hapishane olarak düşünmüş, yapı içindekilerin her daim izlendiklerini hissedecekleri bir tasarım öngörmüştür. Foucault başta olmak üzere, Haggerty & Ericson (2003), Deleuze ve Guattari (1983), Bogard (1996) ve daha pek çok kuramcı bu kavram üzerinde fikir üretmiş, kavramın gelişimine katkıda bulunmuşlardır.

Gözetim kavramına giriş yapmadan önce kavrama kısaca açıklama getirmekte fayda vardır. Gözetim ya da sürveyans, Fransızca "surveillir" kelimesinden (survaillance olarak) İngilizceye ve diğer dillere geçmiştir. Gözetim kavramı, aslen 3 ana başlık altında incelenmektedir: Sürveyans (survaillance), Suveyans (sousveillance) ve Ekiveyans (equiveillance)[3]. Sürveyans'ta ("sur" Fransızca "üstünde" anlamına gelen bir edattır), izleyen, izlenenlerin üzerinde bir pozisyonda konumlanmıştır. Suveyans'ta ("sous" Fransızca "altında" anlamına gelen bir

[2] Pek çok kaynakta Panoptikon tasarımının Jeremy Bentham'ın kardeşi Samuel Bentham'ın fikri olduğu yer almaktadır.
[3] "Sousveillance" ve "equiveillance" terimlerinin Türkçe karşılıkları bulunmadığı için yazar tarafından "sousveillance" terimi için "suveyans", "equiveillance" terimi için "ekiveyans" kelimeleri kullanılmıştır.

edattır) izleyenler, izlenenlerin altında bir pozisyonda konumlanmıştır. Ekiveyans'ta ("equivalence" Fransızca "denklik" anlamına gelen bir isimdir) ise herkes herkesi izleyebilmektedir [4].

Başta felsefe, iletişim, sosyoloji, psikoloji olmak üzere pek çok disiplinde kendine yer bulmuş panoptikon kavramı zamanla sinoptikon ve omniptikona evrilmiştir. Panoptikonda tek taraflı, hiyerarşik, asimetrik ve zorlamaya dayalı bir denetleme söz konusu iken sinoptikon ve omniptikonda rızaya hatta psikolojik tatmine dayalı bir gözetleme söz konusudur. Sinoptikonda, çoğunluk az sayıda kişiyi izlemekte, izlenen azınlığın yaşam biçimi, davranışları ve söylemlerine göre kendi hayatlarına yön vermekte, bir nev'i kendilerini disipline etmektedir. Sinoptikonda kitle iletişim araçlarının etkisi kuşkusuz ki büyüktür. Farklı sosyo-ekonomik statü, yaş, kültür ve tercihlere sahip insan kitleleri, başta televizyon olmak üzere kitle iletişim araçları vasıtası ile az sayıda kişi tarafından oluşturulan ve/veya biçimlendirilen mesajlara maruz kalırlar. Dijital iletişim araçlarının insan hayatına daha fazla girmesi ile de sinoptikondan omniptikona geçilmiştir. Gözetim çalışmalarına sonradan dâhil olan Katoptikon kavramında ise Panoptikon'da yer alan gözetleme kulesinin yerini aynadan oluşmuş bir kule almaktadır ("Catoptrics" ayna vasıtası ile ışık ve görüntü yansıtan sistemleri ifade eden bir terimdir) (Ganascia, 2009).

Görüldüğü gibi, gözetim olgusu üzerinde yapılmış çalışmalarda, kullanılan terminoloji bir hayli geniştir. Bununla beraber gözetim denilince akla ilk olarak "Panoptikon" terimi gelmektedir. Bu sebeple, bu çalışma kapsamında, gözetim olgusu irdelenirken, gözetim ile adeta müsemma olmuş "Panoptikon" terimi kullanılacaktır.

[4] Paragrafta geçen terimlerle ilgili daha fazla bilgi edinmek için, Steve Mann'ın çalışmalarının incelenmesi faydalı olacaktır (ör: http://wearcam.org/anonequiveillance.htm)

Tablo 1. Başlıca Gözetim Çalışmaları[5]

Panoptikon	(Panopticon)	Bentham, 1995
Disiplin toplumu, bakış ve biyo-güç	(Disciplinary society, the gaze and bio-power)	Foucault, 1977, 1998
Sürveyans toplumu, yeni sürveyans ve maksimum güvenlik toplumu	(Surveillance society, the new surveillance and maximum security society)	Marx, 1985, 2015
Ağ genişletme	(Net widening)	Cohen, 1985
Dosya toplumu	(Dossier society)	Laudon, 1986
Veri gözetleme	(Dataveillance)	Clarke, 1988
Süper Panoptikon	(Super-panopticon)	Poster, 1990
Denetim Toplumu	(Society of control)	Deleuze, 1992
Ulus devlet anamorfizisi	(L'anamorphose de l'etat-nation)	Palidda, 1992
Panoptik sıralama: Kişisel Bilginin Politik Ekonomisi	(Panoptic sort)	Gandy, 1993
Minimum güvenlik toplumu	(Minimum security society)	Blomberg, 1987
Sinoptikon	(Synopticon)	Mathiesen, 1997
Güvenlikleştirme	(Securitization)	Buzan vd., 1998
Telematik toplum	(Telematic society)	Bogard, 1996
Tekno-polislik	(Techno-policing)	Nogala, 1995
Şeffaf toplum	(Transparent society)	Brin, 1998
Maksimum gözetim toplumu	(The maximum surveillance society)	Norris and Armstrong, 1999
Akışkan modernite	(Liquid modernity)	Bauman, 2000
Bilgi imparatorluğu	(Information empire)	Hardt and Negri, 2001
Sürveyans topluluğu	(Surveillant assemblage)	Haggerty and Ericson, 2006
Post-panoptikon	(Post-panopticon)	Boyne, 2000
Cam kafes	(Glass cage)	Gabriel, 2005
Ban-optikon	(Ban-opticon)	Bigo, 2006
Yüce Gözetleme	(High policing)	Brodeur and Leman-Langlois, 2006
Mekânsız ve zamansız bilgi işleme	(Ubiquitous computing)	Greenfield, 2006
21. Yüzyıl izleme	(Ubereveillance)	Michael vd., 2008
Ortamsal zekâ	(Ambient intelligence)	Wright vd., 2008
Güvenli toplum	(Safe society)	Lyon, 2007
Sınır tanımayan sürveyans	(Thick and thin surveillance)	Torpey, 2007

Kaynak: (Marx, 2015, s. 733)

Post-Panoptikon ve Dijital Çağda Gözetim

Gözetim (sürveyans) aslında tamamıyla faydasız değildir. Çevrimiçi eylemlerimiz sırasında şirketler ve/veya makinelerle isteyerek ya da istemeyerek paylaştığımız bilgiler, edinilen bu bilgilerin işlenmesi sonucu elde edilen veri ve içgörüler bazı alanlarda kullanıcının lehinedir; örneğin, daha önce satın aldığınız kitaba benzer bir kitabın önerilmesi, ya da kişiye özel içeriklerin kişiye gösterilmesi sonucu kişinin zaman kazanması ve psikolojik olarak daha fazla tatmin olması gibi. Bununla beraber pek az kullanıcının, dijital etkinlikleri sırasında

[5] Liste Gary T. Marx tarafından oluşturulmuş olup, işbu çalışmanın yazarı tarafından Türkçeye çevrilmiştir. Bazı çalışmaların Türkçesi henüz mevcut olmadığından çeviride yazar tarafından uygun görülen kelime ve/veya ifadeler kullanılmış olup, çalışmaların farklı çevirileri de (hâlihazırda veya gelecekte) bulunabilir.

oluşturdukları dijital gölgelerin ne şekilde işlendiği, ne tür amaçlar için kullanıldığı ve kendileri ve toplum açısından ne gibi maliyetleri olacağı konusunda fikri vardır. Dijital etkinliklerin ağırlıklı olarak sosyal ağlar üzerinden gerçekleştiği düşünüldüğünde en temel soru kişilerin sosyal ağlarda neden paylaşım yaptıkları olacaktır. Türk ve Demirci (2016), sosyal ağlarda yapılan paylaşımlar ve gözetleme arasında bir bağ olduğunu belirtmektedir:

> "*Yeni kamusal alan olan sosyal ağlar, daha özgür bir ortam sunmakta, gözetleme (merak) ve gözetlenme (beğeni) kültürünün kullanıcılara daha çok ötekine ulaşma daha çok gözetleme imkânı vermektedir. Bireyler, sosyal medyanın onlara sunduğu özgür ortamda, kendi gibi olan diğerlerinin paylaşımlarındaki özgürlüğü ve mahremiyetinin dönüşümünü görmesiyle hem merak tatmini sağlamakta hem de gündelik yaşamda toplumsal baskıdan kendini soyutladığı oranda yabancılarla paylaşmaktan çekindiği bilgi ve görüntüleri takipçileri ile gönüllü olarak paylaşarak kendini tek ve biricik olarak kurmaktadır. Beğenilme, gözetleme ve gözetlenme sanal dünyanın temelini oluşturmaktadır. Bireyler; yaptıkları paylaşımlarına aldıkları olumlu tepkiler, beğeni ve takipçi sayısı ile doğru orantılı olarak kendi değerini ölçmektedirler."* (Türk & Demirci, 2016).

İnsanoğlu yeni kamusal alanlarda sanal olarak kendini var etmekte, başkalarına kendisini gözetleme iznini gönüllü olarak verirken karşılığında psikolojik tatmin sağlamaktadır. Bu geçici mutluluğun ve özgürlük hissinin "bedava" olmadığından ise kuşkusuz ki pek az insan haberdardır.

Panoptikon Vakfı, Nisan 2009 yılında kurulmuş Polonya merkezli bir kuruluş olup, vakfın misyonu, değişen teknoloji ile paralel olarak artan gözetime karşı temel hak ve özgürlükleri korumaktır (Panoptykon Foundation, 2019). Panoptikon Vakfı, Gözetim Toplumunun 7 günahını şu şekilde açıklamaktadır:

1. Gizliliğe müdahale
2. Ayrımcılık ve dışlama
3. Sistem hataları
4. Artan korku, güvenin aşınması
5. Sorunları çözmek yerine maskeleme
6. Sorumluluğun dağılımı
7. Etik yerine zorlama

Gözetim Toplumunun yedi günahı şu şekilde değerlendirilebilir:

1. Gizliliğe Müdahale: Günümüzde şirketlerin ya da devletlerin günlük hayatta attığımız her adımda bizi izleyebilme imkânları bulunmaktadır. Akıllı telefonlar, akıllı kartlar, kapalı sistem kameralar, çevrimiçi işlemler ve daha pek çok aktivite devlet ve şirketlere veri sağlayabilmektedir. Kişiler ise çoğunlukla bu verilerin toplandığından haberdar olmamakta, haberdar olsalar dahi, verilerin kimler tarafından nasıl ve ne amaçla kullandıklarını bilmemektedirler. Öte yandan, hükümetler ve şirketler kişilerin hayatı

hakkında gittikçe daha fazla şey bilir hale gelmekte - bu yüzden de bilgi asimetrisi büyümektedir (Panoptykon Foundation, 2019).

2. Ayrımcılık ve Dışlama: Günümüzdeki teknolojik imkânlarla, işlenen veriler kişileri pek çok özelliğe göre kategorize edebilmektedir. Kişilerin cinsel tercihlerinden sosyoekonomik seviyelerine, ilgi alanlarından siyasi eğilimlerine kadar pek çok alanda sınıflama yapmak mümkündür. Elde edilen ve işlenen veriler zaman zaman ayrımcılığa veya dışlamaya sebep olabilmektedir.

3. Sistem Hataları: dijital verilerin toplanması ve işlenmesi makineler aracılığı ile yapılmaktadır ve makineler ve sistemler de (henüz) kusursuz değildir. Algoritmaların kişiler ile ilgili yaptığı hatalar, söz konusu kişiler için fiziksel, duygusal ya da maddi pek çok soruna sebep olabilmektedir. Sistem hatalarının maliyeti üzerine güzel bir örnek Gillian Brockell isimli bir kullanıcının 11 Aralık 2018'de Twitter'da paylaştığı "Algoritmalarınız Çocuğumu Kaybettiğimi anlamadı mı?" temalı açık mektuptur. Gillian Brockell açık mektubunda şunları yazmaktadır:

"Sevgili Teknoloji Şirketleri,

Hamile olduğumu bildiğinizi biliyorum. Bu benim suçum, #30haftalık, #bebektekmeledi gibi instagram hashtaglerine direnemedim. Salak ben… Hatta bir iki kez Facebook'ta hamile giysisi reklamlarına bile tıkladım. Bebeğimin doğumuna az bir zaman kala yaptığım partiye gelen arkadaşlarıma yürekten ettiğim teşekkürü, Arizona'dan gelen görümcemin fotoğraflarını görmüşsünüzdür. Hatta iddiaya girerim Google'da hamileliğime yönelik yaptığım aramaları görebilirsiniz. Amazon size hamile olduğumu öğrendiğim gün olan 24 Ocağı bile söyleyebilir. Hesabımı o gün açmıştım. Peki, aynı zamanda "Bunlar braxton kasılmaları mı? "ve "Bebek hareket etmiyor" aramalarımı görmediniz mi? Benim gibi aktif bir kullanıcının 3 gün boyunca sessiz kaldığı dikkatinizi çekmedi mi?

"Kalp kırıldı", "Ölü doğan", "Problem" gibi anahtar kelimeler ve arkadaşlarımdan gelen binlerce ağlama emojisini görmediniz mi? Bu sizin takip edebildiğiniz bir şey değil mi?

Anlayacağınız gibi sadece ABD' de yılda 26 bin çocuk ölü doğuyor, sizin dünya çapındaki kullanıcılarınız arasında ise milyonlarca…

Size hastaneden dünyadaki en boş ellerle dönünce sosyal medyanın nasıl bir yer olduğunu anlatmama izin verin. Günlerinizi yatakta hıçkıra hıçkıra ağlayarak geçirirken bir sonraki ağlama krizinden önce birkaç dakikalık dikkat dağınıklığı için telefonu eline aldığında, şok edici bir şekilde her şey sanki bebeğin hayattaymış gibi.

Ve biz milyonlarca kalbi kırık insan, 'Bu reklamı görmek istemiyorum'a tıklayıp, 'Neden?' sorusuna, korkunç gerçek olan 'Benim ile alakalı değil' cevabını verdiğimizde sizin algoritmanızın ne karar verdiğini biliyor musunuz? Sanki doğum yapmışsınız gibi mutlu bir sonuç bekliyor ve

sizi en iyi emzirme sutyeni (Göğüslerimde lahana yaprakları var çünkü tıp biliminin sütünüzü durdurmak için sunduğu en iyi yöntem bu), bebeği bütün gece uyutacak numaralar (onun ağlamasını duymak için her şeyi verirdim) ve bebeğinizle büyüyecek bebek arabası (benimki her zaman 1,8 kg olarak kalacak) gibi reklamlara boğuyor.

Yaşanan onca şeyden sonra bir darbe de Experion'dan geliyor. Onun asla sahip olamadığı kredisini takip etmek için beni teşvik eden bir spam maili: "Çocuğunuzun kaydını bitirin."

Teknoloji Şirketleri, lütfen sizden rica ediyorum, eğer benim hamile olduğumu, doğum yaptığımı fark edebilecek kadar zeki iseniz bebeğimin öldüğünü fark edecek kadar da zekisinizdir. Bana buna uygun reklam yapın ya da hiç yapmayın.
Saygılarla Gillian" (Tanış, 2018).

Dear Tech Companies:

I know you knew I was pregnant. It's my fault, I just couldn't resist those Instagram hashtags - #30weekspregnant, #babybump. And, stupid me!, I even clicked once or twice on the maternity-wear ads Facebook served up.

You surely saw my heartfelt thank-you post to all the girl friends who came to my baby shower, and the sister-in-law who flew in from Arizona for said shower tagging me in her photos. You probably saw me googling "holiday dress maternity plaid" and "babysafe crib paint." And I bet Amazon even told you my due date, January 24th, when I created an Amazon registry.

But didn't you also see me googling "is this braxton hicks?" and "baby not moving"? Did you not see the three days of silence, uncommon for a high-frequency user like me? And then the announcement with keywords like "heartbroken" and "problem" and "stillborn" and the two-hundred teardrop emoticons from my friends? Is that not something you could track?

You see, there are 26,000 stillbirths in the US every year, and millions more among your worldwide users; and let me tell you what social media is like when you finally come home from the hospital with the emptiest arms in the world, after you've spent days sobbing in bed, and pick up your phone for a couple minutes of distraction before the next wail. It's exactly, crushingly, the same as it was when your baby was still alive. Pea in the Pod. Motherhood Maternity. Latched Mama. Every goddam Etsy tchotchke I was planning for the nursery.

And when we millions of brokenhearted people helpfully click "I don't want to see this ad," and even answer your "why?" with the cruel-but-true "It's not relevant to me," do you know what your algorithm decides, Tech Companies? It decides you've given birth, assumes a happy result, and deluges you with ads for the best nursing bras [I have cabbage leaves on my breasts because that is the best medical science has to offer to turn your milk off], tricks to get the baby to sleep through the night [I would give anything to hear him cry at all], and the best strollers to grow with your baby [mine will forever be 4 pounds, 1 ounce].

And then, after all that, Experian swoops in with the lowest tracking blow of them all: a spam email encouraging me to "finish registering your baby" (I never "started" but sure) to track his credit throughout the life he will never lead.

Please, Tech Companies, I implore you: If you're smart enough to realize that I'm pregnant, that I've given birth, then surely you're smart enough to realize that my baby died, and can advertise to me accordingly, or maybe just maybe, not at all.

Regards,
Gillian

Kaynak: (Brockell, 2018)

Şekil 1. Gillian Brockell'in 11 Aralık 2018'de Twitter Üzerinden Teknoloji Şirketlerine Yazdığı açık Mektup

4. Artan Korku, Güvenin Aşınması: Gözetleme, bir tehdidin var olduğu varsayımından beslenir. Bu tehdit bazen gerçekten vardır, bazen ise sadece bir varsayımdan ibarettir. Tehdit ihtimalinden doğan rahatsızlık, gözetim ve korunma ihtiyacı doğurur. Ancak bu, çoğu zaman bitmek bilmez bir döngüye sebep olmakta, daha çok gözetleme daha çok güvensizlik, daha çok güvensizlik daha çok gözetime yol açmaktadır.
5. Sorunları Çözmek Yerine Maskeleme: Gözetlemenin, bazı sosyal problemlere çözüm olma anlamında faydalı olduğu düşünülebilir. Örneğin çevrimiçi bazı içeriklerin algoritmalar tarafından engellenmesi özellikle (çocuk, ergen gibi) bazı kesimlerin korunması anlamında olumlu olabilir. Bununla beraber bu tür palyatif çözümler gerçek sorunu ortadan kaldırmamakta sadece maskelemektedir. Örneğin; Temmuz 2019 itibarı ile dünya çapında endekslenen toplam web sitesi sayısı 5.83 milyar sayfadır (World Wide Web Size, 2019). Bununla beraber, bazı tahminlere göre, Derin Ağ'ın (Deep Web) bu sayının yaklaşık 400 ila 500 katı hacimde olduğu tahmin edilmektedir (Thompson, 2015). Derin Ağ'ın yasadışı içerik paylaşan kısmı ise Karanlık Ağ (Dark Web) olarak adlandırılmaktadır. Karanlık Ağ'ın en bilinen sitelerinden biri İpek Yolu (Silk Road) kapandığı tarihe kadar milyarlarca dolarlık işlem hacmine ulaşmış, uyuşturucudan organa, fuhuştan kiralık katil hizmetine kadar pek çok işleme aracılık etmiştir.
6. Sorumluluğun Dağılımı: Gözetlemenin psikolojik etkilerinden biri çoğulcu cehalet (pluralistik ignorance) ve seyirci kalma etkisini (bystander effect) tetiklemesidir. Gözetlemenin olduğu bir ortamda kişilerin inisiyatif alma ihtimali azalır, kişiler yanlış olduklarını düşündükleri uygulamalara, fikirlere, olaylara karşı pasifize olurlar.
7. Etik Yerine Zorlama: Gözetim, ahlaki değerlerin / iç değerlerin yerine denetimi koyar. Kişi bir eylemi yanlış olduğuna inandığı için değil gözetlemeye takılmamak için yapmaktan kaçınır hale gelir.

Teknoloji akıl almaz bir hızla ilerlerken, çoğunluğu dijital okuryazar olmayan pek çok insan bir dijital panoptikonda yaşadıklarını bilmeksizin dijital araçları kullanmakta, bu gözetlemeye karşı insanların temel hak ve özgürlüklerini korumak ise kısıtlı sayıda, gönüllü kişi ve kurumlara düşmektedir.

Veri İzleri ve Dijital Gölgeler

Gözetleme eskiden fiziksel, tercihen de kapalı ortamlarda yapılırken günümüzde sanal ve veri odaklı olacak şekilde evrilmiştir. Dijital ortamlarda yapılan paylaşımlar, başta reklamcılar olmak üzere pek çok şirket ve devletler için oldukça değerlidir. Özellikle sosyal medyada yapılan paylaşımlar devletler, kişiler ve şirketlerin kolaylıkla ulaşabildiği paylaşımlar olup, sosyal medyanın bir kamusal alan olup olmadığı sıklıkla tartışılmaktadır. Kamusal alan tartışmasında, kavramın tanımlarında ortaya çıkan en önemli unsurlardan bir tanesi de "özel alan" kavramıdır (Çalışkan, 2014). Kişinin, paylaştığı içerik kendi özeli ile ilgili olsa bile, içeriği paylaştığı mecranın kamuya açık olup olmamasının verinin elde edilebilirliğinin meşruluğuna işaret ettiğini savunan görüşler de bulunmaktadır. Sanal ortamda yapılan paylaşımın saati, alışveriş yapılan siteden alınan giysi, hastalıklarla ilgili yapılan arama ya da çevrimiçi sitelerde dinlenilen müzik gibi -paylaşanın kişisel eylemlerini oluşturan- pek çok rutin işlem özellikle şirketler için

birer veri olmaktadır. Bu tür işlemler sırasında yaratılan her türlü bilgi, veri izi (data trace) olarak nitelendirilmektedir. Veri izlerinin bir araya getirilip anlamlı bir bilgi edinilmesi sonucu da dijital gölgeler oluşur.

Bruce Schneier, Veri ve Dev (Data and Goliath) isimli kitabında 6 tür veriden bahsetmektedir:

- *"Servis verileri: Kullanmak için bir sosyal paylaşım sitesine verdiğiniz verilerdir. Hangi site olduğuna bağlı olarak, bu veriler yasal adınızı, yaşınızı ve kredi kartı numaranızı içerebilir.*
- *Açıklanan veriler: Blog yazıları, fotoğraflar, mesajlar ve yorumlar gibi kendi sayfalarınızda yazdığınız verilerdir.*
- *Güvenilen veriler: Başka kişilerin sayfalarına yazılan verilerdir. Bu tür veriler, temelde açıklanan verilerle aynı tür verilerdir, tek farkla; bu tür veriler kullanıcı tarafından bir kez yayınlandığında, kullanıcı veriler üzerinde artık kontrol sahibi olamaz, ancak diğer kullanıcı bu verileri kontrol edebilir.*
- *Tesadüfi veriler: Başkalarının sizinle ilgili yayınladığı verilerdir. Sizin hakkınızda bir başkasının yazdığı bir paragraf veya başkasının çektiği ve gönderdiği bir resim bu tür verilere örnek gösterilebilir. Bu tür verilerin üzerinde herhangi bir kontrolünüz olamayacağı gibi verilerin yaratıcısı da siz değilsinizdir.*
- *Davranışsal veriler: Sitenin, sizin kiminle, ne yaptığınızı izleyerek alışkanlıklarınız hakkında topladığı verilerdir.*
- *Türetilmiş veri: Sizin hakkınızda tüm diğer verilerden çıkarılan verilerdir. Örneğin, arkadaşlarınızın % 80'i kendilerini eşcinsel olarak tanımlanırsa, muhtemelen siz de eşcinselsinizdir."* (Schneier, 2016, s. 143).

İnsanoğlu, tarih boyunca servet ve iktidar için savaşmıştır. Yuval Noah Harari'nin, 21. Yüzyıl İçin 21 Ders isimli kitabında belirttiği gibi eskiden toprak için savaşan insanlık modern çağda makineler ve fabrikaların kontrolüne odaklanmıştır (s.84). 21. Yüzyılda ise insanoğlunun odak noktası veri olacaktır. Harari, günümüz insanının hâlihazırda veriye bakış açısını ise şu şekilde ifade etmektedir:

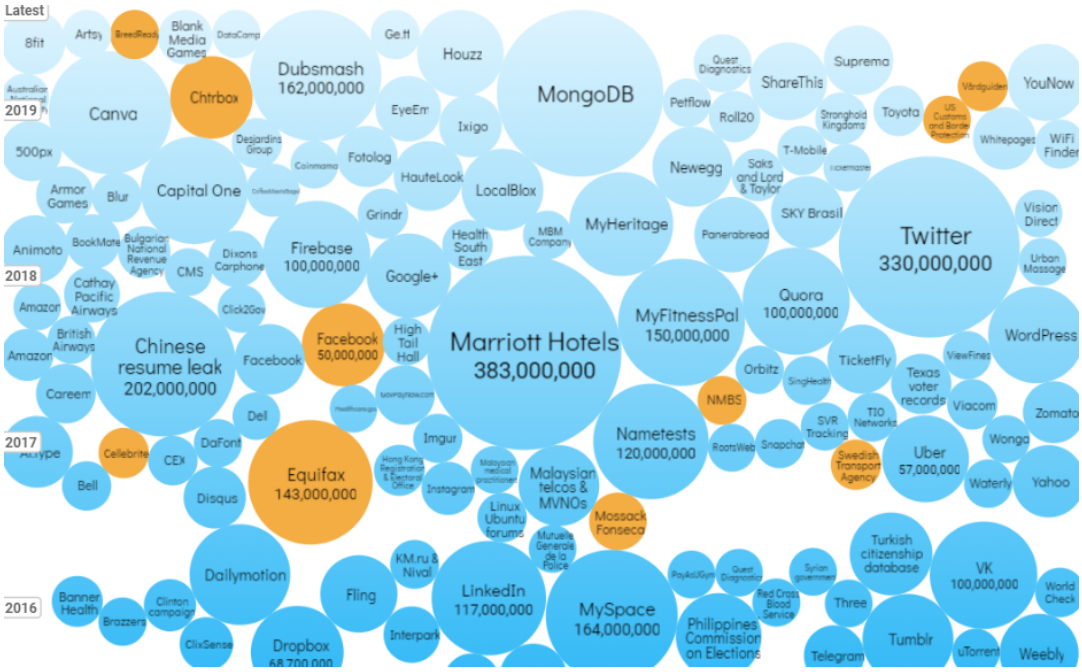
> "*Günümüzde insanlar en değerli varlıklarını yani kişisel verilerini ücretsiz elektronik posta hizmetleri ve komik kedi videoları karşılığında teslim etmekten son derece memnun. Bu durum, ne yaptığının farkında olmadan koca toprakları üç beş renkli boncuk ve ıvır zıvır karşılığında Avrupalı emperyalistlere satan Afrika ve Kuzey Amerika yerlilerinin durumuna benziyor biraz."* (Harari, 2018, s. 85).

Shoshana Zuboff da, veriyi "yeni petrol" olarak tanımlamaktadır. Zuboff, "Sürveyans (Gözetleme) Kapitalizmi" kavramını ortaya atarak kavramı şu şekilde açıklamaktadır:

> "*Sürveyans kapitalizmi, insan deneyimini bedava bir hammadde olarak, tek taraflı şekilde davranışsal verilerin eldesi sürecine sunmaktadır. Bu verilerin bir kısmı ürün veya hizmet iyileştirmesinde kullanılır, geri kalan kısmı ise tescilli bir davranışsal fazlalık (behavioral*

surplus) olarak ilan edilmek suretiyle "makine zekâsı" olarak bilinen ileri üretim süreçlerine beslenir ve şimdi, yakında veya sonraki zamanlarda ne yapacağınızı tahmin eden öngörüler üretmek üzere kurgulanır. Son olarak, bu tahmin ürünleri, "Davranışsal Vadeli Piyasalar" olarak adlandırdığım yeni bir pazarda işlem görmeye başlar. Sürveyans kapitalistleri bu ticaret operasyonları sayesinde oldukça zenginleşmektedirler, çünkü birçok şirket gelecekteki davranışlarımız üzerine bahis oynamaya heveslidir." (Zuboff, 2019, s. 14).

Sıradan bir insanın ayağının onlarca metre altında bulunan petrol yataklarını bilmemesi, bu kaynakların varlığını ancak ürünü kendi gözleri ile gördüğünde, satın aldığında, kullandığında veya ürünün ticaretini yaptığında fark etmesi gibi, yeni petrol olarak nitelendirilen "kendi" verisinin de ederini çoğunlukla çok geç olduktan sonra fark etmesi olasıdır. Pek çok insan ancak veri sızıntıları ya da veri kullanımı ile ilgili olağandışı durumlar, hatta zaman zaman skandallar olduktan sonra verinin öneminin farkına varmakta, ancak kısa bir süre sonra tekrar dijital panoptikondaki konforlu hücrelerine dönmeyi tercih etmektedir.



Kaynak: (Information is Beautiful, 2019)

Şekil 2. Dünyanın En Büyük Veri Sızıntıları

Dijital Mikro-hedefleme (Digital Microtargeting)

Teknolojinin gelişmesi ile birlikte pazarlama ve politik kampanyalarda kullanılan yöntem ve araçlar da değişmektedir. Mikro-hedefleme çoğunlukla siyasette ve pazarlamada rastlanan bir yöntem olmakla birlikte, bireylerden toplanan verilerin işlenmesi vasıtasıyla, hedef alınan kişi ve/veya kişilere uygun, daha terzi işi iletişim yapma olarak nitelendirilebilir.

Pazarlama açısından bakıldığında, mikro-hedeflemenin pazarlama etkinliğini artırmak ve maliyet düşürmek açısından çok değerli olduğu görülebilir. Günümüzde reklam harcamaları

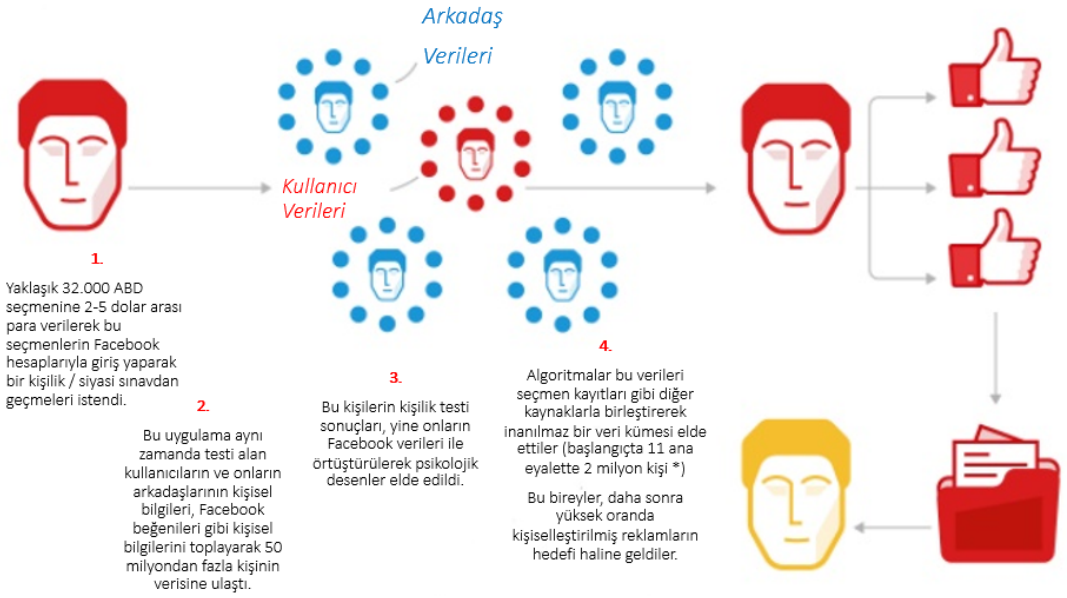
inanılmaz bir boyuta ulaşmıştır. Ünlü sanayici John Wanamaker'ın "Reklama harcadığım paranın yarısı boşa gidiyor. Problem şu ki hangi yarısının boşa gittiğini bilmiyorum (Bradt, 2016)" sözü günümüzde reklam endüstrisinin belki de en büyük problemini ortaya koymaktadır. Tüketicinin maruz kaldığı reklam miktarı her geçen gün artmakta, reklamverenlerin tüketicinin dikkatini çekme olasılığı ise azalmaktadır. Reklam maliyetlerinin doğru hedeflere yönlendirilmesi bu anlamda büyük önem taşımaktadır. Hedeflenmiş reklam (targeted advertising), kişilerin demografik ve davranışsal verilerinin analiz edilmesi suretiyle kişiye özel olarak tasarlanan reklam olarak nitelendirilebilir. Amazon CEO'su Jeff Bezos'un " eğer 4,5 milyon müşterimiz varsa tek bir mağazamız olamaz; 4,5 milyon mağazamız olmalı" (Walker, 1998) sözü hedeflenmiş reklam stratejisinin ne kadar yerinde bir strateji olduğunu ortaya koymaktadır.

Siyasal iletişim açısından da benzer durum söz konusudur. Özellikle genç seçmen kitleleri sosyal ağları yoğun olarak kullanmaktadır ve bu ağlar sayesinde siyasal partiler için sosyal medya, daha ucuz, hızlı ve etkili bir iletişim aracı görevi görmektedir (Kurban, 2014). Mikro-hedefleme, var olan bütçenin daha etkili kullanılmasına, ek olarak hedef kitleyi daha etkili şekilde ikna etmeye olanak verir. Etik ve doğru uygulandığında siyasal mikro-hedefleme oldukça mantıklı bir stratejidir. Bununla beraber mikro-hedeflemenin kötü amaçlı kullanımı da mümkün ve yaygındır.

Uluslararası Demokrasi ve Seçim Desteği Enstitüsü dijital mikro-hedeflemeyi şu şekilde tanımlamaktadır:

> "*Belirli veri kümelerini analiz ederek, siyasi partiler seçmenlerin davranışlarını, fikirlerini ve duygularını ayrıntılı bir şekilde analiz edebilir ve bu da partilerin, seçmenleri gruplar halinde kümelemelerine olanak sağlayabilir. Bu tür kümelere daha sonra seçmenlerin ilgi alanları ve görüşleri doğrultusunda çevrimiçi politik reklamlar gönderilir. Bu çevrimiçi mesajlar yalnızca hedef kümelerdeki seçmenler tarafından görülebilir. Buna dijital mikro-hedefleme denir.*
>
> *Her bir seçmen hakkında elde edilen bilgiler ne kadar ayrıntılı olursa, siyasi kampanyaların hedefi de o kadar doğru olur. Mikro-hedefleme bir siyasi partinin seçmenlerle iletişim kurma biçimini temelden değiştirmeyi vaat eder. Bununla beraber, yeni yasal, etik ve politik boyutların da daha çok anlaşılmasını ve daha çok ele alınması gerektirir. Özellikle dijital mikro-hedefleme, politik kampanyaları yepyeni bir karmaşıklık seviyesine getirmekte ve hem olumlu hem de olumsuz olarak kullanılabilmektedir.*" (International Institute for Democracy and Electoral Assistance, 2018).

Mikro-hedefleme temel olarak 3 aşamadan oluşur. Birinci aşamada kullanıcıların bilgileri elde edilir. Bu bilgiler arasında demografik bilgiler ve bu bilgilere ek olarak daha kişisel bilgiler (ilgi alanları, dini ve/veya siyasi görüş vb.), hatta davranışlar (izlenen filmler, tüketilen yiyecekler, yapılan aktiviteler vb.) de bulunur. İkinci aşamada her bir grup için farklı içerik üretilir. Üçüncü ve son aşamada ise üretilen içeriğin bu mikro hedeflerle iletişimi yapılır. Farklı kullanıcılara ya da gruplara farklı tür ve tarzda mesajlar gönderilebileceği gibi iletişim ortamı da çeşitlilik gösterebilir.



Kaynak: (Hern, 2018)

Şekil 3. Bir Mikro-hedefleme Örneği olarak Cambridge Analytica: 50 Milyon Facebook Kaydı Nasıl Çalındı[6].

Borgesius ve diğerleri dijital politik mikro-hedefleme ile ilgili çalışmalarında özellikle siyasi mikro-hedeflemenin oluşturduğu tehditlerden şu şekilde bahsetmektedir (Borgesius, ve diğerleri, 2018):

- Vatandaşlar açısından; mikro-hedefleme 3 tür tehdit oluşturabilir. Birincisi, vatandaşların (özel hayatlarının) gizliliğini ihlal eder, ikincisi toplanan verinin çalınma ihtimali vardır, üçüncüsü ise toplanan veriler beklenmedik, hatta zaman zaman zararlı olabilecek sonuçlara yol açabilir. Gizlilik tehditlerinin yanı sıra mikro-hedefleme manipülasyon riski de taşımaktadır. Örneğin yabancı düşmanı bir seçmene göçmenlerle ilgili kışkırtıcı bir bilgiyi sosyal medya aracılığı ile iletebilir. Mikro-hedefleme kutuplaşma, dezenformasyon, kışkırtma gibi sonuçlara sebep olabilir. Mikro-hedeflemenin vatandaşlar açısından oluşturduğu bir başka tehdit ise şudur ki, mikro-hedefleme bazı seçmen gruplarına hiç ulaşmayabilir. Bazı seçmen grupları zaman, para ve emek kaybı olarak görüldüğü için iletişimin bir parçası olmaktan çıkarılır. Bu da bu grupların demokratik haklarını zedeleyici bir durumdur.

- Siyasi partiler açısından mikro-hedefleme iki tür tehdit içerir. Birincisi mikro-hedeflemenin maliyeti yüksek olabilir. Partilerin seçmen kayıtlarını toplaması, bu kayıtları muhafaza etmesi, analiz etmesi, bu analizlere göre iletişim tasarlanması ve bu iletişimin yönetilmesi ciddi bir maliyet, bili ve tecrübe gerektirir. İkincisi mikro-hedefleme sebebi ile bazı gruplar (çoğunlukla aracılar) inanılmaz bir güç sahibi haline gelebilirler. Anket şirketleri, dijital şirketler, veri analistleri, dijital iletişimciler vb. kişi ve gruplar bu yapı içerisinde yeni eşik bekçileri konumuna gelebilirler.

[6] Mayıs 2018'de Facebook tarafından yapılan resmi açıklamaya göre çoğu ABD'den olmak üzere yaklaşık 87 milyon kişinin Facebook bilgileri Cambridge Analytica ile uygunsuz şekilde paylaşılmıştır (Facebook Newsroom, 2018).

- Kamuoyu açısından mikro-hedeflemenin temel olarak iki tehdit yarattığı söylenebilir. Birincisi mikro-hedefleme yolu ile seçmenin bazı spesifik konularda yoğun iletişime maruz kalması, seçmenin bu konuyu gerektiğinden fazla önemli bulmasına yol açabilir. Kamuoyu açısından ikinci tehdit ise kamusal tartışmalar boyutudur. Seçmenin sadece bazı konularla ilgili iletişime maruz bırakılması seçmenin görüşlerinin yanlılaşmasına sebep olur. Bu sebeple de kamusal tartışmalar daha az demokratik hale gelir, karşılıklı müzakere süreçleri darbe alır.

Tüm bu tehdit ve açmazlar göz önüne alındığında, mikro-hedeflemenin şeffaf ve etik uygulanmasının önemi ortaya çıkmaktadır. Bununla beraber bu tür çalışmaların kim ya da hangi merci tarafından, nasıl denetleneceği büyük bir sorundur. Hedeflemenin ve hedefleme sonucunda yapılacak iletişimin manipülatif, kışkırtıcı, anti-demokratik ve ayrımcı olmaması için ne tür önlemler alınabileceği kadar bu önlemlerin pratikte uygulanabilirliği de tartışma konusudur. Elde edilen verinin büyüklüğü, veri işlemede kullanılan teknolojilerin birbirinden farklılığı, ülkeden ülkeye değişen yasal düzenlemeler ve daha pek çok etken mikro-hedefleme uygulamalarının denetimini neredeyse imkânsız hale getirmektedir.

Panoptikon ve Netnoğrafya

Türkçe Bilim Terimleri Sözlüğü, etnografyayı (budunbetim), "görece küçük ölçekli teknoloji ve ekonomiye sahip olan, dış dünyadan yalıtılmış budunların bozulmamış kültürlerini betimsel olarak saptayan bilimsel yöntem" olarak tanımlamaktadır (Türkiye Bilimler Akademisi, 2011). Kartarı ise etnografyanın herhangi bir şeyi keşfetme, farklı, değişik, ilginç bir şeyler bulma kaygısının olmadığını; araştırma nesnesini gündelik yaşam rutini içinde anlamaya çalıştığını belirterek şöyle der:

> "*Etnografi araştırma nesnesini gündelik yaşam rutini içinde anlamaya çalışır. Öznenin gündelik yaşamı hem somut hem de soyut bileşenleri içerir. Bir tarafta gündelik yaşamın akışı içinde, farklı bağlamlardaki davranışları, sözleri, görünür etkileşimleri, diğer tarafta duyguları, inançları, söylemleri vardır. Etnografik çalışma bunların her birini tek tek hem de hepsini bütün olarak anlamaya çalışma çabasıdır."* (Kartarı, 2017).

Netruğrafya (Netnografi) ise veri toplama işlemlerinin dijital ortamlarda gerçekleştiği etnografya biçimi olarak tanımlanabilir. Netnografinin, yazında, dijital etnografya, siber etnografya, sanal etnografya, çevrimiçi etnografya, mobil ya da elektronik etnografya vb. isimlerle de anıldığı görülmektedir. Robert V. Kozinets (2010, s. 56) tarafından bilimsel yazına kazandırılan netnografi ile ilgili Kozinets, "…, titiz bir şekilde kullanıldığında, netnografi, araştırmacıya toplumsal tartışmalar gibi doğal olarak ortaya çıkan davranışlar hakkında bir pencere sağlayabilir ve araştırmacıya tartışmalara ve karşılıklı görüşmelere katılma gibi (daha müdahaleci) imkanlar sağlayabilir" demektedir.

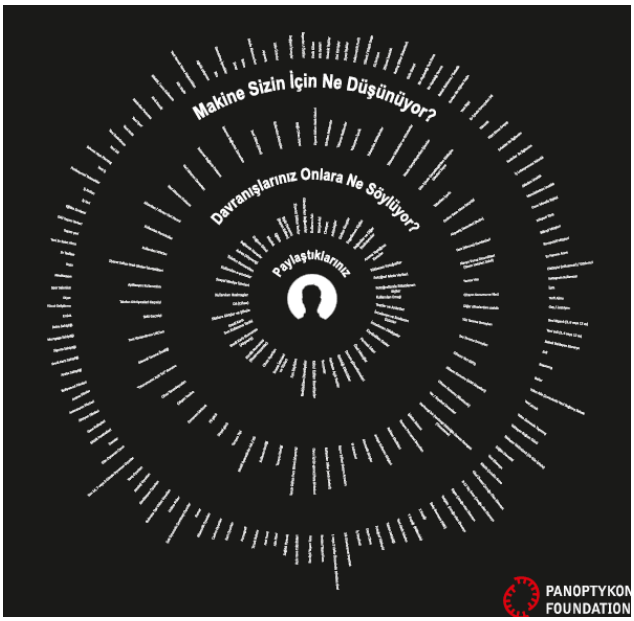
İnternette, sosyal ağlarda, akıllı cihaz aplikasyonlarında, çevrimiçi hizmetlerde ve diğer dijital ortamlarda her saniye milyonlarca terabayt veri paylaşılmaktadır. Paylaşılan bu verinin büyük bir kısmı paylaşımı yapanlar tarafından gönüllü olarak paylaşılmakla beraber paylaşılan bu

verinin nasıl kontrol edildiği paylaşımı yapanlar tarafından çoğunlukla bilinmemektedir. Sosyal dinleme, bilgisayar ortamında, elektronik ve sosyal kanallar aracılığıyla çeşitli ortamlara katılmak, bu ortamları gözlemlemek, yorumlamak ve yanıt vermeyi içeren aktif bir süreçtir (Stewart & Arnold, 2018). Günümüzde pek çok şirket, kurum ve kuruluş tarafından sosyal dinleme yapıldığı bilinmekte hatta sosyal dinleme hizmeti satan şirketler bulunmaktadır.

Panoptikon Vakfı çevrimiçi yapılan paylaşımlar ve bu paylaşımlar sonucu doğrudan ya da dolaylı şekilde edinilen bilgiler ile ilgili bir şema oluşturmuştur. Şemaya göre, kişilerin çevrimiçi eylemleri genel olarak üçe ayrılmaktadır. Birinci tabakada kişinin çevrimiçi platformlarda yaptığı seçimler ve paylaşımlar bulunmaktadır. Kişinin bu veri üzerinde kontrolü vardır. Bu tür veriler, genellikle, kişinin kullanıcı adı, cihaz ayarları, yüklenen fotoğraflar, kabul edilen davetiyeler, ilişki durumu, alışveriş yaptığı ürünler vb. gibi çok temel verilerdir.

İkinci tabakada davranışsal gözlemler bulunmaktadır. Bu tabakada yer alan veriler sayesinde ağırlıklı olarak davranışsal desenler elde edilir. Bu veriler, genellikle kişinin üçüncü kişilerle paylaşmayı pek de tercih etmediği, işletim sistemi, cihaz konumu, ziyaret edilen sitelerin istatistikleri, alınan ve aktarılan veri hacmi, yapılan etkinliğin zaman damgası, tıklanan reklamlar, klavye vuruş desenleri ve yazma hızı, tüketilen içerik vb. verilerdir.

Üçüncü tabakada ise birinci ve ikinci tabaka verilerin algoritmalar tarafından işlenmesi sonucunda çıkan yorumsal veriler yer alır. Birinci ve ikinci tabaka veriler işlenir, gerekli istatistiki analizler yapılır, anlamlı bağlantılar bulunur, veriler diğer kullanıcıların verileriyle karşılaştırılır ve işlenen bu bilgiler ışığında kimliğimiz, gelecekteki tüketim davranışlarımız, içinde bulunduğumuz sosyal, psikolojik, ekonomik vb. durum ve daha birçok çıkarım elde edilebilir. Örneğin, zihinsel hastalık, siyasi ve dini görüş, cinsel tercih, yiyecek tüketimi, emlak satın alma düşüncesi vb. veriler dahi bu algoritmalar tarafında tespit edilebilir. Bu tabakada yer alan veriler çoğunlukla başkaları tarafından bilinmesinin istenmediği, mahrem sayılabilecek verilerden oluşmaktadır.



Kaynak: Yazar tarafından orijinal görselin kullanım izni Panoptykon Foundation'dan (2019) 20 Şubat 2019 tarihinde alınmıştır.

Şekil 4. Dijital Gölgenin 3 Katmanı

Tablo 2. Dijital Gölgenin 3 Katmanı (Liste)

Paylaştıklarınız	**Davranışlarınız Onlara Ne Söylüyor?**	**Makine Sizin İçin Ne Düşünüyor?**
Kullanıcı Adı	Ziyaret Edilen Web Siteleri	Etnik Köken
Gerçek Ad	Görülen Reklamlar	Aile üyeleri
Cinsiyet	Tıklanan Reklamlar	Mesleki İlişkiler
Arkadaşlar	Yok sayılan İçerik	Dini Görüşler
Girilen Gruplar	Yok sayılan Etkileşimler	Siyasi İlişkiler
Engellenen Kişiler	Tıklanan Makaleler ve Gönderiler	Psikometrik Profil
Beğeniler ve Diğer Reaksiyonlar	Sitede Gerçekleştirilen İşlemler	Yüksek / Düşük Saygı
Arama Yaptığınız Konular	Gün İçinde Gerçekleştirilen Etkileşim / Gönderi Sayısı	IQ Seviyesi
Yüklenen Fotoğraflar	Tüketilen İçerik	Zihinsel hastalık
Fotoğraf Meta Verileri	Online Satın Alma Geçmişi	Rating (İtibar Sistemleri)
Fotoğraflarda Etiketlenen Kişiler	Alışveriş Desenleri (Rutin)	Gelir düzeyi
Kullanılan Emoji	Fare (Mouse) Hareketleri	Bir Alışkanlığı Terk Etme
Testler ve Anketler	Klavye Vuruş Dinamikleri (Yazım Hataları Dâhil)	Bir Hastalığı Yenme
İncelenen ve Sıralanan Ürünler	Yazma hızı	Bebek Bekleme / Gebelik
İmzalanan Dilekçeler	Cihazın Konumu ve Yönü	Sevilen Bir Kişinin Kaybı
Kaydedilen Sesler	Diğer Cihazlardan Uzaklık	Yeni İlişki
Parmak İzleri	Yüz Tanıma Sonuçları	Ev İçinde Konuşulan Dil
Özel Mesajlar	Ses Tanıma Sonuçları	Yalnızlık
Durum güncellemeleri	Cihazın Yeri (GPS)	Flört Etme Arayışı
Katıldığı Etkinlikler	Cihazın Konumu (WiFi Sinyalleri)	Erkekler ile İlgilenim
Herkese Açık Yazılar	Cihazın Konumu (Bluetooth)	Kadınlar ile İlgilenim
Yorumlar	Yer / Seyahat Desenleri	İş Lokasyonuna Yakınlık
Kabul Edilen Davetiyeler	Herhangi bir Çevrimiçi Etkinliğin Zaman Damgası (Timestamp)	Aileden Uzaklık
Reddedilen Davetiyeler	İşletim Sistemi	Memleketten Uzaklık
Fan Sayfaları	Tarayıcı Penceresi Boyutları	Uzun Mesafe İlişkisi
Dosya İsimleri ve Türleri	Reklam **k**imlikleri	Müşteri Türü
Cihaz Ayarları	Ardışık Kullanıcı Girişleri	Bilinçli Müşteri
Kimlik Numarası (Rezervasyonlar)	Otomatik Girişler	Kompulsif Müşteri
Kredi Kartı Numarası (Alışveriş)	IP Adresleri	Ev Hanımı Anne
Kredi Kartı Son Kullanma Tarihi	Rapor Edilen Sistem Arızaları	Etkileyici (Influencer) / Gözlemci
Sitelere Girişler ve Şifreler	Kullanılan Diller (web siteleri)	Instagram Kullanıcısı

Dil (Cihaz)	Oyun İçi (In-game) Para Birimleri	İşsiz
Kullanılan Hashtagler	Tercih Edilen Para Birimi (alışveriş)	Terfi Alma
Sosyal Medya İsimleri	Tarayıcı kimliği	Gay / Lezbiyen
Kullanılan e-postalar	Kullanıcı kimliği	Yeni Nişanlı (3, 6 veya 12 ay)
Telefon Numaraları	Mobil Operatörün Adı / ISS	Yeni evli (3, 6 veya 12 ay)
Adres (Alışveriş)	Tarayıcı Tipi	Bebek Bekleyen Ebeveyn
Bağlantılı Hesaplar	Sinyal gücü	Evli
Doğum Günü	Pil gücü	Boşanmış
Meslek	Donanım Sürümü	Bekâr
Eğitim	Çalışan Yazılım	Yakın Aile Çevresinde Yeni Doğmuş Bebek
İlişki Durumu (Beyan Edilen)	Cihaz Tanımlayıcıları	Yeni çocuk
Ziyaret Edilen Yerler	"Oturumumu Açık Tut" durumu	Yakın Zamanda Taşınmış
Gönderilen Bağlantılar	Güvenli Tarama Özelliği	Yaklaşan Doğum Günü
	Tam Yönlendirme URL'leri	Yaklaşan Yıldönümü (30 Gün İçinde)
	SMS Geçmişi	Düğün davetlisi
	Telefon Görüşmeleri Geçmişi	Yeni Ebeveyn
	Aplikasyon Kullanımları	Küçük Çocuklu Anne
	Ziyaret Edilen Web Siteleri İstatistikleri	Okul Öncesi Çocuğu Olan Ebeveyn
	Kullanılan VPN'ler	Erken Okul Çağında Çocuğu Olan Ebeveyn
	Kullanılan Protokoller	8-12 Yaş Arası Çocuğu olan Ebeveyn
	Aktarılan / Alınan Veri Hacmi	Ergen Çocuğu olan Ebeveyn
	Veri Aktarım Frekansı	Yetişkin Çocuğu olan Ebeveyn
	Veri Aktarım Zamanları	Baby Boomers (ABD)
	İnternet Bağlantı Frekansı	X Kuşağı
	İnternet Bağlantısı Zamanları	Y Kuşağı (Millenials)
	Saat Dilimi (Cihaz)	Yeni Akıllı Telefon
	Kullanılan Eklentiler	Tablet Sahipliği
	Bağlı Cihaz Sayısı	Fotoğraf Yükleyici
		Expat Olma
		İş Seyahati
		Sık Uluslararası Seyahat
		1 veya 2 Hafta Öncesinde Dönülen Gezi
		Kentsel Yaşam Tarzı
		Banliyö Yaşam Tarzı
		Açık Hava Etkinlikleri
		Sağlıklı Yiyecek
		Aile Filmi
		Fast Food
		Tırnak Bakımı

Pornografi
Kart Oyunları
Casino Oyunları
Nişancılık Oyunları
Kumar
Çok Oyunculu Çevrimiçi Oyunlar
Online Poker
Bulmaca Tipi Video Oyunları
Simülasyon Oyunları
Strateji Oyunları
Yarış Oyunları
Son 14, 7 veya 3 Günde Oynanan Oyunlar
Dün Oynanan Oyun
Danslar
Müzik Festivalleri
Gece Kulüpleri
Aksiyon Filmleri
Animasyon Filmleri
Anime Filmler
Bollywood Filmleri
Araba Sahipliği
Kredi Kartı Sahipliği
Sigorta Sahipliği
Mortgage Sahipliği
Daire Sahipliği
Emlak
Vücut Geliştirme
Diyet
Spor Salonları
Meditasyon
Koşu
Ağırlık çalışması
Bira
Damıtılmış İçecekler
Şarap
Kahve
Moda Aksesuarları
Alışveriş
Lüks Ürünler
Değişen İnançlar
Başarılar / Ödüller
Dövme veya Piercing
Yeni Dil
Yeni Enstrüman
Yeni Hobi
Yeni Spor
Kaldırılan Parantez
Kırık Kemik

	Gözlük / Lens Kullanımı
	Kilo Kaybı
	Yeni Yemek Yeme Alışkanlıkları
	Ev Tadilatı
	Yeni Ev Satın Alma
	Yaşam yeri
	Eski Yaşam Yerleri
	Eğitim Seviyesi
	İş Yeri
	İş Kolları
	Profesyonel Yetenekler
	Yeni İş

Kaynak: (Panoptykon Foundation, 2019)[7]

Gerek kişiler tarafından gönüllü olarak paylaşılan veriler gerekse algoritmalar tarafından yorumlanarak elde edilen veriler, devletler, pazarlama şirketleri, sigorta şirketleri, bankalar, işverenler, telekomünikasyon şirketleri ve daha pek çok kişi ve kurum için oldukça değerlidir ve bu veriler belli kişi veya kuruluşlarla paylaşılabilir ya da onlara satılabilir. İnsanların üzerinde çok da düşünmeksizin paylaştığı, kendileri ile ilgili pek çok bilgi böylelikle finansal değeri olan bir ürün haline dönüşmektedir. İnsanlar için bir hikâyeden, bir eğlenceden ibaret olan paylaşımlar, bu paylaşımları kullanan kişi ve kurumlar için birer maden gibi işlem görmektedir. Peki, insanlar neden kendi verilerini bu kadar kolay ve fütursuzca paylaşmaktadırlar? Bu sorunun birkaç cevabı vardır. Birincisi pek çok insanın dijital araçlara kolaylıkla ulaşabilmekte buna rağmen pek az insan verinin bir maddi karşılığı olduğunu bilmektedir. İkincisi, pek çok insan hangi verinin değerli olduğunu ve değerli verinin nasıl koruması gerektiğini bilmemekte ve bunun sonucunda devekuşu sendromu yaşamakta, harekete geçmek yerine sorunu görmezlikten gelmeyi tercih etmektedir. Üçüncüsü, verinin korunumu ile ilgili Türkiye'de ve dünyada yeterli yasal düzenleme bulunmamaktadır. Bu sebepler göz önüne alındığında, verinin değeri, veriyi ele geçirenlere nasıl bir güç sağladığı ve verinin nasıl korunacağına dair gerekli iletişimin sıradan insanların anlayabileceği bir dille, uygun iletişim kanalları ile yeterli frekansta yapılması büyük önem taşımaktadır. Bununla beraber gerekli yasal düzenlemelerin teknoloji ile paralel bir hızla yapılması ve verinin kötü amaçlı kullanımına ile ilgili adil ve caydırıcı cezaların yürürlüğe konması bir gerekliliktir.

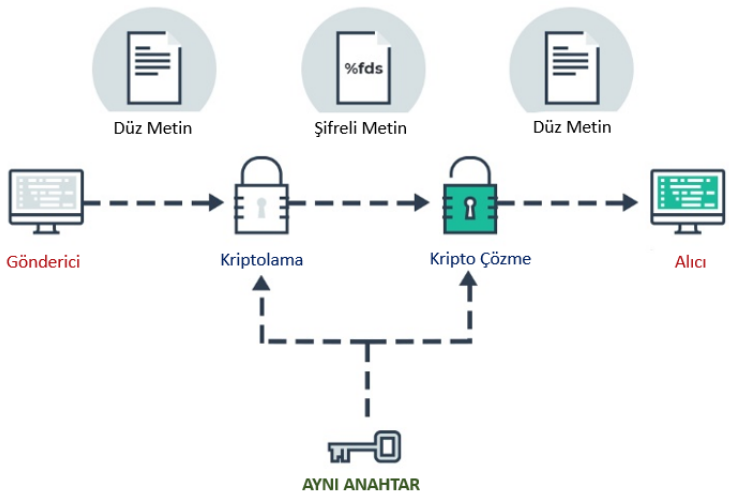
Gözetlemeden ve Algoritmalardan Korunma

Algoritmalar, kuşkusuz ki tümüyle kötü değildir. İnsanoğlunun –algoritmaların aksine- insana özgü yanılgıları, hataları, yanlılıkları (bias) ve kestirmeleri (heuristics) vardır. Bundan dolayıdır ki pek çok algoritma insan kaynaklı hatalardan kaçınmak açısından oldukça faydalıdır. Örneğin ayrımcılık konusunda, insanlar (istemeden de olsa) ayrımcılık yapabilirler. Oysa algoritmalar, bu tür bir bilgi kodlanmadığı sürece ayrımcılık yapmaz hatta ayrımcılığa karşı bir mekanizma olabilirler. Kleinberg ve diğerleri algoritmalar ile ayrımcılığı ispatlamanın daha kolay olacağını ya da en azından olması gerektiğini ve bunun yapılabilir olduğunu iddia etmektedir (Kleinberg,

[7] Tablodaki içerik 20 Şubat 2019 tarihinde Panoptikon Vakfı'ndan alınan izinle Türkçeye çevrilmiştir.

Ludwig, Mullainathan, & Sunstein, 2018). Algoritmalar, bu anlamda fayda sağlayabilmekle beraber mahremiyetin ihlali açısından bakıldığında algoritmalardan korunmak da zaman zaman gerekli olmaktadır.

Kullanıcıların, mahrem ya da üçüncü kişi veya kurumlar tarafından bilinmesini istemedikleri bilgilerinin, kişi veya kurumların eline geçmemesi için alması gereken bir dizi önlem bulunmaktadır ve günümüz internet kullanıcılarının pek az bir kısmının bu önlemlerden haberdar olduğu düşünülmektedir. Bunların başında şifreleme (encryption – kriptolama) gelmektedir. Genel olarak şifreleme, bir mesajın, şifre çözücü anahtara sahip olmayan kişilerce okunmasını engelleyen işlem olarak açıklanabilir. Örneğin; mesajlaşma, bankacılık işlemleri gibi işlemlerde uçtan uca şifreleme (sadece uç kullanıcıların okuyabildiği, iletişim yolu üzerindeki diğer kullanıcıların okuyamadığı şifreleme) sıklıkla kullanılmaktadır. Sıklıkla kullanılan Telegram, Whatsapp, Facebook Messenger, Facetime, Wire, Signal gibi uygulamalar uçtan uca şifreleme kullanan uygulamalara örnek verilebilir.



Kaynak: (PixelPrivacy, 2019)

Şekil 5. Metin Şifreleme

İnternet siteleri de dijital gözetlemenin önemli bir parçasıdır. Kullanıcı herhangi bir internet sitesini ziyaret ettiğinde üçüncü parti izleyiciler (çerezler (cookies), web işaretçileri (web beacons), pixel tag vb.) devreye girer. Web sitelerinin hangi üçüncü parti izleyicileri kullanacakları tamamen web sitesinin kendisine bağlı olup, bazı web sitelerinin onlarca üçüncü parti izleyici kullandıkları bilinmektedir. Üçüncü parti izleyiciler, kullanılan cihaz ve ziyaret edilen web siteleri ile ilgili sayısız bilgi toplayabilir; topladığı bu bilgileri devlete, reklam şirketlerine ya da diğer şirketlere verebilir veya satabilir.

Kullanıcı, bir web sitesini ziyaret ettiğinde, çevrimiçi izleyiciler ve sitenin kendisi -kullanıcı kendisini korumak için bir yazılım yüklediyse bile- kullanıcıyı tanımlayabilir; tarayıcıyı, izlemeyi engellemek için yapılandırmak mümkündür, ancak pek çok kişi bunun nasıl yapıldığını bilmemektedir (Electronic Frontier Foundation, 2019). (Tarayıcının izleyemeye

karşı güvenli olup olmadığını test etmek için Panopticlick sitesinin testi[8] kullanılabilir. Ayrıca LightBeam[9], Trackography[10] (Türkiye için veri sağlayamamaktadır) gibi araçlar kullanıcının kim tarafından izlendiği hakkında bilgi verebilmektedir.

İzleyicileri engelleyen eklentiler ve araçlar da izlemeye karşı kullanılabilir. Bu tür eklentilere ve araçlara Privacy Bagder, Adblock Plus, Disconnect, Https Everywhere, Noscript, Scriptsafe, Click&Clean örnek verilebilir (Me and My Shadow, 2019).

Uzaktan erişim yoluyla farklı ağlara bağlanma imkânı vermek sureti ile gizlilik sağlayan Sanal Özel Ağlar (VPN - Virtual Private Network) da izleyicilere karşı (yüzde yüz olmasa da) koruma sağlayabilmektedir. En bilinen sanal özel ağların başında Tor Browser gelmekle birlikte, ExpressVPN, NordVPN, Hotspot Shield vb. onlarca alternatif bulunmaktadır.

Facebook ve Google başta olmak üzere pek çok internet sitesinin kişisel verileri topladığı ve işlediği bilinmektedir. Bu durumu ortaya koyan en basit örneklerden biri Google'ın "Aktivitelerim" uygulamasıdır. Myactivity.google.com aracılığı ile kişiler, oturumları açıkken internette yaptıkları bütün aramalara, hangi cihazlardan hangi uygulamaları açtıklarına, sesli etkinliklerine, konum geçmişlerine, fotoğraf konumlarına ve YouTube izleme ve arama kayıtları gibi pek çok veriye ulaşabilir. Yetişkin içerikli 22.484 adet çevrimiçi site üzerinde yapılan 2019 tarihli bir araştırmaya göre ise, kullanıcı verilerinin %93'ü üçüncü partilere sızmaktadır (Maris, Libert, & Henrichse, 2019). Aynı çalışmada, bazı sızıntıların kullanıcı siteye gizli modda (incognito mode) girse dahi olabileceği belirtilmektedir.

Çevrimiçi sızıntılar çocuklar için de bir tehdit oluşturabilmektedir. Özellikle son yıllarda daha sıklıkla kullanılır olan akıllı oyuncaklar ve akıllı saatler gibi çocuklar için üretilmiş ürünlerde bazı güvenlik açığı vakaları meydana gelmiştir. Bununla ilgili Apple firmasının geliştiricilere gönderdiği bildiriye göre artık çocukların kullanacağı uygulamalarda; takip için kullanılabilecek istatistik amaçlı bilgiler toplayan servisler, davranış bazlı reklam sunan servisler ve satın alım için açık bir şekilde yönlendirme yapan içerikler bulunamayacaktır (Can, 2019). Güvenlik açıkları şirketlerin itibarını da zedelediği için, Apple'a benzer şekilde adı sık sık veri sızıntısı ihlallerine ve davalarına karışan Facebook da İngiltere'de ücretsiz gizlilik kontrolü sağlayacak 5 kafe açmak üzere girişimde bulunmuştur. Benzer şekilde Google da 2007-2010 yılları arasında Google Sokak Görüntüsü uygulaması ile coğrafi görüntü alırken aynı zamanda etraftaki wi-fi şifrelerini de topladığının ortaya çıkmasının ardından 13 milyon dolar ceza ödemiş ve kaydettiği tüm verileri sildiğine dair kamuoyuna açıklama yapmıştır. Büyük teknoloji şirketlerinin mahremiyet ihlallerine güncel bir örnek de Ağustos 2019'da Apple'ın ses asistanı Siri'nin konuşma dinleme açıklaması ve özrüdür. Apple, mahremiyetin temel bir insan hakkı olduğunu belirterek kullanıcı güvenini yeniden kazanmak için politika değişiklikleri yaptığını vurgulamış ve kullanıcılarından özür dilemiştir (McGee, 2019).

[8] https://panopticlick.eff.org/
[9] https://addons.mozilla.org/en-US/firefox/addon/lightbeam/
[10] https://trackography.org/

Akıllı telefonlarda sıklıkla kullanılan fal uygulamaları, FaceApp gibi yüz tanıma uygulamaları, adet takipçisi ya da kilo takipçisi gibi uygulamalar kişisel verilere kolaylıkla erişebilmektedir. Bu veriler, fotoğraflar, e-posta, kullanım verileri (trafik), ziyaret edilen web sayfaları ve eklentiler gibi verilerden oluşmaktadır. Kişilerin gönüllü olarak kendileri hakkında verdiği bilgiler bu uygulamaların sahibi olan şirketler tarafından işlenebilmekte hatta satılabilmektedir. Örneğin FaceApp uygulamasını kullanmak için kullanıcının öncelikle gizlilik sözleşmesi ve kullanım şartlarını onaylaması gerekmektedir. Bu sözleşmeyi onaylayan kullanıcı, uygulama ile paylaştığı içeriğin üzerinde mülkiyet hakkını kaybetmektedir. Kullanıcı içeriği paylaştığında ise içerik ile ilgili tüm bilgiler (konum, kullanıcı adı gibi) artık herkese açık hale gelmektedir. Uygulama üzerinden üretilen tüm içerik uygulama tarafından ticari amaçlarla kullanılabilir ve bu kullanımla ilgili kullanıcıya herhangi bir bildirimde bulunma zorunluluğu bulunmamaktadır. İçerik kullanıcı tarafından kaldırılsa dahi uygulama tarafından kullanılmaya devam edebilir. Kullanıcı, oluşturduğu içeriğin silinmesini ancak uygulamanın sahibi şirketin izin vermesi durumunda gerçekleştirebilir. Kullanıcıların çok büyük kısmının, kullandıkları uygulamaların hüküm ve şartlarını (terms & conditions) okumadan onayladıkları düşünüldüğünde bu tür uygulamaların kullanıcılar açısından yarattığı tehdidin bir başka boyutu daha ortaya çıkmaktadır. Hüküm ve şartların imzalanması, teoride uygulamada olmakla birlikte pratik anlamda kullanıcı açısından sadece bir formaliteden ibarettir ve kullanıcı bu sözleşmeleri onaylarken karşılaşması muhtemel tehlikelerin farkında değildir. Hüküm ve şartlar çoğu zaman kullanıcının anlayacağı dilde (çoğunlukla İngilizce olması ve hukuki bir dille yazılması) ve uzunlukta değildir. Örneğin Paypal uygulamasının hüküm ve şartlar belgesi Shakespeare'in Hamlet eserinden daha uzundur (The Behavioural Insights Team, 2019).

İnternet kullanıcılarının aşina oldukları "hüküm ve şartlar" ya da "gizlilik politikaları" teoride çok önem arz etmekle beraber pratikte çoğunlukla okunmadan geçilen metinlerden ibarettir. 2008 yılında yapılan bir çalışmaya göre American Online (AOL) 2005 verilerine göre en çok tıklanan 75 web sitesinin gizlilik politikasının ortanca (medyan) kelime uzunluğu 2,514 kelime olarak tespit edilmiştir (M. McDonald & Cranor, 2008, s. 554) . Standart okuma süresi dakikada 250 kelime olarak kabul edildiğinde ortalama bir gizlilik politikasının okunma süresi yaklaşık 10 dakika olarak hesaplanabilir ki bu metinlerin gün geçtikçe daha da detaylandığı düşünüldüğünde bu sürenin de yıllar içinde artmış olduğu kanaatine ulaşılabilir. Benzer şekilde, 2017 yılında Londra'da açılan "The Glass Door: Looking into Your Online Life (Cam Oda: Çevrimiçi Hayatınıza Bakış)" sergisinde bir sanatçı Amazon Kindle'ın Hüküm ve Koşullarını gerçek zamanlı olarak okumuş ve bu okuma yaklaşık 9 saat sürmüştür (Jeong, 2017).

Hızla dijitalleşen dünyada artık kamu yönetimi de çevrimiçi hizmetler ve özellikle e-devlet uygulaması ile birlikte dijitalleşmeye başlamıştır (Darı, 2019). Ancak devletler sadece kendi dijital uygulamalarını değil aynı zamanda vatandaşları ile üçüncü kişi ve kurumlar arasındaki veri paylaşımını da ihlallere karşı korumak ve bu veri akışını uygun şekilde yönetmek durumundadırlar. Dünyanın farklı ülkelerinde farklı uygulamalar olmakla birlikte, çoğu ülkede kişilerin, kendilerine ait verilerini korumalarına yönelik yasalar bulunmakta ve bu yasalar teknoloji ile paralel olarak geliştirilmektedir. Örneğin 2015 yılında, Beyaz Saray bir "Tüketici Gizliliği Hakkı Beyannamesi" yayınlamıştır. Avrupa Birliği'nde (AB), AB Genel Veri Koruma

Yönetmeliği (EU General Data Protection Regulation - GDPR) geçerlidir. Türkiye'de ise 24 Mart 2016 tarihinde, 6698 sayılı Kişisel Verilerin Korunması Kanunu Türkiye Büyük Millet Meclisinde kabul edilmiş, kanun 7 Nisan 2016'da yayımlanarak yürürlüğe girmiştir. Bu kanunla beraber Kişisel Verileri Koruma Kurumu da 12 Ocak 2017'de devlet teşkilatına katılmıştır. Kurumun misyonu, "Anayasada öngörülen özel hayatın gizliliği ile temel hak ve özgürlüklerin korunması kapsamında, ülkemizde kişisel verilerin korunmasını sağlamak ve buna yönelik farkındalık oluşturarak bilinç düzeyini geliştirmek, aynı zamanda veri temelli ekonomide özel ve kamusal aktörlerin uluslararası rekabet kapasitelerini artırıcı bir ortam oluşturmak (Kişisel Verileri Koruma Kurumu, 2019)." olarak nitelendirilmiştir. Kişisel Verileri Koruma Kurumu Başkanı tarafından Anadolu Ajansı'na yapılan açıklamaya göre, Ağustos 2019 tarihi itibarı ile kuruma yapılan şikâyet sayısı 691, ihbar sayısı 83, veri ihlal bildirimi sayısı ise 108 olup toplam 882 başvurudan 439'u sonuçlandırılmıştır (Anadolu Ajansı, 2019).

Kişisel verilerin korunması amacı ile yasal veya gönüllü pek çok düzenleme, uygulama ve araç olmasına rağmen insanların kendi kişisel verilerini koruma altına alma isteklerinin, ya da çabalarının sınırlı olduğu söylenebilir. Dünyada ve Türkiye'de pek az sayıda insan yasal düzenlemelerden haberdardır. Yine pek az sayıda insan dijital araçları kullanırken farkında olarak ya da olmayarak onayladıkları taahhütlerin farkındadır. Amerika'da 2019 yılında 2.416 kişi ile yapılan bir ankette, tüketicilerin kendi verilerinin gizliliğini korumak için ödemeye razı oldukları ortanca (medyan) ücret 5$/ay iken kişisel verilerine ulaşılması için talep ettikleri ücret 80 $/ay olmuştur (Winegar & Sunstein, 2019). İnsanlar kişisel verilerine değer vermektedir, bununla beraber verilerinin korunması konusunda çok da hassas davranmamaktadırlar.

Sonuç

Gözetim, tarih boyunca güç ve iktidar kazanmanın gerekliliği olmuş bir olgudur. Gözetim ve gözetleme ile ilgili pek çok çalışma yapılmış ve halen yapılmakta olup bu çalışmalardan en iyi bilineni ve adeta bir nirengi noktası haline gelmiş olanı Panoptikon'dur. Panoptikon merkezinde, Süper-panoptikon, Sinoptikon, Omniptikon, Katoptikon gibi pek çok kavram da yazına girmiş ve gözetim çalışmaları tarih içerisinde daha da zenginlik kazanmıştır. Küreselleşme, iletişim araçlarının ve iletişim formalarının çeşitlilik kazanması, dünyada sosyal ve ekonomik dengelerde meydana gelmekte olan değişimler ve güç savaşları gibi pek çok etken panoptikon (ve panoptikon merkezli diğer tasarımları) konu alan çalışmalar için kaynak oluşturmaktadır.

Post-panoptik çağ olarak nitelendirilebileceğimiz günümüzde gözetim ortadan kalkmamış, aksine, çeşitli formlarda gün geçtikçe günümüz insanının hayatına daha çok girer olmuştur. Kapalı sistem kameralar, biyometri, akıllı nesneler, şeylerin interneti, bulut bilişim, blok zinciri ve elbette sosyal medya birer post-panoptik gözetim aracı haline gelmişlerdir. Pek çok insan gerek zorunluluk (örneğin faks teknolojisinin neredeyse kullanımdan kalkarak yerini elektronik postaya bırakması ya da pek çok yasal işlemin devlet daireleri yerine elektronik devlet üzerinden işlemesi gibi) gerekse gönüllü olarak yeni teknolojileri kullanmaktadırlar. Yeni teknolojilerin insan hayatında gittikçe daha çok kullanılır hale gelmesinin yanı sıra insanlar sosyal medyayı

da daha çok kullanır, varlıklarını adeta sosyal medyadaki görünürlükleri ile ispat eder duruma gelmişlerdir. Bu durumda gözetleme, teoride, bir "alan memnun, satan memnun" durumudur. Post-panoptik araçların gün geçtikçe daha fazla sayıda insan tarafından, yoğunluğu ve frekansı artan bir şekilde kullanılması (Elisabeth Noelle-Neumann'ın "Suskunluk Sarmalı" teorisine benzer şekilde) adeta bir "Post-panoptik Sarmal" yaratmakta, mevcut gözetim gittikçe daha fazla gözetim yaratmaktadır.

Post-panoptik araçlar çoğu zaman insanların kullanımına -neredeyse- bedavaya sunulmaktadır. Örneğin Facebook ya da Instagram'da hesap açmak, fal uygulamasında fal baktırmak ya da YouTube'da video izlemek ücretsizdir. İnsanlar kendilerine sunulan bu ürün ya da hizmetleri çoğu zaman memnuniyetle ve gönül rızası ile kabul etmekte ve kişisel bilgilerini ürün ve hizmet sağlayıcılarla paylaşmakta sakınca görmemektedirler. Oysa çoğu kısa bir süre öncesinde -deyim yerindeyse- küçük garajlarda kurulmuş olan bu küçük şirketlerin şimdinin dev şirketlerine dönüşmüş olmasının altında yatan en önemli sebep şu cümlede gizlidir: "Eğer bir şey için ödeme yapmıyorsanız ürün sizsiniz.".

Bu çalışmada post-panoptik araçlar vasıtası ile elde edilen verinin ne amaçla, hangi yöntemlerle, nasıl elde edildiği ve ne amaçla kullanıldığı incelenmiş, elde edilen verinin sadece kişiler özelinde değil, toplumlar için de yarattığı ve yaratacağı tehditler irdelenmiş, şahsi verinin kişisel önlemler ve hukuki düzenlemeler ile nasıl korunması gerektiği incelenmiş aynı zamanda araştırmacılar için bütüncül ve Türkçe bir kaynak oluşturulmaya çalışılmıştır. Gözetim hâlihazırda pek çok araştırmacının ilgi duyduğu ve üzerinde çalıştığı bir alandır. Konu ile ilgili; özellikle popüler çevrimiçi ortamlar üzerinde yapılacak nicel çalışmaların da ilgi çekici sonuçlar ortaya koyma olasılığı oldukça yüksektir.

Kaynakça

Anadolu Ajansı. *Kişisel Verileri Koruma Kurumu'na 882 başvuru*. 17 Ağustos 2019 tarihinde aa.com.tr/tr/turkiye/kisisel-verileri-koruma-kurumuna-882-basvuru/1558495 adresinden erişildi.

Birleşmiş Milletler. *SDG Indicators, Metadata Respository*. 20 Temmuz2019 tarihinde unstats.un.org/sdgs/metadata/?Text=&Goal=16&Target=16.9 adresinden erişildi.

Bogard, W. (1996). *The simulation of surveillance: Hypercontrol in telematic societies.* Cambridge: Cambridge University.

Borgesius, F., Möller, J., Kruikemeier, S., Fathaigh, R., Irion, K., Dobber, T., . . . de Vreese, C. (2018). Online political microtargeting: Promises and threats for democracy. *Utrecht Law Review*, *14*(1), 82-96.

Bradt, G. (2016). *Wanamaker Was Wrong - The Vast Majority of Advertising Is Wasted*. 19 Temmuz 2019 tarihinde forbes.com/sites/georgebradt/2016/09/14/wanamaker-was-wrong-the-vast-majority-of-advertising-is-wasted/#64a46909483b adresinden erişildi.

Brockell, G. (2018). *An open letter to Facebook, Twitter, Instagram and Experian Regarding Algorithms and My Son's Birth*. 21 Temmuz 2019 tarihinde twitter.com/gbrockell/status/1072589687489998848?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed&ref_url=https%3A%2F%2Fwww.cnbc.com%2F2018%2F12%2F12%2Fwoman-calls-out-tech-companies-for-serving-baby-ads-after-stillbirth.html adresinden erişildi.

Can, M. (2019). *Apple, Reklamsız Uygulama Dönemini Başlatıyor!* 29 Ağustos 2019 tarihinde shiftdelete.net/apple-reklamsiz-cocuk-uygulamalari-istiyor adresinden erişildi.

Çalışkan, O. (2014). Kamusal alan bağlamında ağ toplumu ve yeni kamusal alan arayışı. *Maltepe Üniversitesi İletişim Fakültesi Dergisi, 1*(1), 41-62.

Darı, A. (2019). Kamu yönetiminin gelenekselden dijitale dönüşümü ve e-devlet uygulaması. *3. uluslararası GAP sosyal bilimler kongresi* (s. 144). Ankara: İKSAD- İktisadi Kalkınma ve Sosyal Araştırmalar Enstitüsü.

Deleuze , G., & Guattari , F. (1983). *Anti oedipus: Capitalism and schizophrenia*. Minneapolis: University of Minnesota.

Desai, V., Diofasi, A., & Lu, J. (2018). The Global İdentification Challenge: Who are the 1 Billion People without Proof of Identity? 2 Ağustos 2019 tarihinde blogs.worldbank.org/voices/global-identification-challenge-who-are-1-billion-people-without-proof-identity adresinden erişildi.

Electronic Frontier Foundation. *Panopticlick 3.0, Is your browser safe against tracking?* 21 Temmuz 2019 tarihinde panopticlick.eff.org: https://panopticlick.eff.org/ adresinden erişildi.

Facebook Newsroom. (2018). *An Update on Our Plans to Restrict Data Access on Facebook*. 2 Ağustos, 2019 tarihinde newsroom.fb.com/news/2018/04/restricting-data-access/ adresinden erişildi.

Foucault, M. (2007). *İktidarın Gözü, Seçme Yazılar, çev. Mehmet Ali Kılıçbay*. İstanbul: Yapı Kredi.

Ganascia, J. (2009). The Great Catopticon. *8th International Conference Computer Ethics: Philosophical Enquiry* (s. 252-26). Corfu: Ionian Academy.

Haggerty , K., & Ericson, R. (2003). The Surveillant Assemblage. *The British Journal of Sociology*, 605-622. doi:https://doi.org/10.1080/00071310020015280

Harari, Y. (2018). 21. *Yüzyıl İçin 21 Ders*. İstanbul: Kolektif Kitap.

Hern, A. (2018). *Cambridge Analytica: how did it turn clicks into votes?* 21 Temmuz 2019 tarihinde https://www.theguardian.com/news/2018/may/06/cambridge-analytica-how-turn-clicks-into-votes-christopher-wylie adresinden erişildi.

Identification For Development - World Bank. (2019). *Global Identification Challenge by the Numbers*. 15 Ağustos 2019'da id4d.worldbank.org: https://id4d.worldbank.org/global-dataset adresinden erişildi.

Information is Beautiful. *World's Biggest Data Breaches & Hacks*. 23 Temmuz 2019 tarihinde informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/?utm_content=buffer6c5c7&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer adresinden erişildi.

International Institute for Democracy and Electoral Assistance. (2018). 19 Ağustos 2019 Digital Microtargeting: Political Party Innovation Primer 1. adresinden erişildi.

Jeong, S. (2017). *Turning the Specter of Internet Surveillance into Art*. 29 Ağustos 2019 tarihinde theverge.com/2017/11/9/16620452/london-glass-room-art-exhibit adresinden erişildi.

Kartarı, A. (2017). Nitel düşünce ve etnografi: Etnografik yönteme düşünsel bir yaklaşım. *Moment Dergi, 4*(1), 207-220.

Kişisel Verileri Koruma Kurumu. *KVKK Misyon Vizyon*. 29 Temmuz 2019 tarihinde kvkk.gov.tr/Icerik/2074/Misyon---Vizyon adresinden erişildi.

Kleinberg, J., Ludwig, J., Mullainathan, S., & Sunstein, C. (2018). Discrimination in the Age of Algorithms. *Journal of Legal Analysis, 10*, Online. doi:https://doi.org/10.1093/jla/laz001

Kozinets, R. (2010). *Netnography, doing etnographic research online*. Londra: Sage.

Kurban, S. (2014). *Seçim kampanyalarının yürütülmesi sürecinde sosyal medyanın kullanımı ve 28 Temmuz 2013 KKTC genel seçimlerine bir bakış. Dijital İletişim Etkisi*. İstanbul: İskenderiye Kitap.

M. McDonald , A., & Cranor, L. (2008). The cost of reading privacy policies. *Journal of Law and Policy for the Information Society*, 543-568.

Mance, H.. *Is Privacy Dead?* 19 Temmuz 2019 tarihinde ft.com/content/c4288d72-a7d0-11e9-984c-fac8325aaa04 adresinden erişildi.

Maris, E., Libert, T., & Henrichse, J. *Tracking Sex: The Implications of Widespread Sexual Data Leakage and Tracking on Porn Websites (pre-print)*. 15 Temmuz 2019 tarihinde Cornell University, Computer and Society: https://arxiv.org/abs/1907.06520 adresinden erişildi.

Marx, G. (2015). *Surveillance Studies. J. ed. Wright içinde, International Encyclopedia of the Social & Behavioral Sciences*, Second Edition (s. 733-741). Elsevier Ltd. doi:http://dx.doi.org/10.1016/B978-0-08-097086-8.64025-4

McGee, P. *Apple Apologises for Listening to Siri Conversations*. 28 Ağustos 2019 tarihinde ft.com/content/2563911e-c9a9-11e9-a1f4-3669401ba76f adresinden erişildi.

Me and My Shadow. *Prevent Online Tracking*. 21 Temmuz 2019 tarihinde myshadow.org/prevent-online-tracking adresinden erişildi.

Özdemir, Ş. *Modern Zamanlarda Panoptikon: Dijital Gölgenin 3 Katmanı*. 20 Temmuz 2019 tarihinde medium.com/@behavioralist/modern-zamanlarda-panoptikon-dijital-g%C3%B6lgenin-3-katman%C4%B1-e0ab483203cd adresinden erişildi.

Panoptykon Foundation. *7 Sins of Surveillance Society*. 21 Temmuz 2019 tarihinde en.panoptykon.org/idea adresinden erişildi.

Panoptykon Foundation. *About Panoptykon Foundation*. 21 Temmuz 2019 tarihinde en.panoptykon.org/about adresinden erişildi.

Panoptykon Foundation. *Panoptykon Foundation*. 20 Temmuz 2019 tarihinde https://panoptykon.org/ adresinden erişildi.

Panoptykon Foundation. *Three Layers of Digital Shadow*. 21 Temmuz 2019 tarihinde panoptykon.org/sites/default/files/3levels.png adresinden erişildi.

PixelPrivacy. *What Is Encryption And How Does It Work*? 29 Ağustos 2019 tarihinde pixelprivacy.com: https://pixelprivacy.com/resources/what-is-encryption/ adresinden erişildi.

Schneier, B. (2016). *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*. New York: W. W. Norton & Company.

Stewart, M., & Arnold, C. (2018). Defining social listening: recognizing an emerging dimension of listening. *International Journal of Listening, 32*(2), 85-100. doi:10.1080/10904018.2017.1330656

Tanış, A. (2018). *Gillian Brockell: Algoritmalarınız Çocuğumu Kaybettiğimi Anlamadı mı?* 30 Temmuz 2019 tarihinde dokuz8haber.net: https://dokuz8haber.net/gundem/insanhaklari/verilerle-sivil-toplum-ve-dernekler-turkiye-demokratiklesmeye-ne-kadar-gonullu/ adresinden erişildi.

The Behavioural Insights Team (2019). *Improving Consumer Understanding of Contractual Terms and Privacy Policies: Evidence-Based Actions for Businesses.* 25 Temmuz 2019 tarihinde bi.team/publications/improving-consumer-understanding-of-contractual-terms-and-privacy-policies-evidence-based-actions-for-businesses/ adresinden erişildi.

Thompson, C. (2015). *Beyond Google: Everything You need to Know About the Hidden Internet*. 12 Ağustos 2019 tarihinde businessinsider.com/difference-between-dark-web-and-deep-web-2015-11 adresinden erişildi.

Türk, G., & Demirci, E. (2016). Sanal Dünyada Dönüşen Mahremiyet Algısı; İnstagram Örneği. *1st International Academic Research Congress* (s. 518-525). Ankara: Pegem Akademi.

Türkiye Bilimler Akademisi. (2011). *Türkçe Bilim Terimleri Sözlüğü - Sosyal Bilimler*. Ankara: TÜBA (Türkiye Bilimler Akademisi).

Walker, L. (1998). *Amazon Gets Personal With E-Commerce*. 12 Ağustos 2019 tarihinde washingtonpost.com/wp-srv/washtech/daily/nov98/amazon110898.htm adresinden erişildi.

Winegar, A., & Sunstein, C. (2019). How Much Is Data Privacy Worth? A Preliminary Investigation. *Journal of Consumer Policy*, 42, 425-440. doi:https://doi.org/10.1007/s10603-019-09419-y

World Wide Web Size. *The size of the World Wide Web (The Internet*). 20 Temmuz 2019 tarihinde worldwidewebsize.com/ adresinden erişildi.

Zuboff, S. (2019). *The Age of Surveillance Capitalism: The Fight For a Human Future at the New Frontier of Power*. New York: PublicAffairs.