İNSAN&İNSAN, Yıl/Year 10, Sayı/Issue 36, Yaz/Summer 2023, 11-23 Araştırma Makalesi / Research Article
DOI: https://doi.org/10.29224/insanveinsan.1283746 www.insanveinsan.org e-ISSN: 2148-7537

Pandemiden Metaverse'e: Veri Odaklı Toplumun Yükselişi ve Riskleri

From Pandemic to Metaverse: The Rise and Risks of Data-Driven Society

ZÜBEYDE DEMİRCİOĞLU*

* Asst. Prof., İstanbul Medeniyet University, Faculty of Arts and Humanities, Department of Sociology, Göztepe South Campus, Kadıköy/İstanbul, Turkey, E-Mail: zubeyde.demircioglu@medeniyet.edu.tr
https://orcid.org/0000-0002-8749-006X

Öz: *Teknolojideki son gelişmeler fiziksel dünyayla etkileşimimizi değiştirmekte, dijital dönüşüm bu süreci daha da hızlandırmaktadır. Yakın dönemde yaşanan COVID-19 pandemisi de fiziksel ve dijital dünyanın yakınsamasına vesile olarak dijitalleşmeyi bir adım öteye taşımış, verinin merkezi hale gelmesini mümkün kılmıştır. Dijital dönüşümün mevcut nihai aşaması olarak Metaverse ise, sanal dünya ile fiziksel dünya arasındaki karşıtlığı ortadan kaldırarak dijital zaman ve mekân deneyimini fiziksel olana yaklaştırma misyonuyla ortaya çıkmıştır. Öte yandan bu yeni gerçeklik evreninin merkezinde kullanıcıların davranışlarını bilinebilir, öngörülebilir ve hatta kontrol edilebilir kılan, günlük yaşam deneyimini prosedürlere ve hesaplamalara indirgeyen veri odaklı bir anlayış bulunmaktadır. Bu çerçevede, bu çalışma Metaverse'e giden yolu açan dijitalleşmenin ve zihniyet olarak veri odaklılığın yükselişinde COVID-19 pandemisinin önemli bir etkisi olduğunu, Metaverse'ün veri odaklı anlayışının mahremiyet, gözetim ve kontrol gibi etik sorunları derinleştireceğini ileri sürmektedir.*

Anahtar kelimeler: *Dijitalleşme, Verileştirme, COVID-19 pandemisi, Metaverse, Gözetim, Mahremiyet*

Abstract: *Recent advances in technology are changing the way we interact with the physical world, and digital transformation is accelerating this process even further. The recent COVID-19 pandemic has also taken digitalization one step further by enabling convergence of the physical and digital, promoting the centralization of data. The Metaverse, as the current ultimate state of digital transformation, has emerged with the mission of bringing on the digital experience of time and space in a way closer to the physical world by eliminating the contradictions between the virtual and physical worlds. Furthermore, at the center of this new universe of reality underlies a data-driven approach that allows user behavior become knowable, predictable, and even controllable, bringing the daily life experience down to procedures and calculations. In this regard, this study argues that the COVID-19 pandemic had a significant impact on the rise of digitalization and data-centricity as a mindset that paved the way for the Metaverse, and that the data-centric understanding of the Metaverse will deepen ethical issues such as privacy, surveillance and control.*

Keywords: *Digitalization, Datafication, COVID-19 pandemic, Metaverse, Surveillance, Privacy*

Gönderim 15 Nisan 2023
Düzeltilmiş Gönderim 02 Haziran 2023
Kabul 24 Haziran 2023

Received 15 April 2023
Received in revised form 02 June 2023
Accepted 24 June 2023

Yayıncı / Publisher: Okur Yazar Derneği / Literacy Association, İstanbul, Turkey
Website: https://www.okuryazar.org.tr

Giriş

Sürekli gelişen ve yaygınlaşan bilgi ve iletişim teknolojileri gündelik hayatı pek çok açıdan dönüştürüp değiştirmektedir. Kullanıcılar açısından değerlendirildiğinde öncelikle kişisel bilgisayarların ardından internetin ve nihayet mobil cihazların ortaya çıkışı üç önemli teknolojik yenilik dalgası olarak değerlendirilirse dördüncü dalganın sanal ve artırılmış gerçeklik gibi uzamsal teknolojiler olduğu söylenebilir (Mystakidis, 2022: 486). Bu dördüncü dalga; pandemi sürecinde uzaktan eğitim, evden çalışma ve çevrimiçi sosyal etkinlikler gibi gündelik hayatın farklı alanlarına nüfuz etmiştir. Bu anlamda pandemi sürecinin Metaverse'ü ortaya çıkartan koşulları hızlandırdığı ifade edilebilir.

Siber uzay ya da daha yaygın kullanıldığı biçimde sanal alem 1990'larda İnternetin yaygınlaşmasıyla birlikte gündeme taşınmıştır. 1990'lardan bu yana sosyal medya platformlarının ortaya çıkışı ve geniş çapta yaygınlaşması, mobil cihazlarla erişimin sağlanması gibi teknolojik gelişmeler bir dizi bağlantısız sanal dünyadan entegre bir sanal dünyalar ağı olarak Metaverse'e geçiş fikrini mümkün kılmıştır. Bununla birlikte teknolojinin yeni bir aşaması olarak kabul edilen Metaverse; yapay zeka, nesnelerin interneti, blok zinciri, sanal gerçeklik, artırılmış gerçeklik gibi bir dizi teknolojik gelişme ile mümkün hale gelmiştir (Bibri ve Allam, 2022: 3).

İnsanlık yaklaşık otuz yıl boyunca bilim kurgu olarak resmedilen sanal evren fikrine bugün her zamankinden daha yakındır. Kullanıcılara bugüne kadarki deneyimlerinden çok farklı deneyimler vaat eden Metaverse dijital geleceğe ilişkin ilham verici bir vizyon sunuyor olmakla birlikte bazı kritik sorunları ve riskleri de beraberinde getirmektedir. Güvenlik, gizlilik, gözetim, kontrol olarak sıralanabilecek bu risk ve kritik sorunlar; Metaverse'ün merkezinde yer alan kullanıcıların gündelik yaşam deneyimlerini hesaplamalara ve prosedürlere indirgeyen, duygu, motivasyon ve davranışlara ilişkin hesaplamalı anlayıştan kaynaklanmaktadır (Bibri ve Allam, 2022: 6). Bireyi adeta bir istatistiğe indirgeyen bu anlayış veri odaklılıkla doğrudan ilgilidir. Bu çerçevede bu çalışma Metaverse'e giden yolu açan dijitalleşmenin ve zihniyet olarak veri odaklılığın yükselişini ele alarak bu yükselişte COVID-19 pandemisinin önemli bir etkisi olduğunu ileri sürecek ardından Metaverse'ün veriye dayalı yapısına odaklanarak kontrol ve mahremiyete özel bir atıfta bulunarak risklerini ve etkilerini ortaya koymaya çalışacaktır.

Pandeminin Dijital Dönüşüm Üzerine Etkileri

Dijital teknolojilerin hayatın her alanına giderek daha derinlikli bir şekilde nüfuz ettiği bir çağda yaşıyoruz. Bilgi kümelerinin işlenebildiği, iletilebildiği, depolanabildiği, yeniden kullanılabildiği ve hatta manipüle edilebildiği büyük ölçekli bir dijital dönüşümden geçiyoruz. Henüz geçirmiş olduğumuz pandeminin de bu dönüşüm sürecini önemli ölçüde hızlandırdığını söylemek mümkün.

COVID-19 pandemisi ülkelerin, toplumların ve bireylerin önceliklerini değiştirecek ölçüde toplumsal değişimlere neden olmuştur. Bu değişimlere neden olan en önemli faktörlerden biri, sağlık otoritelerinin salgının yayılmasını engellemek ve azaltmak üzere aldıkları fiziksel/sosyal mesafe önlemidir. Alınan pek çok önlemin yanı sıra kısmi ya da yer yer tamamen karantina kararlarıyla fiziksel mesafe önlemi

hayata geçirilmiş, böylelikle gündelik hayatın devamı büyük ölçüde teknoloji bağımlı hale gelmiştir. Sosyalleşme, etkileşim, çalışma, öğrenme, alışveriş hatta seyahat etme, müze ziyaretleri gibi fiziksel alanın dışında tahayyül edilemeyecek etkinlikler çevrimiçi alana taşınmıştır. Dolayısıyla sosyal mesafe politikalarının bir sonucu olarak dijital faaliyetlere geçiş, sanal gerçeklik ile fizikselin birleştirilmesinin önünü açmış, özellikle sosyal etkileşim biçimlerini dönüştürerek yaşam tarzlarında istisnai değişiklikler yaratmış, teknolojinin rolü daha hayati hale gelmiştir (Al-Khatib, 2023). Her ne kadar pandemi sürecinden önce teknoloji felsefecileri artık dijital teknolojilerin ayrı sanal bir öteki oluşturmadığını, fiziksel hayatın içine nüfuz ettiğini savunmaya başlamış olsalar da (Coeckelbergh, 2020: 549); pandemi dijital, sanal ya da çevrimiçi adı verilen alanı gerçekliğimizin bizatihi kendisi haline dönüştürmüş, dijital; günlük eylemlerimiz ve etkileşimlerimizle bütünleşmiş (Demircioğlu, 2021: 112); dünyanın ana anlatısı haline gelmiştir (Mañero, 2020: 671).

Pandemi sürecinde yaşanan hızlı dijitalleşmenin bir diğer boyutu; pandemiyle mücadele için geliştirilen ve yaygınlaştırılan dijital gözetim araçlarıdır. Dünyanın dört bir yanında hükümetler bulaştırma riski taşıyan herkesi belirlemek ve izlemek üzere tasarlanan bu dijital gözetim araçlarını hızlıca benimsemişlerdir (Demircioğlu, 2023). COVID-19 salgınıyla birlikte kontrol ve gözetim araçları, akıllı telefon altyapısının ötesine taşınarak, kitlesel gözetim ve veriye dayalı yönetişime uzanmış, salgının yönetiminde dolaşımların ve temasların izlenmesi ve kontrolü esas alınmıştır. Kitchin'in (2020: 9) ifadesiyle COVID-19 salgınının biyopolitikasının merkezinde bedenlerin dolaşımı ve temasının; mekânsal erişim ve davranışın düzenlenmesi, yakın yönetimi ve kontrolü yer almaktadır. Pandemi sürecinde pek çok hükümet salgınla mücadele etmenin bir yolu olarak kişisel verilerin kullanılmasının önünü açmış; politika yapıcılar ve vatandaşlar, salgının yayılmasını sınırlamak amacıyla gözetim teknolojilerinin kullanılmasının meşruluğunu sorgulamamıştır. Dolayısıyla bütün bu gelişmeler bir yönüyle gözetim, kontrol ve veri odaklı yönetim ile yakından ilgilidir. Bu anlamda pandemi hem yeni dijital teknolojilerle daha incelikli kontrol araçlarının geliştirilmesine olanak tanırken hem de bireysel özgürlüklere karşı halk sağlığı söylemiyle gözetimin norm haline gelmesine imkan sağlamıştır. Bununla birlikte büyük teknoloji şirketlerinin veri politikalarına daha fazla dahil olması, dijital teknolojilerin hızla benimsenmesi, halkın bir halk sağlığı sorunu karşısında güvenlik meselesini ikincil görmesi veri gizliliği sorunlarını arttırmıştır (Li ve diğerleri, 2022). Bu bağlamda COVID-19 pandemisinin gözetim toplumu üzerindeki geniş kapsamlı ve uzun vadeli etkileri üzerinde daha fazla durulmalıdır. Zira çevrimiçi mahremiyet ihlali ve gözetim pratiklerinin yükselişi pandeminin öne çıkardığı sorun alanlarından biridir. Pandemi, 11 Eylül saldırılarından sonraki sürece benzer biçimde ancak sağlık güvenliği gibi farklı bir gerekçeyle gözetimi gündelik yaşamın merkezine taşımıştır. Bu dönüşümün akademik alandaki yansıması yaşamımıza her geçen gün giderek daha fazla nüfuz eden gözetim pratiklerine eleştirel bir yaklaşım sunan gözetim çalışmalarının yükselişe geçmesidir (Yıldırım, 2021: 165).

Pandemiyle birlikte devreye alınan bu dijital sistemlerin "yeni normal" denilen sürecin bir parçası olarak kullanılmaya devam edeceğini iddia edenler bulunmaktadır (Sadowski, 2020). Bibri ve Allam (2022: 6) pandemi nedeniyle gelen ani dijital dönüşümün, gözetim kapitalizminin mantığını insanların gündelik yaşamlarında daha yerleşik, otomatik ve yaygın hale getireceğini ileri sürmektedir. Bu öngörü

meselenin gizlilik, güvenlik, mahremiyet ve yönetimsellik açısından değerlendirilmesini önemli hale getirmektedir. Zira yapay zeka teknikleriyle birleşen büyük veri ve veri yoğun bilgi işlem algoritmalarındaki radikal genişleme COVID-19 salgınıyla daha da artmış, gündelik hayat etkinliklerinin veri ve algoritmalar yoluyla tanımlanabilmesinin önü açılmıştır. Öte yandan tüm bu meselelerin Metaverse ile daha da önemli sorunlar haline gelebileceği öngörülmektedir. Zira Metaverse tarafından üretilecek verinin büyüklüğü önceki dönemde toplanan veriye kıyasla çok daha muazzam olacaktır.

Büyük Veri Çağı Zihniyeti: Verileştirme

Dijitalleşmenin en önemli bileşenlerinden biri hiç şüphesiz veri hatta büyük veridir. Son dönemlerin popüler kavramlarından biri olan büyük veri, normal veri araçları tarafından kaydedilemeyecek, depolanamayacak ve analiz edilemeyecek kadar büyük veri yığınları anlamına gelir. Terimin tanımlayıcısı Laney (2001) büyük veriye ilişkin üç önemli özellikten söz eder: hacim, hız ve çeşitlilik. Özetle büyük veri, karmaşık, değişik türden büyük veri yığınlarını, nerdeyse eş zamanlı olacak biçimde hızlı işlemeyi temsil eder. Büyük veri kümeleri arasında konum verisi gibi mobil veriler, sosyal ağ verileri, ticari veriler, akış verileri ve nesnelerin internetinden gelen duyusal veriler yer almaktadır. Bu verilerden hareketle büyük verinin görselleştirilmesi, duygu analizi, bilgisayar destekli içerik analizi, doğal dil işleme gibi analizler yapılabilmektedir (Mills, 2018: 592). Bu analizlerin yapılabilmesi için gerekli büyük veri yığınları bir verileştirme sürecinin sonucudur. Kavram olarak verileştirme, bir sosyal eylemi veya süreci anlamlı verilere dönüştürme pratiğine (Cukier ve Mayer-Schöenberger, 2013) veya niceliksel bir formata dönüştürme eylemine (O'Neil ve Schutt, 2013) atıfta bulunur. Bu bağlamda büyük verinin toplumsala ilişkin bilgi üretme vaadi, insan davranışlarını anlama ve davranış kalıplarını çözerek tahmin edilebilirliğini arttırma gücüyle ilişkilendirilir. İnsan davranışlarına erişmenin, onları izlemenin ve anlamanın meşru bir yolu olarak görülen verileştirme (van Dijck, 2014: 198) yapay zeka algoritmaları yoluyla tahmine dayalı analiz yapılmasına olanak sağlar.

Günlük etkileşimlerin verileştirilmesi, dijital olarak üretilen verinin yoğunluğu ve bu verilerin analiz edilmesi için geliştirilen hesaplama algoritmalarının gelişmesi verinin iktisadi bir boyut kazanmasıyla doğrudan ilişkilidir. Gerçekten de dijital ekonomik sistemde veri önemli girdi kaynaklarından biri haline gelmiştir. The Economist dergisinin 6 Mayıs 2017 tarihli sayısında ifade edildiği gibi günümüzün en değerli kaynağı artık petrol değil kişisel verilerdir. Verinin iktisadi bir değer kazanmasıyla veri toplama ve işleme sürekli genişleyerek neredeyse tüm toplumsal yaşamı kapsar hale gelmiştir. Bu genişleme gündelik yaşamın birçok alanında artan sayıda "akıllı" cihazın entegrasyonuyla mümkün olmaktadır. Öyle ki, bugün bir bireyin dijital hizmetleri kullanmadan, dolayısıyla birtakım kişisel verilerini paylaşmaksızın günlük işlerini yürütmesi neredeyse imkansız hale gelmiştir (Nissenbaum, 2009). Böylelikle yeni araçlar, uygulamalar, ağlar, platformlar sosyal katılım için gereklilik haline gelirken bireyler de bu dijital araçlara bağımlı hale gelmişlerdir (Zuboff, 2015: 85). İnsanların günlük görev ve etkinliklerini giderek daha fazla çevrimiçi olarak gerçekleştirmeye başlamaları giderek daha büyük bir dijital ayak izi bırakmaları anlamına gelmektedir (O'Brolcháin ve diğerleri, 2016: 6). Sonuç olarak insanlar dijital bir toplumda yaşamanın gerekliliği olarak tüm bu hizmet ve uygulamalar aracılığıyla büyük miktarda dijital bilgi yaymaktadır. van Dijck (2014:

197) bu işlemi bir alışveriş, kullanıcıların dijital hizmetlere ulaşabilmek adına yaydıkları veriyi ise ödeme yapmak için kullanılan bir para birimi olarak kavramsallaştırmaktadır. Zuboff (2015) ise kullanıcıların çevrimiçi ve fiziksel dünyadaki davranışlarını ve hareketlerini izleyerek, insan deneyimine dayalı verileri hammadde olarak kullanarak kâr ve kontrol amacıyla davranışsal verilere dönüştürme çabasını bir tür yeni kapitalizm biçimi olarak tanımlamaktadır. Veriye dayalı bir birikim mantığına işaret eden gözetim kapitalizminin temel bileşenlerinden biri, büyük veridir.

Gözetim kapitalizmi; toplumsallığın dijital dönüşümü ve verinin değeri üzerine inşa edilen bir endüstri ortaya çıkarmış (van Dijck, 2014: 199) ve böylelikle her kullanıcı önemli hale gelmiş, uygulama ve platformlar maksimum kâr elde edebilmek üzere daha fazla kullanıcıdan daha fazla veri elde etme politikasını benimsemiştir. Zira dijital teknolojiler aracılığıyla verileştirilen kullanıcı eylemlerinden çıkarılan algoritmalar çok çeşitli dış aktörlerin kullanımına sunulabilmektedir (Langlois ve Elmer, 2013: 4). Örneğin Google ve Facebook gibi teknoloji devlerinin iş modeli, kullanıcıları hakkında bilgi toplamaya ve bu verileri başkalarına satmaya dayanmaktadır (O'Brolcháin ve diğerleri, 2016: 8). Tam da bu nedenle teknoloji odaklı bu ticari işletmeler veri ifşasını teşvik etmek üzere kullanıcıların iletişim kurmak, sosyalleşmek ve eğlenmek gibi temel ihtiyaçlarına cevap verecek şekilde tasarlanmaktadır (Acquisti, 2015: 512). Böylelikle teknoloji şirketleri kullanıcıların kişisel verilerini paylaşma pratiklerine ilişkin mahremiyet anlayışlarını temelden dönüştürmüştür.

Mahremiyetin kaybı ile ilgili tartışmalar esas olarak 1960'lı yılların ortalarından beri devam etmektedir. O dönem giderek gelişen kamera ve dinleme cihazı gibi izleme teknolojileri ile merkezi ana bilgisayarların yaygın kullanımı, tartışmaların ilk kaynağıdır (Vincent, 2016: 179). Rosenberg 1969 gibi erken bir evrede vatandaşların tüm bilgilerinin saklanacağı ulusal bir bilgisayar sisteminden söz ederek mahremiyetin ölümünü ilan etmiştir. Mahremiyet endişesiyle ilgili ikinci dalga 1983'te internetin 1993'te World Wide Web'in piyasaya çıkması ve eş zamanlı olarak kişisel bilgisayarların yayılması ile yükselmiştir. Bu noktadan itibaren Web'e erişim için her yeni geliştirilen ortamla birlikte, kişisel verileri toplamak üzere yeni yöntemler kullanılmaya başlanmıştır. İlk evrede kullanıcılar, statik web siteleri aracılığıyla sınırlı bir etkileşimle bilgiye erişebiliyorlarken; 2000'li yıllardan itibaren sosyal medya platformlarının ortaya çıkışı kullanıcı davranışı hakkında güçlü bir veri akışını başlatmıştır. İnternet statik bir içerik yığınından etkileşimli özellikler içeren bir alana dönüşmüş, mobil teknolojilerin kullanımı ses, görüntü, video ve coğrafi konum gibi verilerin anlık olarak paylaşılmasını mümkün kılmıştır (Nair ve diğerleri, 2022). Bu anlamda sosyal medya kullanımının hızlı yükselişiyle birlikte mahremiyet meselesine "teşhirci" mahremiyet ve kişisel verilerin şirketlerle paylaşılması endişeleri de eklenmiştir (Vincent, 2016: 214). Ancak bu her zaman kullanıcıların kendi istekleri ile verilerini paylaştıkları anlamına gelmez, kullanıcılar çoğu durumda hangi verilerin toplandığından habersiz hareket etmektedir. Bugün gelinen noktada Metaverse evreni ile birlikte cihazların sayısının artması, cihazlar arası entegrasyonun genişleyecek olması, toplanan verinin büyüklüğü mahremiyet tartışmalarını bir adım öteye taşıyacaktır.

Metaverse

Mekansal düşüncenin hakimiyetinden zaman, süreç ve akış odaklı yaklaşımlara geçişin ilk işaretlerinden biri Baudrillard'ın hiper-gerçeklik kavramıdır. Baudrillard (2006) hiper-gerçeklik kavramıyla gerçeğin tüm göstergelerine sahip olmakla birlikte gerçeğin kendisi olmayan bir modele işaret eder. Zaman içinde yeni teknolojilerin gelişmesiyle gerçekliğin dijitalle bağlantısını analiz etmek üzere başka kavramlar da geliştirilmiştir. Bu kavramlardan biri olan yaşamiçi (onlife)*, çevrimiçi ile çevrimdışı ayrımının ortadan kalktığı yeni bir varoluşsal duruma işaret etmek üzere Floridi (2015) tarafından ileri sürülmüştür. Floridi'nin temel argümanı, bilgi ve iletişim teknolojilerinin yaygınlaşmasıyla dört temel dönüşümüm yaşandığıdır. Bu dönüşümlerden ilki gerçek (çevrimdışı) ile sanal (çevrimiçi) arasındaki ayrımın bulanıklaşması; ikincisi insan, makine ve doğa arasındaki ayrımın bulanıklaşması; üçüncüsü bilginin genişlemesi ve yayılması ve sonuncusu önceliğin özlerden alınarak etkileşimlere atfedilmesidir. Daha önce ifade edildiği üzere Floridi gibi başka teknoloji felsefecileri de (Coeckelbergh, 2020; Feenberg, 2019), sanal dünya ile fiziksel olanın artık birbirinin karşıtı olarak konumlanmadığı, sanal denilen alanın gerçekliğin bizatihi kendisi haline dönüşerek günlük eylemler ve etkileşimlerle bütünleşmiş durumda olduğunu ileri sürmektedir. Özetle gündelik hayatı dijitalle fizikselin bütünleştiği bir alan olarak kurgulamanın kuramsal çerçeveleri uzun süredir çizilmektedir.

Floridi'ye (2022: 2) göre koltuklarımızdan kalkmadan farklı deneyimleri yaşayabileceğimiz bir sanal dünya tasavvuru olarak Metaverse eski bir rüyadır. Kavram, kullanıcıların avatarları aracılığıyla dijital gerçeklikler oluşturabilecekleri ve deneyimlerini paylaşabilecekleri internet tabanlı bir sanal dünyayı işaret etmek üzere ilk defa 1992 yılında Neil Stevenson'ın "Snow Crash" adlı bilim kurgu romanında kullanılmıştır (Park ve Kim, 2022: 4211). Kurgusal bir anlatı olarak otuz yıllık bir geçmişi olan Metaverse yakın zamanda Facebook platformunun adının "Meta" olarak değiştirilmesiyle gündemin önemli başlıklarından biri haline gelmiştir. Sınırlarının muğlaklığı ve kullanım farklılıkları nedeniyle Metaverse'ün tanımıyla ilgili bir uzlaşıdan söz etmek mümkün değildir. Mystakidis (2022: 486) Metaverse'ü fiziksel gerçekliği dijital sanallıkla birleştiren sürekli, kalıcı ve çok kullanıcılı bir gerçeklik sonrası evren olarak tanımlamaktadır. Bu tanımdan yola çıkarak Metaverse'ü önceki sanal gerçekliklerden ayıran en önemli özellik, çok sayıda kullanıcının bir arada olduğu çok boyutlu etkileşime imkân sağlayan sürekli bir ortam olmasıdır. Teknoloji şirketleri açısından bakıldığında Metaverse aynı fiziksel ortamda bulunmayan insanların bir araya gelerek, çalışmak, eğlenmek, öğrenmek, alışveriş etmek gibi bir dizi etkileşimi gerçekleştirebileceği bir sanal dünyadır (Bosworth ve Clegg, 2021).

Metaverse çoğu kez kullanıcıyı çevreleyen üç boyutlu bir evren olarak tahayyül edilir ancak meta veri deposu zorunlu olarak grafiksel değildir; fiziksel mekanın, mesafenin ve nesnelerin maddi varlıklarından soyutlanmasıyla ilgilidir (Radoff, 2021). Bu anlamda kullanıcıların Metaverse'deki varlıkları, fiziksel varlıklarının soyutlanarak kişisel verilere indirgenmesi anlamı taşır. Dolayısıyla Metaverse verileştirme süreçleri açısından bir sonraki teknolojik adımdır.

* Floridi'nin "onlife" kavramı metnin çevirmeni Vedat Kamer tarafından "yaşamiçi" olarak tercüme edilmiş, metinde de bu kullanım tercih edilmiştir.

Web 2.0 nasıl ki kullanıcıların ekranda hangi resme ne kadar baktıkları, hangi sayfalarda ne kadar zaman harcadıkları, fareyi nerede hareket ettirdikleri, hangi ürünleri ve hesapları beğendikleri gibi verilerin elde edilmesini mümkün kılmışsa (Di Pietro ve Cresci, 2021), Metaverse ile birlikte gündelik yaşam biçimlerinin bütünü ile iç içe geçmiş dijital teknolojilerin veri toplama becerileri büyük ölçüde keskinleşecek, kredi kartı işlem kayıtları, e-postalar, telefon görüşmeleri gibi yaygın yöntemlerin ötesinde akıllı telefon uygulamaları, biyometrik giyilebilir cihazlar, gözlük ve kasklar, yüz okuma teknolojileri, akıllı saatler gibi araçlardan veri elde edilebilecektir. Metaverse dayandığı teknolojilerin doğası gereği kullanıcıların kişisel bilgileri, alışkanlıklar ve seçimler gibi kullanıcı davranış bilgileri (Lee ve diğerleri, 2021: 39), profilleri, geçmişleri, bedenleri ve hatta zihinleri ile ilgili büyük miktarda veri toplama kapasitesine sahip olabilecektir (Bibri ve Allam, 2022: 17). Zira platform fikrinin merkezinde yer alan gerçek zamanlı etkileşimi kolaylaştırmak adına, kullanıcıların her hareketi, bakışı, sözü veri akışına dönüştürülerek diğer kullanıcılara anında yayınlanmalıdır (Nair ve diğerleri, 2022). Özetle Metaverse'ün biyometri, yüz ifadeleri, göz hareketleri, iris hareketleri, el hareketleri, beyin dalgası modelleri, alışkanlıklar, seçimler, kullanıcıların aktiviteleri, davranışlar, duygular, ifadeler, kullanıcı konuşmaları, internet geçmişi, vücut hareketleri, kültürel veriler, finansal veriler, iletişimler, konum, yaş, alışveriş tercihleri, favori filmler, kimlikler, tıbbi veriler, dijital varlıklar, sanal öğelerin kimliği, kripto para harcama kayıtları, fizyolojik veriler, fiziksel veriler gibi geniş kapsamlı bir veri toplama kapasitesine sahip olması öngörülmektedir (Canbay ve diğerleri, 2022: 84). Bu derece geniş çapta bir veri toplama kapasitesinin mahremiyet ve kontrol ile ilgili sorun ve riskleri derinleştirmesi kaçınılmazdır.

Metaverse Evreninde Mahremiyet

Lee ve diğerleri (2021: 37-38), Metaverse evrenindeki olası tehditleri mahremiyet endişesi, kapsayıcılık, adalet, bağımlılık ve siber saldırılar olarak sıralarken; Bibri ve Allam (2022: 6) tehditlerin sivil özgürlükler ve yönetimsellik alanlarını da kapsayacak şekilde genişleyebileceğini öne sürmektedir. Wang ve diğerleri (2022: 3) ise Metaverse'deki güvenlik ve gizlilik tehditlerini kimlik doğrulama, veri yönetimi, gizlilik, ağ, ekonomi, yönetişim ve fiziksel/sosyal etkiler olmak üzere yedi başlıkta değerlendirirler. Çalışma, veriye dayalılık odağına uygun biçimde Metaverse'ün veri yönetimi bağlamında içerebileceği mahremiyet endişelerini öncelemiştir. Zira yeni teknolojilerin geliştirilmesi ve kullanımıyla ilgili en önemli etik sorunlardan biri mahremiyettir.

Verileştirme ve mahremiyet birbiriyle yakından ilgilidir. Mahremiyetin sonuna işaret eden büyük veri çağında, insanların kendi başlarına bırakılma hakkına sahip olabilecekleri ve kendilerini dünyaya göstermemeyi seçebilecekleri bir yer bulması gittikçe zorlaşmaktadır. Toplanacak, analiz edilecek, sınıflandırılacak, metalaştırılacak muazzam miktarda veri göz önüne alındığında bu meselenin Metaverse'ün merkezinde de yer aldığı görülecektir. Öte yandan mahremiyetle ilgili endişe, insanların kendi yaşamları üzerine kontrol sahibi olmalarıyla ilgili daha büyük bir endişenin parçasıdır (Bibri ve diğerleri, 2022: 16). Bu anlamda bireylerin kişisel verilerinin üretimi, dağıtımı ve paylaşılması üzerindeki kontrollerinin ortadan kalkmasıyla da yakından ilgilidir. Teknoloji şirketleri sanal gerçeklik dünyasına giderek daha fazla dahil olmaya başladıkça son kullanıcıların kişisel verileri üzerindeki kontrolleri daha da zayıflayacak, kullanıcılar hangi bilgilerin açığa çıktığından

habersiz, kişisel verileri üzerinden kontrolünü yitirecektir.

Allen, bilgi mahremiyeti, fiziksel mahremiyet ve ilişkisel mahremiyet olmak üzere üç farklı mahremiyet türünden söz eder (O'Brolcháin ve diğerleri, 2016: 7). Bilgi mahremiyeti, bireyin düşünceleri, ifadeleri, yazışmaları, mali ve tıbbi kayıtları dahil olmak üzere birey hakkındaki kişisel bilgilerle ilgilidir. Mahremiyetin bu boyutu verilerin dijitalleştirilerek çevrimiçi olarak kaydedilmesi ve daha geniş insan grupları tarafında erişilebilir hale gelmesi nedeniyle tehdit altındadır. Bununla birlikte yukarıda söz edildiği gibi Metaverse ile toplanacak göz hareketleri, duyular, gerçek zamanlı tepkiler gibi ekstra bilgilerle kişisel bilgilere ilişkin mahremiyet tehdidinin derinleşeceği öngörülmektedir. Fiziksel mahremiyet bireyin bedeni ve eylemleri ile ilgilidir. Fiziksel mahremiyete yönelik tehditlerin başında kayıt cihazlarının yaygınlığı gelmektedir. Hem mobil cihazların ve hem de akıllı saat, gözlük gibi bedene entegre teknolojilerin yaygınlaşması fiziksel mahremiyetin korunmasını zorlaştıracaktır. Öte yandan Metaverse'ün duyusal etkileşimi mümkün kılması durumunda fiziksel mahremiyetle ilgili sorunları gündeme getireceği öngörülmektedir. Öyle ki şimdiden Metaverse'de cinsel tacize uğradığını ileri süren kullanıcı beyanlarıyla karşılaşılmaktadır. Son olarak ilişkisel mahremiyet bireyin etkileşime girmek istediği diğerleriyle ilgili kontrol sahibi olması anlamına gelmekle birlikte, fiziksel mahremiyetle oldukça yakından ilgilidir. Metaverse bu açıdan da mahremiyet ihlali olasılığını arttırabilir.

Di Pietro ve Cresci (2021) ise Metaverse'de kullanıcı mahremiyetine ilişkin kişisel bilgiler, davranış ve iletişim olmak üzere üç önemli alandan söz ederler. Metaverse bu alanların her birinde mevcut durumdan çok daha fazla veri toplanmasını mümkün kılacak ve yeni riskler doğuracaktır. Alanlar, uygulamalar ve topluluklar arasında çok sayıda bağlantı ile karakterize edilen Metaverse'de bu riskler kaçınılmaz olarak artacaktır. Öte yandan, daha fazla bağlantı daha fazla kişiler arası iletişim anlamına geldiğinden, bilginin toplanabileceği ve kötüye kullanılabileceği, siber suçların işlenebileceği sayı ve aracıların artmasına neden olması muhtemeldir.

Dijital teknolojilerde mahremiyeti korumak üzere kullanılan en yaygın yöntem bildirim ve onaydır. Ancak daha önce ifade edildiği gibi kullanıcılar sanal hizmetlerden yararlanabilmek için kendisine sunulan şartları kabul etmek durumundadır (Waldman, 2020). Öte yandan kullanıcıların söz konusu dijital ortamda veri paylaşımıyla ilgili yeterince bilgilendirilmiş olması, bu bilgileri anlayabilecek düzeyde bilgi birikimine ve bilgilendirmeleri okuyacak zamana sahip olması tartışmalıdır. Çoğu durumda insanlar bilinçli mahremiyet kararı vermek için gerekli bilişsel yetenekten ya da bilgiden yoksun olabilir. Sınırlı rasyonalite ve eksik bilgi, mahremiyet kararını belirleyen temel etmenlerdendir (Acquisti ve Jens Grossklags, 2005: 26). Araştırmalar kullanıcıların pek çoğunun kullanım hüküm ve koşullarını okumadan ve anlamadan onay verdiklerini göstermektedir (Bibri ve Allam, 2022: 8). Üstelik insanlar mahremiyet endişesi taşısalar bile bu her durumda mahremiyet davranışını doğurmamaktadır. Kullanıcılar mahremiyet konusuna büyük önem verdiklerini beyan ederken aynı zamanda önemsiz ödüller karşılığında önemli kişisel verilerini ifşa etme eğiliminde olabilmektedir. Sözde mahremiyet tercihleri ile gerçek davranışlar arasındaki bu tutarsızlık mahremiyet paradoksu olarak adlandırılmaktadır (Norberg ve diğerleri, 2007). Öte yandan çalışmalar pandemi ile birlikte sosyal etkileşim kurmak üzere dijital platformlara mahkum olmanın, kullanıcıların kişisel verilerini ifşa eğilimlerinin arttığını ileri sürmektedir (Nabity-

Grover, Cheung ve Thatcher, 2020). Dolayısıyla dijital platformlara bağlılıkla birlikte mahremiyet paradoksunun gün geçtikçe daha önemli bir sorun haline geleceği söylenebilir.

Bütün bunların yanında Metaverse ile birlikte hizmetlerin sınırı çok daha fazla genişleyeceğinden kullanıcılar erişim için çok daha fazla kontrol ve karar yetkisini devretmek zorunda kalacaklardır. Özellikle mahremiyet konusunda endişe duyan kullanıcının bu hususta dikkatli olması beklenir ancak şartların kapsamı ve karmaşıklığı bunun önündeki en büyük engellerdendir. Ayrıca kimi zaman mahremiyetle ilgili fayda maliyet analizi sonucunda mahremiyet endişesi karşısında benlik sunumu, sosyal ilişkilerin kurulması ve sürdürülmesi ve keyif almak gibi faydalar öne çıkmakta ve kullanıcıların mahremiyet davranışını belirlemektedir (Nabity-Grover, Cheung ve Thatcher, 2020: 2).

Dolayısıyla onay ve bildirim uygulamaları tatmin edici önlemler olmaktan uzaktır. Kişisel verilerin kullanımı söz konusu olduğunda tüm sorumluluğun son kullanıcıya verilmesi yerine tasarıma gömülü bir mahremiyetten söz etmek yerinde olacaktır (Lee ve diğerleri, 2021: 47). Bu noktada gözden kaçırılmaması gereken bir husus veriye dayalı ekonomide büyük şirketler, son kullanıcılar ve üçüncü taraflar arasındaki güç ilişkilerinin doğası gereği asimetrik olduğudur (Poell ve diğerleri, 2019: 6). Waldman (2020) teknoloji şirketlerinin platformları, kişisel verilerin ifşasını manipüle etmek ve kullanıcıları ifşaya yönlendirmek üzere tasarladıklarını ileri sürer. Dolayısıyla bu eşitsiz güç ilişkileri içinde son kullanıcı manipüle edilmeye müsait olarak dezavantajlı konumdadır. Bu nedenle sadece teknoloji şirketlerinin politikalarına bırakılan bir tasarım fikrinin kullanıcılar açısından olumsuz sonuçları olacağı ortadadır.

Meta Şirketi, Metaverse'deki sorunlar ve fırsatlar üzerinde düşünmek için politika yapıcılar, uzmanlar ve sektör ortaklarıyla iş birliği içinde çalışıldığını ve birkaç temel alan belirlendiğini öne sürmektedir. Bu temel alanlar arasında gizlilik, güvenlik, eşitlik ve kapsayıcılık başlıkları bulunmaktadır (Bosworth ve Clegg, 2021). Metaverse'ün sürdürülebilirliği, bu etik endişelerin ve tehditlerin göz önünde bulundurulduğu bir tasarım süreciyle bağlantılıdır. Doğrulanabilir bir mahremiyet mekanizması oluşturmak, toplumsal kabul için çözülmesi gereken en önemli sorunlardan biri olarak görülmektedir (Lee ve diğerleri, 2021: 21).

Sonuç

İnsanlık yaklaşık otuz yıl boyunca bilim kurgu olarak resmedilen sanal evren fikrine bugün her zamankinden daha yakın görünüyor. Ancak kullanıcıların bugüne kadarki deneyimlerinden çok farklı deneyimler vaat eden Metaverse, dijital geleceğe ilişkin ilham verici vizyonuyla birlikte bazı kritik sorunları ve riskleri de beraberinde getirmektedir. Dijital teknolojilerin gündelik yaşam pratikleri ile iç içe geçmesi birtakım endişeleri beraberinde getirmekle birlikte Metaverse ile birlikte bu endişelerin giderek daha da derinleşeceği öngörülmektedir. Zira Metaverse; yapay zeka, nesnelerin interneti, blok zincir, sanal gerçeklik, artırılmış gerçeklik gibi bir dizi teknolojinin entegre edilmesiyle ve iç içe geçmesiyle inşa edilen bir evrendir ve bu teknolojilere içkin güvenlik açıklarını ve sorunlarını içermesi (Wang ve diğerleri, 2022: 2) hatta riskleri daha karmaşık hale getirmesi (Chen ve diğerleri, 2022) muhtemeldir.

Bu risk ve sorunlar listesinin başında kitlesel veri akışlarının yönetimi ve kullanıcıların kişisel bilgilerine ilişkin güvenlik ve mahremiyet endişeleri yer almaktadır. Metaverse'ün gerçek zamanlı etkileşimsel deneyim vaadinin gerçekleşmesi devasa büyüklükteki verinin güvenli bir şekilde birleştirilmesiyle/bütünleştirilmesiyle mümkün olacağından; mevcut internet teknolojileriyle karşılaştırıldığında Metaverse, daha önce toplanmamış yüz ifadesi, baş ve göz hareketleri gibi bedensel veri türlerine ihtiyaç duymaktadır. Bu son derece kişisel verilerin üretilmesi ve depolanması olası saldırı durumlarında ciddi tehlikeleri beraberinde getirebilir. Bu anlamda henüz ortaya çıkmakta olan bu sanal dünyanın güvenlik ve gizlilik sorunlarını çözecek araçlarla yapılandırılması kritik öneme sahiptir.

Öncelikle Metaverse de dahil olmak üzere insanlığı doğrudan ve keskin bir şekilde etkileyecek teknolojiler; kullanıcıların ihtiyaç, istek ve görüşlerine uygun biçimde, ahlaki değerleri ve ilkeleri göz ardı etmeden, sosyal yıkıcı etkilerin farkında olarak şekillendirilmeli ve tasarlanmalıdır. Bu anlamda mahremiyet, güvenlik ve gizlilikle birlikte adalet, kontrol ve hesap verebilirlik gibi kamu değerlerini ve ortak iyiyi tanzim etme sorumluluğu sadece teknoloji şirketlerinin tekeline bırakılmamalıdır. Tasarımcılarla birlikte kullanıcıların ve politika yapıcıların birlikte yer aldığı daha katılımcı bir tasarım sürecine ihtiyaç duyulmaktadır. Zira insanların mahremiyetini korumak ve özerkliklerini garanti altına almak, her üç grubun da uzun vadede faydasınadır.

İkinci olarak konuyla ilgili yasa ve yönetmeliklerin geliştirilmesinin ve iyileştirilmesinin gerekliliğinden söz edilmelidir. Teknoloji çok hızlı geliştiğinden gerekli hukuksal düzenlemeler genellikle geride kalmaktadır. Metaverse merkeziyetsiz ve anonim yapısı nedeniyle muhtemelen kontrol edilmesi çok daha zor bir alan olacaktır. Bu nedenle veriler için sorumluluğun dağıtılması, hesap verebilirlik gibi konularda düzenlemeler hızla hayata geçirilmelidir. Ayrıca kullanıcıların mahremiyet davranışını etkileyen koşulların analizi, veri koruma yasalarının kullanıcı lehine yeniden düzenlenmesinin önünü açabilir.

Son olarak Metaverse de dahil dijital teknolojilerle ilişkili etik sorunların boyutunun belirlenmesi ve temel çelişkiler, belirsizlik ve etik sonuçlara ilişkin uygun yanıtlar geliştirmek üzere daha fazla araştırmaya ihtiyaç duyulduğu da eklenmelidir. Öte yandan bu araştırmaların, konunun sadece teknik yanına odaklanan bilgisayar bilimleri ve mühendislik alanlarında değil, hukuktan felsefeye sosyolojiden psikolojiye uzanan bir dizi farklı disiplinde yürütülmesi meselenin farklı boyutlarıyla ele alınmasını mümkün kılacaktır.

Kaynakça

Acquisti, A., ve Grossklags, J. (2005). Privacy and rationality in individual decision making. *IEEE Security & Privacy*, *3*(1), 26–33. https://doi.org/10.1109/MSP.2005.22

Acquisti, A., Brandimarte, L., ve Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science*, *347*(6221), 509-514. https://doi.org/10.1126/science.aaa1465

Al-Khatib, T. (2023). Netiquette rules in online learning through the lens of digital citizenship scale in the post-corona era. *Journal of Information*

Communication and Ethics in Society, *21*(2), 181-201. https://doi.org/10.1108/JICES-08-2021-0089

Baudrillard, J. (2006). *Kusursuz cinayet*. N. K. Sevil (Çev.). Ayrıntı Yayınları.

Bibri, S. E., ve Allam, Z. (2022). The Metaverse as a virtual form of data-driven smart cities: The ethics of the hyper-connectivity, datafication, algorithmization, and platformization of urban society. *Computional Urban Science*, *2*(22). https://doi.org/10.1007/s43762-022-00050-1

Bibri, S. E., Allam, Z., ve Krogstie, J. (2022). The Metaverse as a virtual form of data-driven smart urbanism: Platformization a and its underlying processes, institutional dimensions, a and disruptive impacts. *Computional Urban Science, 2*(24). https://doi.org/10.1007/s43762-022-00051-0

Bosworth, A., ve Clegg, N. (2021, 7 September). Building the Metaverse responsibly. *Economist Impact*. https://about.fb.com/news/2021/09/building-the-metaverse-responsibly/

Canbay, Y., Utku A., ve Canbay, P. (2022, 19-20 Ekim). *Privacy concerns and measures in Metaverse: A review [Konferans sunumu]*. 15th International Conference on Information Security and Cryptography, Ankara, Türkiye. https://ieeexplore.ieee.org/document/9931866

Coeckelbergh, M. (2020). The postdigital in pandemic times: A comment on the Covid-19 crisis and its political epistemologies. *Postdigital Science and Education, 2*, 547–550. https://doi.org/10.1007/s42438-020-00119-2

Cukier, K. N., ve Mayer-Schöenberger, V. (2013). *Big data: A revolution that will transform how we live, work, and think*. Haughton Miffin Harcourt.

Demircioğlu, Z. (2021). Akışkan dünyada pandemi. *Spektrum, 4*, 111-114. https://doi.org/10.1007/s42438-020-00119-2

Demircioğlu, Z. (2023, 1-3 Şubat). *Gözetimin dijitalleşmesi: Pandemi sürecinde yeni gözetim biçimleri [Konferans sunumu]*. 17. Türk Sosyal Bilimler Kongresi, Ankara, Türkiye. http://tsbd.org.tr/?p=1312

Di Pietro, R., ve Cresci, S. (2021, 13-15 December). *Metaverse: Security and privacy issues [Conference presentation]*. Third IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications, Virtual Conference. https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9750221

Feenberg, A. (2019). Postdigital or predigital?. *Postdigital Science and Education, 1*, 8–9. https://doi.org/10.1007/s42438-018-0027-2

Floridi, L. (2015). *The onlife manifesto: Being human in a hyperconnected era*. Springer Nature.

Floridi, L. (2017). Yaşamiçi manifestosu: Hiperbağlı bir çağda insan olmak. V. Kamer (Çev.), *Kutadgubilig Felsefe-Bilim Araştırmaları*, *35*, 203-211.

Floridi, L. (2022). Metaverse: A matter of experience. *Philosophy ve Technology*, *35*(3). https://doi.org/10.1007/s13347-022-00568-6

Ganaele, L., ve Elmer, G. (2013). The research politics of social media platforms. *Culture Machine, 14*.

Kitchin, R. (2020). Civil liberties or public health, or civil liberties and public health? Using surveillance technologies to tackle the spread of Covid-19. *Space and Polity*, *24*(3), 362–381. https://doi.org/10.1080/13562576.2020.1770587

Laney, D. (2001). 3D data management: Controlling data volume, velocity and variety. *META Group Research Note*, *6*(70), 1-4.

Lee, L. H., Braud, T., Zhou, P., Wang, L., Xu, D., Lin, Z., Kumar, A., Bermejo C., ve Hui P. (2021). All one needs to know about Metaverse: Acomplete survey on technological singularity, virtual ecosystem, and research agenda. *arXiv preprint*. Erişim Haziran 20, 2023, https://arxiv.org/abs/2110.05352

Li, V., Ma, L., ve Wu, X. (2022). COVID-19, Policy change, and post pandemic datagovernance: A case analysis of contact tracing applications in east asia. *Policy and Society*, *41*(1), 129-142. https://doi.org/10.1093/polsoc/puab019

Mañero, J. (2020). Postdigital brave new world and its educational implications. *Postdigital Science Education*, *2*, 670–674. https://doi.org/10.1007/s42438-020-00129-0

Mills, K. (2018). What are the threats and potentials of big data for qualitative research?. *Qualitative Research*, *18*(6), 591-603. https://doi.org/10.1177/1468794117743465

Mystakidis, S. (2022). Metaverse. *Encyclopedia, 2*(1), 486-497. https://doi.org/10.3390/encyclopedia2010031

Nabity-Grover, T., Cheung, C. M. K., ve Thatcher, J. B. (2020). Inside out and outside in: How the COVID-19 pandemic affects self-disclosure on social media. *International Journal of Information Management*, *55*, 102188. https://doi.org/10.1016/j.ijinfomgt.2020.102188

Nair, V., Garrido G. M., ve Song, D. (2022). Exploring the unprecedented privacy risks of the Metaverse. *arXiv*. https://arxiv.org/abs/2207.13176.

Nissenbaum, H. (2009). *Privacy in context-technology, policy, and the integrity of social life*. Stanford University Press.

Norberg, P. A., Horne, D. R., ve Horne, D. A. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs*, *41*(1), 100-126. https://doi.org/10.1111/j.1745-6606.2006.00070.x

O'Brolcháin, F., Jacquemard, T., Monaghan, D., O'Connor, N., Novitzky, P., ve Gordijn, B. (2016). The convergence of virtual reality and social networks: Threats to privacy and autonomy. *Science and Engineering Ethics*, *22,* 1-29. https://doi.org/10.1007/s11948-014-9621-1

O'Neil, C., ve Schutt, R. (2013). Doing data science: Straight talk from the frontline. O'Reilly Media Inc.

Park, S. M., ve Kim, Y, G. (2022). A Metaverse: Taxonomy, components, applications, and open challenges. *IEEE access*, *10,* 4209-4251. https://doi.org/10.1109/ACCESS.2021.3140175.

Poell, T., Nieborg D., ve van Dijck, J. (2019). Platformisation. *Internet PolicyReview*, *8*(4), 1-13. https://doi.org/10.14763/2019.4.1425

Radoff, J. (2021, 7 April). The Metaverse value-chain. *Medium*. https://medium.com/building-the-metaverse/the-metaverse-value-chain-afcf9e09e3a7

Rosenberg, J. M. (1969). *The Death of Privacy*. Random House.

Sadowski, J. (2020, 13 April). The authoritarian trade-off: Exchanging privacy rights for public health is a false compromise. *Real Life Magazine*. https://reallifemag.com/the-authoritarian-trade-off/

The Economist (2017, 6 May). The world's most valuable resource is no longer oil, but data. https://l24.im/hVcxM

van Dijck, J. (2014). Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology. *Surveillance & Society*, *12*(2), 197-208. https://doi.org/10.24908/ss.v12i2.4776

Vincent, D. (2016). *Mahremiyet: kısa bir tarih*. D. C. Başaraner (Çev.). Epos Yayınları.

Waldman, A. E. (2020). Cognitive biases, dark patterns, and the privacy paradox. *Current Issues in Psychology*, *31*, 101-105. https://doi.org/10.1016/j.copsyc.2019.08.025

Wang, Y., Su, Z., Zhang, N., Xing, R., Liu, D., Luan, T. H., ve Shen, X. (2022). A survey on Metaverse: Fundamentals, security, and privacy. *IEEE Communications Surveys & Tutorials, 25*(1), 319-352. https://doi.org/10.1109/COMST.2022.3202047

Yıldırım, F. E. (2021). İletişim çalışmaları ve psikoloji birlikteliğinin önemi: COVID-19 pandemisi bağlamında disiplinler arası bir analiz. *Türkiye İletişim Araştırmaları Dergisi*, *38*, 155-173. https://doi.org/10.17829/turcom .862297

Zuboff, S. (2015). Big other: surveillance capitalism and the prospects of an information civilization. *Journal of information technology*, *30*(1), 75-89. https://doi.org/10.1057/jit.2015.