

Yayın Geliş Tarihi: 08.07.2021
Yayına Kabul Tarihi: 23.05.2022
Online Yayın Tarihi: 30.06.2022
<http://dx.doi.org/10.16953/deusosbil.966959>

Dokuz Eylül Üniversitesi
Sosyal Bilimler Enstitüsü Dergisi
Cilt: 24, Sayı: 2, Yıl: 2022, Sayfa: 801-835
ISSN: 1302-3284 E-ISSN: 1308-0911

Araştırma Makalesi

BÜYÜK VERİ TEKNOLOJİSİ ÇAĞINDA KULLANICI VERİLERİNİN MAHREMİYETİNE İLİŞKİN SOSYOLOJİK ANALİZ¹

Seda OFLAS*
Nilüfer ÖZCAN DEMİR**

Öz

21. yüzyılın bilgi ve iletişim teknolojileri, dijital kullanıcı verilerini teknik bir araç olarak kullanmakta ve gelişmiş veri analiz teknolojileri ile endüstriyel üretimi daha verimli ve etkin bir hale getirmeyi hedeflemektedir. Büyük veri teknolojileri, internet kullanıcıları üzerinde sürekli bir gözetim sağlamak ve kullanıcılar tarafından üretilen verileri kullanarak gelişmiş analiz yöntemleri ile isabetli çıkarımlar yapabilmektedir. Büyük veri analiz tekniklerinin, kullanıcılara ilişkin detaylı davranışsal verileri toplayabilme ve işleme gücü, kullanıcı verilerinin gizlilik ve mahremiyetine ilişkin endişeler yaratmaktadır. Veri teknolojilerinin gelişim aşamalarına dair bir özet sunan ve bu teknolojilerin içerdiği tehlikeleri, kapitalizmin süregelen ve yeni dinamikleri ile bağlantısı dahilinde analiz eden bu çalışma, 307 kişi ile yapılan bir anket uygulamasını içermektedir. Anket, katılımcıların kişisel ve davranışsal verilerine ilişkin temkinlilik ve endişe düzeylerini, internet kullanım alışkanlıklarını, dijital becerilerini, veri gizliliği ihlallerine ilişkin farkındalık düzeylerini ölçen sorulardan oluşmaktadır. Örneklem 3 farklı teknolojik uzmanlık düzeyini içerecek şekilde, Hacettepe Üniversitesi Sosyoloji, Felsefe ve Bilgisayar Mühendisliğinden öğrenciler ile Hacettepe Teknokent'teki teknoloji firması çalışanları arasından seçilmiştir. Çalışma sonucunda, katılımcıların günlük internet kullanma sıklıkları arttıkça davranışsal ve hassas verilerine ilişkin endişe duyma olasılıklarının da yükseldiği bulunmuştur. Kullanıcıların davranışsal verilerine ilişkin tutumları, günlük internet kullanma sıklıklarına ve katılımcıların uzmanlık seviyesine göre farklılık göstermektedir. Çevrimiçi profillemeye ilişkin farkındalığın, katılımcılar arasında yaygın olduğu ancak çevrimiçi davranışlarına ilişkin verilerini gizli tutma alışkanlığının yaygın olmadığı gözlemlenmiştir. Bulgular genel

* Bu makale için önerilen kaynak gösterimi (APA 6. Sürüm):

Oflas, S., Özcan Demir, N. (2022). Büyük veri teknolojisi çağında kullanıcı verilerinin mahremiyetine ilişkin sosyolojik analiz. *Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, 24 (2), 801-835.

Çalışma için, 20.03.2019 tarih 12908312-300/000000515333 sayılı etik kurul onayı alınmıştır. Katılımcılardan bilgilendirilmiş onam formu alınmıştır.

¹ Bu makale “Büyük Veri Teknolojisi Çağında Kullanıcı Verilerinin Gizlilik ve Mahremiyetine İlişkin Sosyolojik Analiz” (2020) başlıklı Yüksek Lisans tezinden üretilmiştir.

* Yüksek Lisans Mezunu, ORCID: 0000-0001-8367-2344. sedaoflas@gmail.com.

** Doç. Dr., Dokuz Eylül Üniversitesi, Edebiyat Fakültesi, Sosyoloji Bölümü, ORCID: 0000-0002-0626-6251. nilufer.ozcandemir@deu.edu.tr.

olarak değerlendirildiğinde, katılımcıların veri teknolojilerinin profillemeye kapasitesi hakkında bilgi düzeylerinin düşük olması durumunda, davranışsal veri gizliliklerini sağlayamadıkları fark edilmektedir. Bu araştırma, örneklemin araştırma evrenini temsil etme kapasitesi bağlamında sınırlılıklara sahiptir. Ancak büyük veri teknolojilerinin gelişimine ilişkin tarihsel arka planı çizmesi, bu teknolojiyi kapitalizmin dinamikleri içerisinde analiz etmesi ve kullanıcıların kişisel verileri ve davranışsal verilerine yaklaşımları arasındaki farklara dikkat çekmesi bakımından yararlı olacağı düşünülmektedir.

Anahtar Kelimeler: Büyük Veri, Enformasyon Teknolojileri, Çevrimiçi Profillemeye, Kullanıcı Gizliliği, Gençlik ve Davranışsal Veri.

A SOCIOLOGICAL ANALYSIS OF THE PRIVACY OF USER DATA IN THE ERA OF BIG DATA²

Abstract

The information and communication technologies of the 21st century use digital user data as a technical tool and aim to increase the efficiency and profitability of industrial production through the use of advanced data analysis technologies. Big data technologies carry out continuous surveillance on internet users and can reach accurate inferences through advanced analysis methods by using data generated by users. The ability of big data analysis techniques to collect and process detailed behavioral data about users raises concerns regarding the privacy and confidentiality of user data. This study, which provides a summary of the developmental stages of data technologies and analyses the dangers contained in these technologies in connection with the ongoing and new dynamics of capitalism, includes a survey of 307 people. The survey consists of questions that measure participants' levels of caution and anxiety regarding their personal and behavioral data, internet usage habits, digital skills, and awareness levels of data privacy breaches. The sample included students selected from the Departments of Sociology, Philosophy and Computer Engineering at Hacettepe University and technology company employees at Hacettepe Teknokent to include three different levels of technological expertise. The study found that participants were also more likely to be concerned about their behavioral and sensitive data as their frequency of daily internet use increased. Users' attitudes to behavioral data vary according to their frequency of daily internet use and the level of expertise of the participants. Participants demonstrated a high level of awareness of online profiling, but the habit of keeping data regarding their online behavior private is not widespread. When the findings are evaluated broadly, it is noted that participants with a limited knowledge of the profiling capacity of data technologies are unable to maintain behavioral data confidentiality. This research has limitations in the context of the sample's capacity to represent the research universe. However, it is thought that it will prove useful in drawing the historical background for the development of big data technologies, analysing this technology within the dynamics of capitalism and in drawing attention to the differences between users' approach to personal data and behavioral data.

² This article is an extract from the Master's thesis entitled "The Privacy of User Data in an Age of Big Data: A Sociological Analysis" (2020).

Keywords: *Big Data, Information Technologies, Online Profiling, User Privacy, Young Generation and Behavioral Data.*

GİRİŞ

Günümüzde internet teknolojileri, günlük hayatın ayrılmaz bir parçası haline gelmiştir. İnternete bağlı olan her cihazın sürekli olarak veri ürettiği ve internet kullanıcılarının da bu hızlı veri dolaşımında asıl üreticiler olduğu çağımızda, gelişen ve çok hızlı ilerleyen dijitalleşme süreci, geçtiğimiz on yılın en çok tartışılan konularından da biri olmuştur. Günümüzde internet teknolojilerinin yaygınlaşması ile birlikte, bu teknolojilerin bilgiye erişim eşitsizliğini ortadan kaldırıp kaldırmayacağı, internet kullanımının birincil ve ikincil toplumsal ilişkiler üzerindeki olumlu ya da çoğunlukla olumsuz olan etkileri, internetin tarafsızlık niteliğini giderek kaybetmesi ve manipülasyon aracı olarak kullanılması, siber zorbalık, düşük medya okur yazarlığı oranları, dijital beceri eksikliği gibi bazı problemler, alan yazını üzerinde tartışılmaya başlanmıştır.

İnternetin artık çalışma ve eğitim hayatı için bir gereklilik olduğu, iletişimin başlıca kanalı haline geldiği, gündelik işlerde birçok pratik kolaylık sağladığı bu dijital çağda, bireylerin gündelik hayattaki her eylemi veri üretmekte ve bu veriler, internet hizmeti sağlayıcıları tarafından analiz edilmek üzere saklanmaktadır. Büyük veri teknolojilerinin gelişimi ile birlikte, internet kullanıcılarının sınırsızca ürettiği bu verilerin, kar elde etme aracı olarak kullanıldığı yeni bir sistem kurulmuştur. Büyük veri teknolojilerinin ortaya çıkardığı bu veri depolama ve analiz kapasitesi, küreselleşen ekonominin de yeni dinamiklerini oluşturmaktadır. Bununla birlikte yaşanan bu durum, veri sahipliği ile ilişkili yeni eşitsizlik biçimlerini de ortaya çıkarmıştır. Büyük veri teknolojileri ile ilişkili toplumsal problemlere ilişkin literatürde, algoritmik eşitsizlik, veri gizliliği ihlalleri, veri sömürsü, Toplum 5.0 gibi sosyo-tekniik sistemlerin stratejik hedefleri, veri odaklı karar verme mekanizmalarının etik problemleri, teknoloji endüstrisindeki şirket yapıları, kullanıcı verilerinin gizlilik ve güvenliğine ilişkin yasal düzenlemeler ve karşılaşılan problemler tartışılan başlıca konular arasındadır.

Bu araştırmada amaçlanan, büyük veri teknolojilerinin yarattığı ileri veri analiz teknikleri kapsamında, kullanıcıların veri gizliliklerine ve mahremiyetlerine ilişkin endişe düzeylerini, veri gizliliklerini sağlama konusunda farkındalık düzeylerini, veri gizliliklerine verdikleri önem düzeylerini incelemektir. Bu sözü geçen unsurların toplanan veri türlerine, internet kullanım alışkanlıklarına ve teknoloji kullanım uzmanlık düzeylerine göre farklılık gösterip göstermediği analiz edilmiştir. Uluslararası literatürün en güncel tartışmalardan biri olan büyük veri teknolojilerinin ortaya çıkardığı toplumsal problemlerin, ulusal alan yazınındaki durumuna baktığımızda, konunun ülkemizde de giderek önem kazandığı, yapılan çalışmalarda görülmektedir. Dijital eşitsizliklerin yarattığı temel problemler (Gökalp ve Sütlüoğlu, 2021), dijitalleşen dünyada büyük verinin kullanımı ile oluşan gözetim

toplumu ve onun yarattığı problemler (Zinderen, 2021), yeni iletişim teknolojileri ve oluşan çevrimiçi topluluklar (Karaman, 2021), yeni iletişim teknolojileri bağlamında kimlik ve dönüşümü (Zinderen, 2021), dijital sosyoloji temel alanı çerçevesinde (Aydın 2021) problemin önemine dair yapılan ulusal çalışmalardan sadece birkaçıdır.

Bu çalışmada, enformasyon ve iletişim teknolojilerindeki dijitalleşmeye ilişkin en güncel tartışma konularından biri olan büyük veri teknolojilerinin, kapitalist ekonominin dinamikleri içerisinde hangi dinamikleri ürettiği de ele alınmaktadır. Bu anlamda, Christian Fuchs'un tarihsel materyalizmin temel argümanları çerçevesinde geliştirdiği teorisi ile büyük verinin gözetleme kapasitesinin, bireylerin gizliliği ve mahremiyeti ile ilgili ne tür değişimler yarattığı da tartışılacaktır. Çalışmada yürütülen tartışmaların temel hedefi, kapitalizmin dinamikleri içerisinde daha fazla kar elde etme hedefiyle gerçekleştirilen kullanıcı verilerinin metalaştırılması sürecinin, kullanıcıların veri gizliliğini ve kullanıcı mahremiyetini tehdit eden unsurlarına dikkat çekmektir.

Çalışmanın özgün bakışı çerçevesinde veriler; kullanıcı verileri, kişisel veriler, davranışsal veriler ve hassas veriler arasında bir ayrım gözetilerek ele alınmıştır. Kişisel veriler, kullanıcılara ait demografik bilgileri, konum bilgileri ve parolalar gibi bireylerin çevrimdışı dünyada da gizlilik ve mahremiyet kapsamında korumaya aldıkları bilgilerdir. Bireylerin dijital platformlarda bu bilgilerinin gizliliğine ilişkin olarak duyacakları endişelerin, bilgilerin güvenliğine yönelik farkındalık taşımalarını ve bu tür verilerin güvenliğini sağlama konusunda daha bilinçli olmalarını sağlayacağı düşünülmektedir. Davranışsal veriler ise, bireylerin internete bağlı oldukları her an, sürekli olarak ürettikleri ve çoğu zaman ürettiklerinin dahi farkında olmadıkları verilerdir. Büyük verinin ileri analiz kapasitesi ile değer ve anlam kazanmış olan bu veri türü, kullanıcıların internet kullanım alışkanlıklarına dair örüntülerden yola çıkılarak, bir sonraki davranışlarının öngörülmesine yardımcı olmaktadır.

KAVRAMSAL ÇERÇEVE

Veri Teknolojisine İlişkin Kavramlar

Veri, olgu, kavram ya da komutların, iletişim, yorumlama ve işlem için kullanılabilir duruma getirilme özelliği olan bilgi ortamı, kayıtlar bütünlüğüdür (Ayverdi, 2008, s.3359) Bu konuda Sadowski (2019, s. 2) de veriyi, teknoloji kullanan insanların yarattığı ve değer biçtiği bir dünyanın, kayıt altına alınmış soyut bir hali olarak tanımlamıştır.

Kişisel veri, Avrupa Birliği'nin veri koruma yasalarında tanımlandığı şekliyle, hayatta olan kişilerin kimlik bilgilerini içeren ya da kimlik tespitinin yapılmasına olanak sağlayan her türlü enformasyonu kapsamaktadır. Tekrar kimlik teşhisi yapılabilecek şekilde kimliksizleştirilen, şifrelenen ya da anonimleştirilen veriler de kişisel veri kapsamında değerlendirilmektedir. İsim, soy isim, ev adresi, isim-soy isim içeren mail adresleri, kimlik numarası, konum bilgisi, IP adresi,

telefonların ticari kimliği, kişisel veri olarak değerlendirilirken; anonimleştirilmiş veriler, kimlik bilgisi içermeyen mail adresleri, şirket sicil numaraları ise kişisel veri kapsamının dışında bırakılmaktadır (Handbook on European Data Protection Law, 2018, s. 420).Türkiye'nin Kişisel Verileri Koruma Kanunu'nda ise, kişisel verilerin, kimlikleri belirli veya belirlenebilir asıl kişiye ilişkin tüm bilgiyi ifade ettiği belirtilmektedir (Kişisel Verilerin Korunması Kanunu, 2016).

Davranışsal veriler, kullanıcıların ürettikleri çevrimiçi içerikleri, tekrarlanan website gezintileri, etkileşimleri, arattıkları ya da yazdıkları anahtar kelimeleri içermektedir. Davranışsal verilerin, büyük veri gibi gelişmiş algoritmalar kullanan bir teknoloji kullanılarak işlenmesiyle birlikte, veriyi kullanıcıların tutum ve davranışlarını kategorilendirmek için kullanmanın da bir adım ötesine geçilerek, kullanıcının ses örüntülerine (örneğin çekingen bir sesle mi konuşuyor, özgüvenli bir sesle mi), mesaj yazarken uyguladıkları kuvvete (hangi mesaj yazılırken harflere daha sert hareketlerle basılmış) ya da vücut sıcaklıklarına ilişkin verilerden de anlam çıkarmak mümkün hale gelmiştir (Handbook on European Data Protection Law, 2018, s. 359).

Hassas nitelikli verilere gelince, Avrupa Birliği Veri Koruma Yasası hassas nitelikli verileri, bireylerin etnik köken, siyasi görüş, felsefi ya da dini inancı, mezhebi, giyinişleri, sosyal gruplara üyelikleri, sağlıkları, ceza ve güvenlik tedbirleriyle ilgili verileri ile biyo-metrik ve genetik verilerini, kişiye özel hassas nitelikli veri olarak kabul etmektedir (Handbook on European Data Protection Law, 2018, s.96).

Büyük Veri, hacim, çeşitlilik ve hız bakımından büyük olan verinin toplanması, işlenmesi ve bu veriden öngörücü ve yeni bilginin çekip çıkarılmasını mümkün kılacak şekilde gelişen teknolojik kapasiteyi ima etmektedir. Bu kapasite ayrıca, bireyleri ve grupları ilgilendiren karar verme hedefleri için, bir veri analizi yazılımı aracılığıyla yeni ve öngörücü bilgiyi sentezlemeyi de içermektedir (Europe, 2017).

Büyük Veri Gözetimi Kavramı

Alan yazınında, enformasyon ve iletişim teknolojilerinin gelişimi ile toplumsal dünyanın ekonomik, politik ve kültürel unsurlarının, önceki dönemlerden farklı biçimler aldığı konusunda bir uzlaşma mevcuttur. Ancak bu değişen biçimlerin, kapitalist ekonominin bir uzantısı olup olmadığı, kapitalist ekonominin önceki dönemlerden daha az ya da daha fazla sömürüye dayandığı konusunda görüş ayrılıkları bulunmaktadır. Bu bağlamda, enformasyon ve iletişim teknolojilerine bağlı değişmeyi inceleyen teoriler arasında, kapitalizmin dinamiklerinde bir süreklilik mi yoksa bir çeşit kopuş mu gözlendiğine göre bir ayırım yapılabilmektedir. Gerçekleştirilen bu ayırmda 4 temel teorik eğilim belirlenmektedir. Bu teorik eğilimler, dijital teknolojilerin kapitalizmin dinamikleri içerisinde nasıl konumlandırılacağına dair bir tartışma da sunmaktadır. Çalışmamızda bu teorik eğilimlerin temel argümanlarının ortaya koyulmasının ardından, Fuchs'un teorik yaklaşımı ele alınacaktır.

Bu eğilimlerden ilki, enformasyon ve iletişim teknolojilerine bağlı değişme ile toplumsal dünyanın tüm dinamiklerinin radikal bir dönüşüme uğradığını ve bu dönüşüm dolayısıyla Marksist anlamda bir kapitalist toplumdaki söz edilemeyeceğini iddia eden açıklamalardır. Webster'in de (2014, s.347) ifade ettiği gibi, enformasyon teknolojilerinin gelişimi ile devrimsel dönüşümler gerçekleştiğini iddia etmek, toplumsal değişimde, failerin kendilerini bu değişime uyumlamak ve ona alışmak dışında başka bir şansları olmadıkları algısını yaratmaktadır. Castells'in "enformasyonel kapitalizm" anlayışı, bu ilk eğilimin en önemli örneklerinden biridir. Castells (1996) ağ toplumu teorisinde, 198'lerde başlayan enformasyon devrimi ve küreselleşme eğilimleri ile küresel ağların ve küresel enformasyon akışlarının temel işlev kazandığı yeni bir tekno-ekonomik sistemin ortaya çıktığını iddia etmektedir.

İkinci eğilim ise, toplumsal dünyanın köklü bir değişim geçirdiğini kabul etmekte ancak enformasyon toplumu gibi radikal değişim ima eden söylemleri reddetmektedir. Bu eğilim, enformasyon teknolojilerinin yeni bir toplum inşa ettiğini savunan görüşleri, neo-liberal ideolojinin bir uzantısı olarak görmekte ve bunu bir tekno-optimizm ve teknolojik determinizm olarak yorumlamaktadır (Fuchs ve Chandler, 2019, s.10). Golding (2000, s.170), enformasyonun değerinde ve miktarında saptanan devrim niteliğindeki artışa dikkat çeken enformasyon toplumu teorilerini, bilgisayar ve iletişim teknolojilerindeki gelişmelerin şirketleştirilmesi ve enformasyonun serbest piyasanın yayılmasını sağlayacak şekilde özelleştirilmesi hedeflerini desteklemekle eleştirmekte ve teknolojinin yeni potansiyellerine çok fazla yoğunlaşan teorilerin, bu potansiyellerin nasıl önlendiğinin eleştirisini yapamadıklarını düşünmektedir.

Düşünceleri ikinci eğilimde değerlendirilebilecek diğer bir teorisyen ise Herbert Schiller'dir. Schiller'a göre (1973, ss.19-21), enformasyon toplumu teorisyenlerinin, teknolojiye gelişmelerin demokratikleşmeyi getireceği ve farklı görüşlerin yaratılmasını sağlayacağı yönündeki iddiaları isabetli değildir. Çünkü büyük medya şirketleri, bu şirketlerin sahiplerinin ve reklamcılarının çıkarlarına ters düşecek her şeyi dışarıda bırakacak şekilde görüntü, haber ve eğlence akışını filtrelemektedirler. Bu akışların filtrelenmesi ve çıkar sahiplerinin hedefleri doğrultusunda izleyicilerin bilinçlerinin manipüle edilmesi, toplumsal ilişkilerin metalaştırılmasını sistematik olarak şiddetlendirilmektedir.

Üçüncü eğilimde ise, çağdaş kapitalizmin bir türü ve mevcut dönemdeki en temel boyutu olarak "bilişsel kapitalizm"den söz edilmektedir. Bu yaklaşım otonom Marksizm yaklaşımı içerisinde gelişmiştir. Bilişsel kapitalizmin teorisyenlerinden olan Vercellone, bu isimlendirmedeki "kapitalizm" in, kapitalist üretim biçimindeki değişmeyen yapısal faktörlere işaret ettiğini, "bilişsel" ifadesinin ise emek ve sermaye arasındaki çelişkili ilişkinin yeni doğasına ve sermaye birikimini sürdüren yeni sahiplik biçimlerine dikkat çektiğini ifade etmiştir. Bilişsel kapitalizm teorisinin geliştirilmesinin sebeplerinden biri, kitlesel üretim ile sermaye birikimine ilişkin açıklamalar sunan Post-fordist kuramların, kapitalizmdeki güncel gelişmeleri

açıklamak için yeterli olmamasıdır. Post-fordist kuramlar, üçüncü endüstri devrimi ile başlayan mikro elektronik alanındaki icatlara dair bir açıklama sunmaktadırlar. Gerçekleştirdikleri bu açıklamalar ile kuramlar, klasik montaj bandı ile üretim biçimi, enformasyon devrimi ve düşük maliyetli üretim yöntemlerinin birleşmesi ile talebin istikrarsız ve uçucu doğasına uyum sağlayabilmişlerdir. Ancak bu kuramlar, Vercellone'ye göre, kapitalizmin yeni biçimine dair bazı faktörleri tespit etmekte başarılı olsalar da bunları fordist-endüstriyel mantığın bir sonraki gelişimi olarak görmektedirler. Bu sebeple, enformasyonun yönlendirici işlevi üzerinde temellenen bir ekonominin gelişimi ile ilişkili olarak, sermaye ve emek arasındaki antagonistik ilişkilerdeki (üretim araçlarına sahip olanlar ile olmayanlar arasında uzlaşmanın imkansızlığını ve bu iki karşıt grup arasındaki ilişkinin ancak sınıf mücadelesi olabileceğini ifade eden ilişki) değişime dair kapsamlı bir anlayış sunmakta yetersizdirler. Bilişsel kapitalizm teorisi de bu anlayışı ortaya koymayı hedeflemektedir (Vercellone, 2007, s.14).

Dyer-Witheyford (2005, s.73) bilişsel kapitalizmde, bireylerin sabit sermaye niteliğindeki teknolojilerin geliştirilmesindeki ve işletilmesindeki konumlarına dikkat çekmiştir. Bireylerin, yüksek teknoloji ekonomilerin işletilmesini sağlayan teknik, kültürel, dilsel ve etik uzmanlıklarını (know-how) kullanarak, yüksek teknoloji meta üretimini gerçekleştirdiklerini ileri sürmüştür. Bilişsel kapitalizmin büyük veri ile ilgili görüşleri ise “ortak aklın” sömürülerek bir değere (ağ değeri) dönüştürülmesi amacıyla, yaşayan emeğin ve yaşanan zamanın ele geçirilmesi ve gözetim ya da denetimin bir aracı olarak kullanılması ekseninde şekillenmektedir. Ortak akıl (kolektif zekâ), ücretsiz kullanıma açık verileri ifade etmektedir. Google gibi kullanıcı verilerini kullanarak internet hizmeti sağlayan şirketler ise, kullanıcılara bir yandan ücretsiz hizmet sağlarken, diğer taraftan da internet reklamcılığı aracılığı ile sermaye değeri taşıyan kullanıcı verilerinin birikimini yapmaktadırlar (Pasquinelli, 2009, s.9).

Harvey'in düşünceleri ise, dördüncü bir eğilimi ortaya koymaktadır. Harvey, post-fordist teorideki “zaman-mekân sıkışması” kavramını, postmodern kültür ile ilişkilendirmiştir. Harvey'e göre, kapitalizm; coğrafi sınırlarını genişleterek ve metaların dolaşımında kalma süresini artırarak aşırı üretim riskinden kaçabilmiştir. Böylece yaşam temposunda ciddi bir artış ortaya çıkmış ve mekân anlayışı genişlemiştir. Harvey, postmodernizmin, kapitalizmin çalışma dinamiklerinde gördüğü köklü değişimlere karşı şüphe ile yaklaşırken, toplumsal öznelğin inşasında, algıda ve kültürde yakaladığı değişimleri de önemsemektedir (Harvey, 1989, s.112). Harvey, geçmiş ile bugün arasında nasıl bir fark olduğuna dair masalsi bir anlatı içeren, “dünün sanayileşme ve modernizminin yerini bugün post sanayileşme ve post modernizm aldı” biçimindeki teleolojik önermeleri, toplumsal değişimin esas unsurları ile yüzleşme açısından zararlı bulmaktadır. Bu açıdan, Marx'ın teorisinde yer alan ve bugünü anlamak için gerekli olan unsurları, sadece bu değişim trendlerini takip etme hedefiyle terk etmeyi “*araştırmacı burnumuzu koparmak*” olarak görmektedir (Harvey, 2008, ss.27-28). Onun düşüncesinde, kapitalizmin dönüşen unsurları dahilinde dijital teknolojiler, zaman-mekân

sıkışmasının araçlarıdır. Dijital teknolojilerin açık erişimli ürün ve hizmetler ortaya koyacağı, işbirlikçi üretim ve eşitlikçi bir düzeni getireceği tasarısı, sermayenin ücretsiz bir şekilde beslendiği bir hiper-sömürü biçimini almıştır. Kendi becerilerini kendi geliştiren işgücünün, ürettiği ücretsiz mallar, büyük sermaye sahibi şirketler tarafından kontrolsüzce yağmalanmaktadır (Harvey, 2017, s.96).

Tarihsel Materyalist Yaklaşım

Düşüncelerini tarihsel materyalist kuramda temellendiren Fuchs, dijital teknolojilerin yaygınlaşmasını takiben dijital sermaye ve kamusal dijital kaynaklar arasında, Marksist anlamda bir çelişkinin var olduğundan söz etmektedir. Fuchs'un düşüncesindeki temel soru, sermayenin kaynağı ve birikimi için itici güç konumunda olan emeğin, çağdaş dünyada, üreten tüketicilerle gerçekleştirilen, katılıma açık, kolektif üretimin koşulları içerisinde, hangi yeni biçimleri aldığı ve nasıl organize olduğudur. Fuchs, ücretsiz sosyal medya platformları, yaşamın kendisinin metalaştırılması, oyun ve emeğin bir bileşiğinin doğuşu gibi güncel olguları çağdaş kapitalizmin dijital boyutları ile ele almaktadır (Fuchs ve Fisher, 2015, ss.3-4).

Fuchs (2015), insan ihtiyaçlarının sadece yemek, barınma ve giyinmeden ibaret olmadığına, eğitim, öğrenme ve iletişim yoluyla toplumsal yeniden üretimin de bir ihtiyaç olduğuna dikkat çekmiştir. Bu anlamda gıda, barınma, giyim gibi ihtiyaçlar fiziksel kullanım değerlerini ifade ederken; sosyal ilişkiler, iletişim ve mutluluk, fiziksel olmayan kullanım değerlerini ifade etmektedir. Bu ayrım enformasyon ve iletişim teknolojileri aracılığıyla üretilen değeri konumlandırmaya yardımcı olmaktadır. Çevrimiçi platformlarda kullanıcılar tarafından üretilen ve yine kullanıcılar tarafından tüketilen içerikler, kullanıcıların sosyal ve psikolojik ihtiyaçlarını karşılamaları bakımından "fiziksel olmayan kullanım değeri" taşımaktadırlar. Ancak kullanıcıların içerik üretimi ve tüketimi esnasında arkalarında bıraktıkları veriler, çevrimiçi platformların sahibi olan ulusötesi şirketler için bir "değişim değeri" de üretmektedirler. Bu noktada ilk problem, kullanıcı verilerinin ürettiği değişim değerine, bu şirketler tarafından ücret ödenmeden ve üreticinin rızası alınmadan el koyulmasıdır. İkinci problem ise, kullanıcılardan toplanan verilerin içeriğinin, kullanıcılar hakkında çok detaylı kişisel ve mahrem bilgiler içermesidir. Dijital emeğin ve dijital sömürünün, gözetim ve denetimi de içeren yöntemlerinin ortaya koyulması, kullanıcıların veri sahiplikleri konusunda bilinçlerinin artırılması açısından önemlidir. Fuchs, büyük verinin gelişiminin daha ziyade dualist, belirlenimci ve doğrusal mantığı daha da derinleştirecek bir dijital çözümcülük anlayışını yaydığı görüşündedir. Bu anlayış, sömürünün ve baskının yeni niteliklerinin gelişimini beraberinde getiren, araçsal nedenlerin daha da yoğunlaşmasına sebep olmuştur (Fuchs ve Chandler, 2019, ss.48-49).

Fuchs'un teorisinde, bireyler, medyanın ideolojik manipülasyonu karşısında pasif kalma ve direnme kabiliyetine sahiptirler. Bilgisayarların ve bilgisayar ağlarının, enformasyonu, iletişimi ve dayanışmayı örgütlemek için sunduğu yeni kapasiteler de mevcuttur. Bilgisayarların çağdaş toplumun merkezi kaynağı haline gelmesi ile bu yeni kapasiteler, insan ihtiyaçlarını karşılamının da bir parçası

olmuşlardır. İnsanların, sevmek ve hatırlanmak gibi bilişsel ihtiyaçları, arkadaşlıklar ve topluluklar kurmak gibi iletişimsel ihtiyaçları ve belirli hedeflere ulaşmak için diğer insanlarla birlikte çalışmak gibi, iş birliğine ilişkin ihtiyaçları bulunmaktadır. Dijital teknolojilerin bu yeni kapasiteleri, insanların söz konusu ihtiyaçlarına karşılık verebilecek daha iyi bir yaşam sağlamak için kullanılmadığında ise, bugün olduğu gibi insanların yaşamlarına zarar vermeye devam edecektir (Fuchs, 2020, s.11) .

Fuchs ve Chandler'a göre (2019, s.58), istihbarat hizmetleri ve polis, veriyi ve toplumu güvenli hale getirmek için büyük veri akışına erişim elde etmeyi hedeflemektedirler. Böylece, gözetimi kar elde etme amacı ile kullanan özel güvenlik servislerine de kaynak sağlayabileceklerdir. NSA Ulusal Güvenlik Ajansı'nin iki binden fazla özel güvenlik şirketi ile sözleşmesi bulunmaktadır. Batılı kapitalist iletişim şirketleri, ürettikleri gözetim teknolojilerini, aktivistleri izleyen ve sonra onları tehdit eden, işkence eden ve baskılayan rejimlere satmaktadırlar (Fuchs, 2015, s.8). Bu durum da gözetim-endüstri bileşiminde, sermaye gözetimi ve devlet gözetiminin kaynaşmış olduğunu göstermektedir. Büyük Veri kapitalizmi ve algoritmik güç, dünyayı, ticari mantığın da toplumu kolonize ettiği, insanların neredeyse her yerde reklamların hedefi olduğu dev bir alışveriş merkezine dönüştürme kapasitesine sahiptir. Büyük veri çağında algoritmaların araçsal mantığı, insan ihtiyaçlarını hesaplamak ve bu ihtiyaçları karşılamak için karar vermek üzere kullanılmaktadırlar. Problem bu algoritmaların ve makinaların etik ve ahlak anlayışlarının olmamasıdır. Gözetim, bu algoritmalar ile merkezsizleşmiştir ancak tüm toplanan veriler birbirleri ile de bağlantılıdır. Bu anlamda Fuchs ve Chandler'in iddiası büyük veri çağında gözetimin panoptik olduğu, devlet ve sermayenin ikili merkezi panoptik kontrolü sağladığıdır (2019, s.59).

Panoptik gözetim teorilerinin başlangıç noktası, İngiliz filozof Jeremy Bentham'ın 18. yüzyılın sonlarında, bir hapishane olarak tasarlamış olduğu "Panoptikon" isimli mimari çizimin, Foucault (2005) tarafından modern gözetim pratiklerini açıklayıcı bir metafor olarak kullanılmasıdır. Literatürde gözetimi bütünüyle negatif bir konsept gibi değerlendirmek yerine, daha az eleştirel yaklaşan, pozitif çıktılarını değerlendirmeye alan panoptik olmayan eğilimler de mevcuttur. Ancak Fuchs, bebekleri uykusunda izleyen ya da depresyon tespit eden sistemler gibi gözetlemenin yapıcı kullanımları olmasına rağmen, gözetim teknolojilerinin bu tip kullanımlarına dikkat çekmenin, politik açıdan tehlikeli olacağını düşünmektedir. Bunun yerine baskıyı, sömürüyü, sınıfı, kapitalizmi, patriyarkayı, ırkçılığı ve benzer negatif fenomenleri ortaya çıkaran bir denetim biçimi olarak değerlendiren, bütünüyle negatif bir gözetim kavramına ihtiyaç olduğunu savunmaktadır (Fuchs, 2015, s.7). Çünkü büyük verinin kategorik şüphelere dayalı gözetim mantığı, bir kişinin suçu kanıtlanana kadar suçsuz kabul edildiği masumiyet karinesini yıkmakta ve bunun yerine "masum olduğun kanıtlanana kadar bir suçlusun" gibi bir mantıkla işleyen suçluluk karinesi prensibine dayanmaktadır (Fuchs ve Chandler 2019, s.59).

Bireyin gerçek benliğine verilen zarar Fuchs'un düşüncesinde veri tabanlarının değil, bütün toplumsal sistemin çıktısıdır. Bireylerin, kendilerine dayatılan ve kaçamadıkları belirli bir faaliyet alanında kısıtlanmak zorunda olmadıkları, istedikleri aktiviteye yönelebilecekleri fırsatları ve zamanları olduğu bir düzenin şart olduğunu düşünmektedir. Bu sayede, günümüz koşullarının insana dayattığı iş bölümünün ve yaşama tarzının etkisiyle kalıplaşan tek boyutlu karakteri aşabileceklerdir. Fuchs, çok yönlü bir benliğin inşası için gerçek özgürlüğün kazanılmasını zorunluluk olarak görmektedir. Onun bu düşüncesi, Marx'ın yabancılaşma kavramı ile temellendirilmektedir. Fuchs'a göre, insanlar kapitalizmde gerçek bir topluluğun değil sadece kendilerinin dışında da var olan aldatıcı bir topluluğun parçası olabilmektedirler. Oysa insanlar, ancak gerçek bir topluluk içinde ve birlik olarak özgürleşebilirler. Bu da insanın kendi benliğine geri dönmesi, kendi türüyle yeniden bütünleşerek, kendine ve türüne yabancılaşmayı aşması ve böylece, toplumsal bir varlık olan insanın, özüne bütünüyle dönmesi ile mümkün olacaktır (Fuchs, 2003, ss.57-58).

ARAŞTIRMA YÖNTEMİ

Araştırmanın Amacı

Araştırmanın amacı, büyük veri teknolojilerinin gelişimi ile verilerin asıl sahibi olan kullanıcıların veri gizliliklerini sağlama ve koruma konusunda karşılaştıkları problemleri ortaya koymaktır. Bu problemlerin ortaya çıkma aşamasında enformasyonun değişen ticari değeri, bu araştırma kapsamında temel etken olarak ele alınmıştır. Günümüzde enformasyonun giderek artan piyasa değeri karşısında, geçmiş dönemde mal ve hizmetler için rekabet eden şirket ve devletler, enformasyon kaynakları için rekabet etmeye başlamışlardır. Enformasyonun değeri, ondan ne kadar kullanışlı bilgi elde edilebildiği ile belirlenmektedir. Büyük veri çağında kullanışlı bilginin üretimi, dijital ortamda üretilen verilerin, veri analiz teknolojileri kullanılarak işlenmesiyle gerçekleşmektedir. Veri analiz teknolojileri, ön görücü algoritmalar kullanarak anlamlı tahminlerde bulunabilmekte ve böylece isabetli ticari ve politik kararlar alınmasına hizmet etmektedir.

Araştırmanın Önemi

Bu çalışma, enformasyonun değerinin birinci sanayi devriminden, dördüncü sanayi devrimi hedefleri arasında geçen sürede nasıl değiştiğini ortaya koymak amacıyla taşımakta ve büyük veri teknolojilerinin gelişim sürecini, kapitalizmin dinamikleri içerisinde konumlandırmaktadır. Bu anlamda Fuchs'un tarihsel materyalizm yaklaşımı ile değerlendirdiği Büyük Veri Kapitalizmi analizleri, araştırmanın kuramsal çerçevesini oluşturmaktadır. Araştırmanın uygulama kısmında ise, internet kullanıcılarının farklı uzmanlık derecelerine sahip oluşlarıyla ilişkili olarak, veri paylaşımlarına ilişkin farkındalıkları, internet kullanım alışkanlıkları ile mahremiyet ve gizlilik anlayışları, verilerini kullanma konusundaki temkinleri ve davranışsal ve kişisel verilerine yaklaşımları analiz edilmiştir. Bu bağlamda çalışmanın önemi, büyük veri teknolojilerinin yüksek karlılık ve verimlilik gibi hedeflerle yarattığı pozitif algının eleştirisini yapması ve bu

teknolojilerin eşitsizlik problemlerine çözüm üretmek yerine, onları güçlendirecek dinamikler içerdiğine dikkat çekmesidir.

Bu araştırma, örneklemin araştırma evrenini temsil etme kapasitesi bağlamında sınırlılıklara sahiptir. Ancak çalışmanın, büyük veri teknolojilerinin gelişimine ve kullanıcı gizliliğine ilişkin sosyolojik bir analiz sunması ve veri teknolojilerine ilişkin kavramları sosyolojik bağlamı içerisinde konumlandırması bakımından alan yazınına önemli bir katkı sağlayacağı düşünülmektedir. Literatürdeki internet kullanıcılarının gizlilik endişeleri üzerine yapılan araştırmaların, örneklemini “tüketiciler” olarak değerlendirilme eğiliminin aksine (Bellman vd., 2004; Graeff ve Harmon, 2002; Sheehan, 2002), (Joseph Phelps vd., 2000), bu çalışmada internet kullanıcıları, verilerinin sahibi ve içerik üreticisi olarak konumlandırılmıştır. Bu bağlamda araştırma, internet kullanıcılarının gizlilik ve mahremiyetlerini, çevrim içi platformlarda koruma konusundaki bilinçlerini artıracak ve onları tüketiciler yerine, aktif üretici olarak yeniden konumlandıracak uygulamaların önemini ve aciliyetini de vurgulaması açısından önem arz etmektedir.

Veri Toplama Tekniği

Araştırma, büyük veri teknolojilerinin mevcut veri toplama, saklama ve analiz tekniklerinde meydana getirdiği gelişmelerin kullanıcılar tarafından ne düzeyde fark edildiğinin, kullanıcıların kişisel, davranışsal ve hassas veri gizliliğine ilişkin bilinç düzeylerinin ve endişe düzeylerinin belirlenmesini hedefleyen nicel bir çalışmadır. Neuman’a göre (2006, s. 21), anlam inşa etmek yerine nesnel olguları ölçen, etkileşim içindeki süreçler yerine değişkenlere odaklanan, değerlerden bağımsız olan ve araştırmacının tarafsız bir konumda olduğu araştırmalar nicel araştırmalardır. Veri teknolojilerinin veri gizliliklerini ve mahremiyetlerini tehdit eden unsurlar karşısında, bireylerin farkındalık, bilinç ve endişe düzeylerini odağa yerleştirmek ve gelecek araştırmalar için genel bir tablo çizebilmeyi odağına alması sebebiyle, bu çalışmanın nicel araştırma yöntemi ile yapılmasına karar verilmiştir. Çalışma için, 20.03.2019 tarih ve 12908312-300/000000515333 sayılı Hacettepe Üniversitesi Etik Kurul onayı alınmıştır.

Araştırmada verilerin toplanması için anket tekniği kullanılmıştır. Katılımcıların demografik özellikleri, katılımcıların kişisel ve davranışsal verilerine yaklaşımları, mahremiyet ve gizlilik anlayışları, kullanımdaki endişe düzeylerine ilişkin sorular sorulmuş ve internet üzerinden edindikleri bilginin güvenilirliğine karar verişlerine dair belirlenen ifadeleri seçmeleri istenmiş, bu bağlamda da verilen cevaplar doğrultusunda, katılımcıların dijital okur-yazarlık becerilerinin değerlendirilmesi amaçlanmıştır.

Araştırma Evren ve Örneklemi

Araştırmanın genel evreni, haftada en az bir kez internet kullanan her kullanıcıyı kapsamaktadır. Böylesine geniş bir evren üzerinden gerçekleştirilecek olan çalışma evreni ise, uygulayıcının yaşadığı şehir ve veriye ulaşma kolaylığı açısından, Ankara’da yaşayan, nispeten interneti buldukları konum itibarıyla daha

çok ve efektif kullanan, internet kullanıcısı genç üniversite öğrencileri ve Bilgisayar ve İletişim Teknolojileri firmaları çalışanları ile sınırlandırılmıştır. Buna göre, araştırma evreni popülasyonu, Hacettepe Üniversitesi Sosyoloji, Felsefe, Bilgisayar Mühendisliği bölümlerinin lisans örgün eğitiminde kayıtlı toplam öğrenci sayısı ve Hacettepe Teknokent bilişim ve yazılım firması çalışanlarının toplam sayısı 2563'tür.

Belirlenen bu evren içinde, örnekleme deseni doğrudan örneklemeye fırsat verdiği için (bireylerin tek tek isimlerinin bilgisine ulaşılabilirdiği için) tek aşamalı örnekleme yöntemi kullanılmıştır. Bu aşamada, çalışmada evren içindeki toplam sayılara (isim listelerine) ulaşılmış ve Hacettepe Üniversitesi Sosyoloji, Felsefe ve Bilgisayar Mühendisliği bölümlerinde lisans düzeyinde örgün eğitim görmekte olan toplam 1556 kişiden 90% güven aralığı ve 2.87% hata payı ile 189 öğrenci, Hacettepe Teknokent'te yer alan bilişim ve yazılım firmalarında çalışan toplam 997 kişiden 90% güven aralığı ve 3.81% hata payı ile 109 çalışan kişi, rastgele örnekleme yöntemi kullanılarak seçilmiştir. Örnekleme, bilişim teknolojileriyle ilgili farklı uzmanlık düzeylerine göre 3 gruba ayrılmıştır. Örnekleme kategorilendirmek için kullanılan bu karakteristikler ise şu şekildedir; bilişim teknolojisi açısından bireylerin temel özelliklerine göre, ilk grup bilişim teknolojileri alanında hiçbir uzmanlığı olmayan gençleri, ikinci grup bilişim teknolojileri alanında orta düzey uzmanlığı olan gençleri, üçüncü grup ise, bu alanda uzmanlığı olan kullanıcıları içermektedir.

Tablo 1: Örneklemin Teknolojik Uzmanlık Düzeylerinin Dağılımı

Uzmanlık Düzeyi	Frekans	Geçerli Yüzde
Düşük Uzmanlık Düzeyi	116	38,9
Orta Düzeyde Uzmanlık	73	24,5
Yüksek Düzeyde Uzmanlık	109	36,6
Toplam	298	100
Cevapsız	9	
Toplam	307	

İlk grup için, bilişim teknolojileri ile ilişkili konularda uzmanlığı olmayan grubu temsil edecek şekilde, araştırmaya hız ve pratiklik kazandırma amacı da güdülenerek, çalışmacının da eğitim gördüğü üniversite olan Hacettepe Üniversitesi Sosyoloji ve Felsefe bölümündeki toplam 808 genç arasından 116 kişiye ulaşılmıştır. İkinci grubu oluşturan orta düzey uzmanlığa sahip Hacettepe Üniversitesi Bilgisayar Mühendisliği bölümünde okuyan 758 genç arasından, 73 kişiye ve üçüncü grubu, yani uzmanlardan oluşan grubu temsil edecek katılımcılar için de Hacettepe Teknokent'in bünyesinde bulunan, toplam 43 adet Bilgisayar ve İletişim Teknolojileri ve Yazılım firmasındaki 997 çalışan arasından, 109 kişiye ulaşılmıştır. Böylece toplam 307 kişiye anket uygulaması yapılmış ancak uzmanlık düzeyine

ilişkin anket sorusunun cevapsız bırakılması sonucu, 9 kişilik örneklem kaybı yaşanmıştır. Bu sebeple toplam 298 kişi ile çalışma gerçekleştirilmiştir.

Araştırmanın Hipotezleri

H1: Bireylerin davranışsal verilerine ve kişisel verilerine yaklaşımları arasında anlamlı bir farklılaşma vardır.

H2: İnternet kullanım alışkanlıkları ile mahremiyet ve gizlilik anlayışları arasında anlamlı bir ilişki vardır.

H3: Güvenilir bilgiye ulaşma aracı olarak interneti kullanan bireyler, kişisel verilerini koruma konusunda daha temkinlidir.

Şekil 1: Veri Türlerine İlişkin Ayrım



Araştırma kapsamına dahil edilecek olan veri türleri, Şekil 1'deki gibi kategorilendirilmiştir. Kişisel veriler, davranışsal veriler ve hassas verilere ilişkin Kişisel Verileri Koruma Kanunu ve Avrupa Birliği Veri Koruma Tüzüğü'nde yer alan tanımlamalardan (Kişisel Verilerin Korunması Kanunu, 2016 ve Handbook on European Data Protection Law, 2018) yola çıkılarak çalışmanın özgün bakışı çerçevesinde araştırmacılar tarafından oluşturulmuştur.

Şekil 1'deki gruplandırmanın ilki, demografik veriler, internet alışverişleri ve indirme geçmişleri, IP adresleri, konum bilgileri ve güvenlik parolaları gibi kişisel verileri içermektedir. Katılımcıların, kişisel veri olarak sahipliğini üstlendikleri ve gizliliğini çevrim dışı dünyada da önemsedikleri veri türleri olarak kategorilendirilmiştir. Bir başka deyişle, kişisel veri türleri, büyük veri analizi

teknolojileri var olmadan önce de işlenen ve kullanılan verilerdir (örneğin, internetin yaygınlaşmasından önce de kullanılan mağazaların müşterilerine verdikleri sadakat kartları, müşterilerin mağaza alışverişlerine ilişkin konum, zaman, ürün bilgisi gibi kişisel verilerini içermekteydi.) Bu çalışma kapsamında, kullanıcıların isim, konum, yaş, cinsiyet, gelir bilgileri ile birlikte, ilgi alanları, çevrimiçi alışveriş ve indirme geçmişleri ve kullanıcıların tarayıcılarına kaydetmiş oldukları diğer otomatik form doldurma verileri, kişisel veri kapsamında değerlendirilmektedir.

İkinci grupta yer alan davranışsal veriler, katılımcıların sosyal medya gönderileri, internet kullanım alışkanlıkları, kullanıcı profilleri, tıklanan reklamlar ve gönderiler, çevrimiçi platformlarda etkileşime girdikleri bireyler gibi çeşitli verileri içermektedir. Bu veri tipi, büyük veri analitiğinin gelişimi ile ortaya çıkmıştır ve gizlilik endişesi yaratan bir diğer bilgi türünü oluşturmaktadır. Davranışsal verilerin işlenmesi ile internet kullanıcılarının karakterlerine ve gelecek davranışlarına ilişkin isabetli tahminler yapılabilmekte ve böylece kullanıcılar belirli bir eylemi gerçekleştirmeye yönlendirilebilmektedir. Örneğin, bir internet mağazasından alışveriş yapan kullanıcıların, davranışsal verileri analiz edildiğinde, o kullanıcıların websitesinin neresinde konumlanmış bir reklama tıklama olasılığının daha yüksek olduğu saptanabilmektedir. Böylece kullanıcıların davranışlarına ilişkin veriler kullanılarak, o reklamın hedefine ulaşma oranı artırılmaktadır. Bu çalışma özelinde davranışsal veri kapsamında değerlendirilecek olan verileri, kullanıcıların internet tarayıcısında ve kullandıkları cihazlarda saklanan izleme verileridir. Kullanıcının hangi gönderide ne kadar vakit geçirdiği, hangi reklamlara tıkladığı, hangi gönderileri beğendiği, çevrimiçi etkileşim kurulan diğer kullanıcılar, uygulamaya giriş ve çıkış yapılan saatler bu araştırma kapsamında davranışsal veriler olarak değerlendirilecektir.

Son grupta yer alan hassas veriler, tıbbi veriler, biyo-metrik veriler, siyasi görüş, etnik köken ve cinsel kimliklere ilişkin kullanıcı verilerini ifade etmektedir. Bu grupta yer alan veriler, çalışmaya katılanların çevrim dışı dünyada da mahremiyet alanı içerisinde değerlendirdikleri ve gizliliğinden en çok endişe duyacakları veri türlerini içermektedir. Hassas veriler, yapay zekâ teknolojisinin geliştirilmesi gibi doğrudan belirli amaçlar için kullanılabilirliği gibi, diğer veri türlerinden gelen bilgiler ile eşleşerek, kullanıcı davranışlarının ve tutumlarının manipüle edilmesi için de kullanılabilirliği vardır. Örneğin, göçmen karşıtı politikaların propagandasını yapan içerikler, konuya karşı çekimser ve kararsız olduğu daha önce tespit edilen kullanıcıların profillerinde gösterilebilmektedir. Böylece hedeflenen kullanıcı profilinde istenen fikir değişikliği daha kolay sağlanmış olmaktadır. Bu çalışma kapsamında hassas nitelikli veriler, kullanıcıların siyasi görüşleri, etnik kökenleri, cinsel yönelimleri, dini inançları, tıbbi verileri, biyo-metrik ve genetik özelliklerini içeren sensör verileri gibi kullanıcıların toplanması, saklanması ve üçüncü taraflarla paylaşılması konusunda özel hassasiyet gösterecekleri mahrem bilgilerine atıfta bulunmaktadır.

Bu bağlamda araştırma soruları, söz konusu verilere ilişkin endişe düzeyleri arasındaki ayrımı ortaya koymak ve hipotezleri ölçebilmek için oluşturulmuştur. Her

hipotez bu gruptandırılmış veriler bağlamında aşağıda açıklanmıştır. İlk hipotezde, katılımcıların kişisel verilerine ve davranışsal verilerine yaklaşımları, her birine ilişkin gizliliklerine verdikleri önem çerçevesinde incelenmiştir. Şekil 1'de görüldüğü üzere "kişisel veriler" ve "hassas veriler" kategorisinde değerlendirilen veriler, örneklemin çevrim dışı dünyada da gizliliğine önem verdikleri bilgileri kapsamaktadır. Davranışsal veriler ise büyük veri analitiğinin gelişimi ile gizlilik endişesi yaratan bilgileri içermektedir. Bu durum dikkate alınarak oluşturulan H1 hipotezinde, örneklemin kişisel veri gizliliğine verdikleri önem ile davranışsal veri gizliliğine verdikleri önem arasında anlamlı bir farklılık aranmaktadır.

İkinci hipotezde, katılımcıların mahremiyet ve gizlilik anlayışları bağımsız değişkeni, her bir veri tipi için endişe düzeyleri ile ölçülmüştür. Katılımcılardan her bir veri tipi için endişe düzeylerini, 5'li likert ölçeğiyle (Endişe duymuyorum- Biraz endişe duyuyorum- Kararsızım- Oldukça endişeliyim- Çok endişeliyim) puanlamaları istenmiştir. Analiz için aynı veri tipine ait olan değişkenler gruplanmış (kişisel veri-davranışsal veri- hassas veri) ve her grubun kendi içinde ortalaması alınarak analize dahil edilmişlerdir. İnternet kullanım alışkanlıklarının ölçülebilmesi için, katılımcıların günlük internet kullanma sıklıkları, dijital becerilerini ifade eden uzmanlık düzeyleri ve teknolojik ürünleri kullanım kolaylığı bağımlı değişken olarak ele alınmıştır. İnternet kullanma sıklığında, 1. Grup günde 1-3 saat arası süreyle internet kullananlar, 2. Grup günde 3-6 saat internet kullananlar, 3. Grup günde 6-9 saat internet kullananlar, 4. Grup günde 9 saatten fazla süreyle internet kullananlara karşılık gelmektedir.

Üçüncü hipotezin test edilebilmesi için, anket formunda örneklemin internet aracılığıyla edindikleri bilginin güvenilirliğine nasıl karar verdiklerine ilişkin ifadeler yer verilmiş, verilen cevaplar doğrultusunda katılımcıların dijital okuryazarlık becerileri için 4 seviye belirlenmiştir. Temkinlilik düzeyini ölçmek için anket formunda, birden fazla işaretlenebilen 11 ifadeye yer verilmiştir. 11 ifade, 1- düşük temkinlilik düzeyi ve 4- yüksek temkinlilik düzeyi olarak artan seviyede gruplandırılmıştır. Örneklemin cevabını yönlendirmekten kaçınma amacıyla gruplandırılan ifadeler, ilgili sorularda, sırası karışık olarak verilmiştir.

Veri analizi aşamasında ise katılımcıların demografik bilgilerine, kullandıkları teknolojik ürün ve servislere, internet kullanım süre ve amaçlarına, uzmanlık düzeylerine ilişkin betimsel analiz verileri yorumlanmıştır. Araştırma kapsamında, katılımcılarının yaş, cinsiyet, eğitim düzeyi gibi bilgileri analiz amacıyla değil, örneklemin eşit dağıldığını kontrol etme amacıyla sorulmuştur. Bu sebeple bu değişkenlere göre bir analiz yapılmamıştır. Oluşturulan hipotezlerin testi, Pearson Korelasyonu, Anova ve Kruskal-Wallis analizinden faydalanılarak yapılmıştır.

H1 hipotezindeki değişkenler arasındaki ilişkinin tespiti için Pearson Korelasyonu analizi yapılmıştır. Örneklemin kişisel veri gizliliğine verilen önem ve davranışsal veri gizliliğine verilen önem bağımlı değişkenlerin üzerinde uzmanlık

düzeıı bağımsız deęişkeninin etki düzeyini tespit edebilmek ve böylece uzmanlık düzeyine göre olası bir farklılaşmayı tespit edebilmek için Anova hipotez testi yapılmıştır. Farklılaşmanın hangi gruplar arasında olduğunu tespitinde, varyansları homojen dağılan gruplar için uygun olan Post Hoc Scheffe testi kullanılmıştır.

H2 hipotezinin test edilmesi için, her bir veri türüne ilişkin (kişisel veri/ davranışsal veri/ hassas veri) endişe düzeyi deęişkeni ile katılımcıların günlük internet kullanma sıklıkları, teknoloji ürünlerini kullanım kolaylıkları ve farklı uzmanlık düzeyleri arasında olası bir farklılaşmayı tespit etme hedefi ile varyansları homojen dağılan gruplarda Anova analizi, varyansları homojen dağılmayan gruplarda Kruskal-Wallis analizi yapılmıştır. Hangi gruplar arasında farklılaşma olduğunu tespitinde ise Post-Hoc Tamhane's T2 testi kullanılmıştır.

H3 hipotezinin test edilmesi için, katılımcıların dijital okur-yazarlık becerilerini ölçen deęişken ile katılımcıların kişisel verilerini koruma konusundaki temkinlilik düzeyini ölçen deęişkenlerin ortalaması analize sokulmuştur. Gruplar homojenlik varsayımını sağlayamadığı için hipotez, Kruskal Wallis Analizi ile test edilmiştir.

BULGULAR

Demografik Verilerin Analizi

Araştırma örnekleminin (307) %52'sini erkekler, %47'sini kadınlar oluşturmaktadır. Örneklem ağırlıklı olarak üniversite öğrencileri arasından seçildiği için, en yoğun örneklem grubunu 18-25 (%55) yaş grubu arası gençlerden oluşturmaktadır. Bunu 26-35 (%29) yaş grubundakiler takip etmektedir. 36-45 yaş grubu örneklemin yalnızca %6'sını, 46-55 yaş grubundaki örneklem grubu ise %9'unu oluşturmaktadır. Araştırma örnekleminin, %55'i lisans mezunu, %35'i lise mezunu, %9'u lisansüstü eğitim mezunudur. Örneklemden yalnız 2 kişi, eğitim düzeyini lise öncesi olarak işaretlemiştir. Araştırma örnekleminin yaklaşık %43'ünün gelir seviyesi aylık 1000 TL kazancın altındadır. Örneklem %50'den fazlasının öğrenci statüsünde olması, düşük gelir düzeyi oranının fazla olmasını açıklamaktadır. Örneklem %24,8'inin gelir düzeyi 3000 TL üzerindedir. Dolayısıyla araştırma örnekleminin alt ve orta düzey geliri olan bireyleri temsil düzeyi daha yüksektir.

HİPOTEZ ANALİZLERİ

Birinci Hipotezin Analizi

H0: Katılımcıların kişisel verilerine yaklaşımları ile davranışsal verilerine yaklaşımları arasında anlamlı bir farklılık yoktur.

H1: Katılımcıların kişisel verilerine yaklaşımları ile davranışsal verilerine yaklaşımları arasında anlamlı farklılık vardır.

Çalışmaya katılanların kişisel verilerine ve davranışsal verilerine yaklaşımları, her birine ilişkin gizliliklerine verdikleri önem çerçevesinde

incelenmiştir. Değişkenlerin analiz için normallik ön koşulunu sağlayıp sağlamadığı, Normallik testi ile kontrol edilmiştir.

Tablo 2: Katılımcıların Kişisel Verilerine ve Davranışsal Verilerine Yaklaşımları, Her Birine İlişkin Gizliliklerine Verdikleri Önem Normallik Testi

Normallik Testi						
	Kolmogorov-Smirnov			Shapiro-Wilk		
	Statistik	Df	Sig.	Statistik	df	Sig.
Davranışsal Veri Gizliliğine Verilen Önem	,192	305	,000	,897	305	,000
Kişisel Veri Gizliliğine Verilen Önem	,229	305	,000	,904	305	,000

Normallik testi sonucu her iki değişken için de $p < 0,001$ bulunmuştur. Bu anlamda normal bir dağılım gözlenmektedir. Veriler Pearson Korelasyonu ile test edilmek için uygundur.

Kişisel Veri Gizliliğine Verilen Önem ile Davranışsal Veri Gizliliğine Verilen Önem arasında, “- 0,154” olarak elde edilen korelasyon değeri, p değerinin 0,05’ten küçük olması ($p=0,007$) bağlamında anlamlı bulunmuştur. Söz konusu değişkenler arası ilişki negatif yönlüdür. Kişisel veri gizliliğine verilen önem düzeyi arttıkça, davranışsal veri gizliliğine verilen önem düzeyi azalmaktadır.

Tablo 3: Katılımcıların Uzmanlık Düzeylerine Göre, Davranışsal Verilerine Yaklaşımları ve Kişisel Verilerine Yaklaşımları Arasındaki İlişki

ANOVA						
		Kareler Toplamı	df	Ortalama Kare	F	Sig. (p)
	Gruplar Arasında	8,862	2	4,431	1,668	,190

Davranışsal Veri Gizliliğine Verilen Önem	Gruplar İçinde	778,273	293	2,656		
	Toplam	787,135	295			
Kişisel Veri Gizliliğine Verilen Önem	Gruplar Arasında	25,198	2	12,599	6,442	,002
	Gruplar İçinde	575,044	294	1,956		
	Toplam	600,242	296			

Katılımcıların uzmanlık düzeylerine göre, davranışsal verilerine yaklaşımları ve kişisel verilerine yaklaşımları arasında anlamlı bir fark olup olmadığı test edilmek üzere, önce uygun analiz yöntemini seçmek için varyansların homojen dağılıp dağılmadığı test edilmiş, sonuç olarak varyansların homojen dağıldığı gözlenmiştir. Daha sonra, fark analizi için ANOVA hipotez testi uygulanmıştır. Davranışsal veri gizliliğine yaklaşımları bakımından gruplar arasında anlamlı bir fark saptanmamıştır.

Tablo 4: Kişisel Veri Gizliliğine Yaklaşımları Bakımından Gruplar Arasındaki Fark

Post Hoc- Scheffe Çoklu Karşılaştırma Testi						
Bağımlı Değişken: Kişisel Veri Gizliliğine Verilen Önem						
Scheffe Testi						
(I) Uzmanlık Seviyesi	(J) Uzmanlık Seviyesi	Ortalama Fark (I-J)	Std. Hata	Sig.	95% Güven Aralığı	
					Alt Sınır	Üst Sınır
Düşük Düzey	Orta Düzey	-,74563*	,20894	,002	-1,2597	-,2316
	Yüksek Düzey	-,35281	,18701	,171	-,8129	,1073
Orta Düzey	Düşük Düzey	,74563*	,20894	,002	,2316	1,2597

	Yüksek Düzey	,39282	,21191	,181	-,1285	,9142
Yüksek Düzey	Düşük Düzey	,35281	,18701	,171	-,1073	,8129
	Orta Düzey	-,39282	,21191	,181	-,9142	,1285
*. Ortalama fark, 0,05 düzeyinde anlamlıdır.						

Kişisel veri gizliliğine yaklaşımları bakımından gruplar arasında anlamlı bir fark gözlenmiştir ($p=0,002$). Farklılaşmanın hangi gruplar arasında olduğunun tespiti için, varyansları homojen dağılan gruplar için uygun olan Post Hoc Scheffe testi kullanılmıştır. Kişisel veri gizliliğine yaklaşımları bakımından, düşük düzey uzmanlığa sahip sıradan internet kullanıcıları olan gençler ile orta düzey uzmanlığa sahip bilgisayar mühendisliği bölümünde öğrenci olarak bulunan gençler arasında anlamlı bir fark saptanmıştır ($p=0,002$).

İkinci Hipotezin Analizi

Araştırmanın ikinci hipotezi aşağıdaki gibidir. Değişkenlere ilişkin gerekli açıklamalar “Araştırmanın Hipotezleri” başlığında verilmiştir.

H0: Katılımcıların internet kullanım alışkanlıkları ile mahremiyet ve gizlilik anlayışları arasında anlamlı bir ilişki yoktur.

H2: Katılımcıların internet kullanım alışkanlıkları ile mahremiyet ve gizlilik anlayışları arasında anlamlı bir ilişki vardır.

Örneklemin internet kullanım sıklığı, günlük internet kullanılan süreye göre gruplandırılmıştır. 1. Grup günde en az sıklıkla internet kullananları (1-3 saat), 4. Grup en yüksek sıklıkla internet kullananları (9 saatten fazla) temsil etmektedir. Örneklemin mahremiyet ve gizlilik anlayışlarını ise kişisel, davranışsal ve hassas verilerin toplanması ve saklanmasına ilişkin endişe düzeylerine göre gruplandırılmıştır (1- Endişe duymuyorum, 5- Çok endişeliyim). İlk aşamada katılımcıların internet kullanım sıklığı ile mahremiyet/gizlilik anlayışları arasındaki ilişkinin analizi için grupların varyanslarının homojenliği test edilmiştir.

Tablo 5: Katılımcıların İnternet Kullanım Sıklığı ile Mahremiyet/Gizlilik Anlayışları Arasındaki İlişki

Varyansların Homojen Dağılımı Testi					
		İstatistik	df1	df2	Sig. (P)
Hassas Veriler	Ortalama temelinde	,804	3	299	,492
	Medyan temelinde	,694	3	299	,556
	Ayarlanmış df medyan temeli ile birlikte	,694	3	278,714	,556
	İşlenmiş ortalama	,840	3	299	,473
Kişisel Veriler	Ortalama	1,829	3	299	,142
	Medyan	1,333	3	299	,264
	Ayarlanmış df medyan temeli ile birlikte	1,333	3	289,932	,264
	İşlenmiş ortalama	1,831	3	299	,141
Davranışsal Veriler	Ortalama	4,146	3	294	,007
	Medyan	4,072	3	294	,007
	Ayarlanmış df medyan temeli ile birlikte	4,072	3	272,890	,007
	İşlenmiş ortalama	4,253	3	294	,006

Varyansların homojen dağılımı testinin sonuçlarına göre, davranışsal verilere ilişkin endişe düzeyi dışındaki grupların homojen bir dağılıma sahip olmadığı görülmektedir. Bu nedenle, davranışsal verilere ilişkin endişe düzeyi değişkeni ile katılımcıların günlük internet kullanma sıklıkları arasında anlamlı bir farklılaşma olup olmadığını ölçmek için **ANOVA** testi, diğer değişkenler için **Kruskal-Wallis Testi** kullanılmıştır.

Tablo 6: Davranışsal Verilere İlişkin Endişe Düzeyi Değişkeni ile Katılımcıların Günlük İnternet Kullanma Sıklıkları Arasındaki İlişki Kruskal-Wallis Testi

Kruskal-Wallis Testi	
	Hassas Verilere İlişkin Endişe Düzeyi
Kruskal-Wallis H	13,024
Df	3
Asymp. Sig.	,005
a. Kruskal Wallis Testi	
b. Grup Değişkeni: Günlük İnternet Kullanım Sıklığı	

Kruskal-Wallis Testi sonucunda iki değişken arası ilişkide anlamlı bir farklılaşma olduğu tespit edilmiştir.

Tablo 7: Davranışsal Verilere İlişkin Endişe Düzeyi Değişkeni ile Katılımcıların Günlük İnternet Kullanma Sıklıkları Arasındaki Çoklu Karşılaştırma

Post Hoc- Tamhane Çoklu Karşılaştırma Testi						
Bağımlı Değ.: Hassas Verilere İlişkin Endişe Düzeyi						
Tamhane						
(I) Günlük İnternet Kullanım Sıklığı	(J) Günlük İnternet Kullanım Sıklığı	Ortalama Fark (I-J)	Std. Hata	Sig.	95% Güven Aralığı	
					Alt Sınır	Üst Sınır
1,00	2,00	-,00404	,22277	1,000	-,6055	,5974
	3,00	-,16259	,22453	,978	-,7686	,4434
	4,00	-,56225	,22500	,084	-1,1692	,0447

2,00	1,00	,00404	,222 77	1,0 00	-,5974	,6055
	3,00	-,15855	,169 48	,92 5	-,6099	,2928
	4,00	-,55821*	,170 11	,00 7	-1,0108	-,1057
3,00	1,00	,16259	,224 53	,97 8	-,4434	,7686
	2,00	,15855	,169 48	,92 5	-,2928	,6099
	4,00	-,39967	,172 41	,12 3	-,8587	,0594
4,00	1,00	,56225	,225 00	,08 4	-,0447	1,1692
	2,00	,55821*	,170 11	,00 7	,1057	1,0108
	3,00	,39967	,172 41	,12 3	-,0594	,8587
*. Ortalama fark, 0,05 düzeyinde anlamlıdır.						

Tespit edilen farklılaşmanın hangi gruplardan kaynaklandığını analiz etmek için, varyansların homojen dağılmadığı gruplarda kullanılan Post Hoc Tamhane testi, tamamlayıcı bir karşılaştırma yapabilmek üzere kullanılmıştır. Bu analizin sonucuna göre, hassas verilere ilişkin endişenin, günlük internet kullanım sıklığı en yüksek olan kullanıcıları (9 saatten fazla) ifade eden 4. Grubun üzerinde en fazla etkiye sahip olduğu tespit edilmiştir ($p < 0,05$).

Tablo 8: Davranışsal Verilere İlişkin Endişe Düzeyi ile Katılımcıların Günlük İnternet Kullanım Sıklığı Arasındaki İlişkideki Olası Farklılaşma

ANOVA
Davranışsal Verilere İlişkin Endişe Düzeyi

	Kareler Toplamı	Df	Ortalama Kare	F	Sig. (p)
Gruplar Arası	59,683	3	19,894	11,817	,000
Gruplar İçinde	496,659	295	1,684		
Toplam	556,342	298			

Davranışsal verilere ilişkin endişe düzeyi ile katılımcıların günlük internet kullanım sıklığı arasındaki ilişkideki olası farklılaşma ANOVA testi ile analiz edilmiştir. Sonuç olarak günlük internet kullanım sıklığı en yüksek olan kullanıcıları (9 saatten fazla) ifade eden 4. Grubun, davranışsal verilere ilişkin endişe düzeyi üzerinde en yüksek etkide bulunduğu bulunmuştur ($p < 0,001$).

Tablo 9: Davranışsal Verilere İlişkin Endişe Düzeyi ile Katılımcıların Günlük İnternet Kullanım Sıklığı Arasındaki İlişkideki Olası Farklılaşma Kruskal-Wallis Testi

Kruskal-Wallis Test Değerleri	
	Kişisel verilere ilişkin endişe düzeyi
Kruskal-Wallis H	6,070
df	3
Asymp. Sig.	,108
a. Kruskal Wallis Test	
b. Grup Değişkeni: günlük internet	

Kişisel verilere ilişkin endişe düzeyi ile katılımcıların günlük internet kullanım sıklığı arasındaki olası bir farklılaşmanın tespiti için Kruskal-Wallis testi uygulanmıştır. Testin sonucunda, gruplar arasında anlamlı bir farklılaşma olmadığı saptanmıştır.

Kişisel, Davranışsal ve Hassas Verilere ilişkin endişe düzeyinin, örneklemin uzmanlık düzeyine göre farklılaşma olasılığı değerlendirilmiştir. Uygun analiz

teknğine karar verebilmek için grupların varyans dağılımlarının homojenliği test edilmiştir. Analiz sonuçlarına göre, kişisel verilere ilişkin endişe düzeyi için varyans dağılımının homojenliği sağlanmış ancak diğer gruplar için sağlanamamıştır. Bu anlamda, örneklemin kişisel verilere ilişkin endişe düzeylerinde, uzmanlık düzeyi ile ilişkili olası bir farklılaşmanın tespit edilebilmesi için ANOVA testi uygulanmıştır.

Tablo 10: Kişisel, Davranışsal ve Hassas Verilere İlişkin Endişe Düzeyinin, Katılımcıların Uzmanlık Düzeyi Arasındaki İlişki

ANOVA					
Kisisel_Verilere İlişkin Endise_Duzeyi					
	Kareler Toplamı	df	Ortalama Kare	F	Sig.
Gruplar Arasında	16,584	2	8,292	5,633	,004
Grupların İçinde	431,266	293	1,472		
Toplam	447,850	295			

ANOVA analizi sonucunda gruplar arası anlamlı bir farklılık tespit edilmiştir ($p=,004$). Katılımcıların davranışsal ve hassas verilere ilişkin endişe düzeylerinde, uzmanlık düzeyi ile ilişkili olası bir farklılaşmanın tespit edilebilmesi için ise Kruskal Wallis Analizi uygulanmıştır.

Tablo 11: Kişisel, Davranışsal ve Hassas Verilere İlişkin Endişe Düzeyinin, Katılımcıların Uzmanlık Düzeyi Arasındaki İlişkiye Yönelik Kruskal-Wallis Testi

Kruskal-Wallis Test Değerleri	
Davranışsal Veri	Hassas Veri
15,941	11,889
2	2
,000	,003
a. Kruskal Wallis Test	

b. Grup Değişkeni: Uzmanlık Seviyesi

Kruskal Wallis Analizi sonucunda, gruplar arası anlamlı bir farklılaşma olduğu tespit edilmiştir ($p=,003$). Farklılaşmanın hangi gruplar arasında olduğunun tespitinde ise Post-Hoc testi yapılmıştır. Varyansların eşit olması dolayısıyla “kişisel verilere ilişkin endişe düzeyi” değişkeni ile analiz yapılırken Scheffe testi, diğer değişkenlerde ise varyansların eşit olmaması dolayısıyla Tamhane’s T2 testi kullanılmıştır. Katılımcıların kişisel verilerinin gizliliğine ilişkin endişe düzeyleri, sıradan internet kullanıcıları ve orta düzey uzmanlığa sahip internet kullanıcıları arasında anlamlı bir fark saptanmıştır ($p=,004$).

Davranışsal verilerinin gizliliğine ilişkin endişe düzeyleri ise sıradan internet kullanıcıları ve orta düzey uzmanlığa sahip internet kullanıcıları ($p=,001$) ile sıradan internet kullanıcıları ve yüksek düzey uzmanlığa sahip internet kullanıcıları ($p=,004$) arasında anlamlı bir şekilde farklılaşırken, orta düzey uzmanlığa sahip internet kullanıcıları ile yüksek düzey uzmanlığa sahip internet kullanıcıları arasında anlamlı bir farklılaşma saptanmamıştır.

Hassas verilerinin gizliliğine ilişkin endişe düzeyleri ile uzmanlık düzeyleri arasında ilişki de benzer bir sonuç vermiştir. Hassas verilerinin gizliliğine ilişkin endişe düzeyleri, sıradan internet kullanıcıları ve orta düzey uzmanlığa sahip internet kullanıcıları ($p=,005$) ile sıradan internet kullanıcıları ve yüksek düzey uzmanlığa sahip internet kullanıcıları arasında ($p=,030$) anlamlı bir şekilde farklılaşırken, orta düzey uzmanlığa sahip internet kullanıcıları ile yüksek düzey uzmanlığa sahip internet kullanıcıları arasında anlamlı bir farklılaşma saptanmamıştır.

Katılımcıların teknoloji ürünlerini kullanım kolaylığı ile kişisel ve hassas verilerine ilişkin endişe düzeyi arasındaki ilişkinin tespiti için Anova analizi uygulanmıştır.

Tablo 12: Katılımcıların Teknoloji Ürünlerini Kullanım Kolaylığı ile Kişisel Ve Hassas Verilerine İlişkin Endişe Düzeyi Arasındaki İlişki

ANOVA					
	Kareler Toplamı	df	Ortalama Kare	F	Sig.

Kişisel Veri	Gruplar Arasında	4,568	4	1,142	,7 5 6	,55 4
	Gruplar İçinde	451,482	299	1,510		
	Toplam	456,050	303			
Hassas Veri	Gruplar Arasında	2,156	4	,539	,3 9 4	,81 3
	Gruplar İçinde	408,492	299	1,366		
	Toplam	410,648	303			

ANOVA analizi sonucunda, teknoloji ürünleri kullanım kolaylığına göre kişisel verilere ilişkin endişe düzeyi ve hassas verilere ilişkin endişe düzeyi arasında anlamlı bir farklılaşma bulunmamıştır. Varyansları eşit dağılmayan davranışsal verilere ilişkin endişe düzeyi değişkeni ile olası ilişkinin tespiti için, parametrik olmayan Kruskal Wallis testi uygulanmıştır.

Tablo 13: Katılımcıların Teknoloji Ürünlerini Kullanım Kolaylığı İle Kişisel Ve Hassas Verilerine İlişkin Endişe Düzeyi Arasındaki İlişkiye Yönelik Kruskal-Wallis Testi

Kruskal Wallis Test Değerleri	
	davranis_veri_ endise_duzeyi
Kruskal-Wallis H	9,108
Df	4
Asymp. Sig.	,058
a. Kruskal Wallis Test	
b. Grup Değişkeni- Kullanım kolaylığı	

Davranışsal verilere ilişkin endişe düzeyi ile teknoloji kullanım kolaylığın arasında anlamlı bir farklılaşma tespit edilmemiştir. Başka bir ifadeyle, örneklemin davranışsal veri gizliliğine ilişkin endişe düzeyleri, teknoloji kullanım beceri düzeylerine göre farklılaşmamaktadır.

Üçüncü Hipotezin Analizi

Araştırmanın üçüncü hipotezi aşağıdaki gibidir;

H0: Güvenilir bilgiye ulaşma aracı olarak interneti kullanan katılımcılar kişisel verilerini koruma konusunda daha temkinli değildir.

H3: Güvenilir bilgiye ulaşma aracı olarak interneti kullanan katılımcılar kişisel verilerini koruma konusunda daha temkinlidirler.

Bu hipotezin test edilmesi için, katılımcıların dijital okur-yazarlık becerilerini ölçen değişken ile katılımcıların kişisel verilerini koruma konusundaki temkinlilik düzeyini ölçen değişkenlerin ortalaması analize sokulmuştur. Gruplar homojenlik varsayımını sağlayamadığı için hipotez, Kruskal Wallis Analizi ile test edilmiştir.

Tablo 14: Katılımcıların Dijital Okur-Yazarlık Becerilerini Ölçen Değişken İle Katılımcıların Kişisel Verilerini Koruma Konusundaki Temkinlilik Düzeyi Arasındaki İlişki Kruskal-Wallis Testi

Kruskal-Wallis Test Değerleri	
	Temkinlilik Düzeyi
Kruskal-Wallis H	45,996
Df	3
Asymp. Sig. (p)	,000
a. Kruskal Wallis Test	

Analiz sonuçlarına göre, $p < 0,5$ değeri, güvenilir bilgiye ulaşma farkındalığına ilişkin değişkenlerin en az bir tanesinin, temkinlilik düzeyi açısından birbirlerinden farklılaştığını göstermektedir. Farklılaşmanın hangi gruplar arasında olduğunu tespit edebilmek için, homojen varyans dağılımı sağlanamadığından, Post-Hoc Tamhane testi yapılmıştır.

Tablo 15: Katılımcıların Dijital Okur-Yazarlık Becerilerini Ölçen Değişken ile Katılımcıların Kişisel Verilerini Koruma Konusundaki Temkinlilik Düzeyindeki Farklılaşmanın Gruplaşma Boyutu

Post Hoc- Tamhane Çoklu Karşılaştırma Testi						
Bağımlı Değişken: Temkinlilik Düzeyi						
Tamhane						
(I)Farkındalık Düzeyi: Güvenilir Bilgiye Ulaşma	(J) Farkındalık Düzeyi: Güvenilir Bilgiye Ulaşma	Ortalama Fark (I-J)	St d. Hata	Sig.	95% Güven Aralığı	
					Alt Sınır	Üst Sınır
1 – (düşük farkındalık düzeyi)	2	,05162	,10021	,997	-,2315	,3347
	3	-,09535	,07117	,708	-,2892	,0985
	4	-,31695*	,05305	,000	-,4662	-,1677
2	1	-,05162	,10021	,997	-,3347	,2315
	3	-,14698	,10157	,643	-,4323	,1384
	4	-,36857*	,08981	,003	-,6306	-,1066
3	1	,09535	,07117	,708	-,0985	,2892
	2	,14698	,10157	,643	-,1384	,4323

	4	-,22159*	,0 55 56	,0 01	-,3736	-,0696
4 – (yüksek farkındalık düzeyi)	1	,31695*	,0 53 05	,000	,1677	,4662
	2	,36857*	,0 89 81	,003	,1066	,6306
	3	,22159*	,0 55 56	,001	,0696	,3736
*. Ortalama fark, 0,05 düzeyinde anlamlıdır.						

Sonuçlar incelendiğinde “kişisel verileri korumada temkinlilik” üzerinde en yüksek etkiye, en yüksek dijital okuryazarlık düzeyini ifade eden grubun etkili olduğu görülmektedir.

TARTIŞMA VE YORUM

Bu çalışmada yürütülen tartışmaların temel hedefi, kapitalizmin dinamikleri içerisinde daha fazla kar elde etme hedefiyle gerçekleştirilen kullanıcı verilerinin metalaştırılması sürecinin, kullanıcıların veri gizliliğini ve kullanıcı mahremiyetini tehdit eden unsurlarına dikkat çekmektir.

Çalışmada öne sürülen ilk hipotez, kullanıcıların kişisel verileri ile davranışsal verilerine yaklaşımlarının arasında anlamlı bir farklılaşma olduğudur. Kişisel ve davranışsal verilerin toplanması ve kullanılması ile ilgili süreçler görünür değildir. Kullanıcıların, işletmelerin ya da devletlerin, kendileri ya da başkalarına ait hangi verileri ne amaçla topladıkları hakkında bilgi düzeyleri genel anlamda çok düşüktür. İsim, kimlik numarası, konum bilgisi, banka işlemleri, kaydedilen otomatik doldurma verileri gibi kişisel verilerin paylaşımı süreci daha görünür ve dolayısıyla fark edilmesi kolaydır. Website gezinti verileri, hangi gönderileri beğendiği ve uygulamada ne kadar vakit geçirdiği gibi istatistikleri içeren davranışsal veri paylaşma süreci, kullanıcılar için görünmez ve fark edilmesi zordur. Spiekermann, Grossklags ve Berendt’in (2001, s.45) internet üzerinde çalışan bir satış botu kullanarak yaptığı deneysel araştırmasının bulgularına göre, internet kullanıcıları kimliklerini saptayabilecek bilgileri vermektan kaçınmalarına rağmen, profillerini ifşa edecek ifadeler karşısında satış botu ile iletişimi kesmedikleri ortaya çıkmıştır. Gizlilik konusunda oldukça temkinli olan kullanıcıların dahi kendilerini açık etme davranışına sürüklendikleri gözlenmiştir. Dolayısıyla internet

kullanıcılarının, kimlik saptayıcı verilerine dair gizliliği sağlama konusuna daha büyük önem atfettiği ancak davranışsal verilerine ilişkin gizliliğini feda edebildiği görülmektedir.

Bu çalışmada ise kişisel veri gizliliğine verilen önem ve davranışsal veri gizliliğine verilen önem arasında bir ilişki aranmış, bu sebeple katılımcıların her iki veri türü için de paylaşımcılık düzeyleri birbirleri ile karşılaştırılmıştır. Analiz sonucunda, kişisel veri gizliliğine verilen önem ve davranışsal veri gizliliğine verilen önem arasında negatif yönde bir korelasyon olduğu saptanmıştır. Uzmanlık düzeyine göre, veri gizliliğine verilen önem düzeyinin farklılık gösterip göstermediği de analiz edilmiştir. Sonuç olarak, teknoloji kullanım konusunda teknik uzmanlığa sahip olmayan grup ile orta düzey uzmanlığa sahip olan grup arasında, kişisel veri gizliliğine verilen önem düzeyinde anlamlı bir farklılaşma bulunmuştur. Davranışsal veri gizliliğine verilen önem düzeyinde ise gruplara göre farklılaşma saptanmamıştır.

Eleştirel teori yaklaşımında, kullanıcıların internette paylaştığı verilerin oluşturduğu gizlilik ihlalinin kullanıcı sorumlu tutulmamaktadır. Kullanıcıların kişisel ve davranışsal verileri aracılığıyla kendilerini açması, kapitalizmin dinamikleri içinde bireylerin kendilerini ortaya koymaları için gerekli bir yol olarak değerlendirilmektedir. Fuchs (2011, s.145) gizliliği, müşteriler ve çalışanların gizliliğini, onlar hakkında enformasyon toplayarak kapitalist üretimin ve reklamların verimliliğini artırmaya çalışan şirket yönetimlerinin karşısında koruyan bir şekilde kavramsallaştırır. Onun teorisine göre, güç piramidinde en aşağıda olan müşterileri ve sıradan vatandaşları, piramidin yukarısında olanların çıkarlarından korunmak için geliştirilen bir gizlilik anlayışına ihtiyaç vardır. Son yıllarda kullanıcıların veri gizliliğine ilişkin ihlallerin (Snowden olayı ve Facebook–Cambridge Analytica gibi) gündeme gelmesi ve kullanıcıların giderek daha isabetli tahminlerde bulunan hedefli reklamcılık stratejilerinin farkına varmaları, konuya ilişkin bireysel kaygıların artacağını da işaretidir.

Bu konuda yapılan başka çalışmalarda, internet kullanıcılarının gizlilik endişeleri ile internet kullanma deneyimi arasında bir ilişki bulunmuştur. Bunlardan biri olan Culnan (1995)'in araştırmasında, mail listesinden isimlerini silme sürecini bilen internet kullanıcılarının, veri güvenlikleri konusunda daha az endişeli oldukları keşfedilmiştir. Amerikan tüketicileri ile araştırma yapan Lohse, Bellman ve Johnson (2000), çevrimiçi gizlilikle ilgili sorunlara ilişkin hassasiyetin, dijital beceriler ile birlikte azaldığını gözlemlemişlerdir. Amerikan internet kullanıcıları ile 38 ülkeden internet kullanıcılarının çevrim içi gizlilik endişe düzeylerini karşılaştıran Bellman, Johnson, Kobrin ve Lohse (2004), internet kullanma deneyimi eksikliğinin, gizlilik endişesi üzerinde etkide bulunduğunu fakat bu etkinin, ortalama internet kullanma deneyimi arttığında azalma eğilimi gösterdiğini bulmuşlardır. Bir başka ifadeyle, bireylerin, internet kullanma deneyimi arttıkça çevrimiçi gizlilik endişeleri azalmaktadır. Daha çok internet kullanıcısı internet kullanım deneyimi sahibi olduğunda, çevrimiçi gizlilik endişe düzeyi azalma eğilimi göstermektedir.

Bu araştırma kapsamında, çevrimiçi gizliliğe ilişkin endişenin, kullanıcıların internet kullanım alışkanlıklarından etkileneceği değerlendirilmiş ve araştırmanın ikinci hipotezi bu bağlamda kurulmuştur. Çalışmanın bu hipotezi, katılımcıların internet kullanım alışkanlıkları ile mahremiyet ve gizlilik anlayışları arasında anlamlı bir ilişki olduğudur. İnternet kullanım alışkanlıkları kapsamında, örneklemin teknoloji kullanımında uzmanlık düzeyleri, internet kullanma sıklıkları ve teknoloji kullanım kolaylığı düzeyleri analiz edilmiştir. Kullanıcıların, gizlilik ve mahremiyetlerine ilişkin tutumları, veri gizliliklerine ilişkin endişe düzeyleri üzerinden 5’li likert ölçeği (1-Endişe duymuyorum, 5- Çok endişeliyim) ile ölçülmüştür. Daha büyük skor, her bir tür veri paylaşımı için daha yüksek endişe düzeyi anlamına gelmektedir.

Analiz sonuçlarına göre, günde 9 saatten fazla internette zaman geçiren kullanıcıların, hassas verilerine ve davranışsal verilerine ilişkin daha fazla endişe duyma olasılığı daha yüksektir. Kişisel verilere ilişkin endişe düzeyleri ile internette geçirilen günlük süre arasında ise bir ilişki bulunmamıştır. Bu anlamda kullanıcıların mahremiyet alanlarına ilişkin olan hassas verilerine (tıbbi kayıtlar, biyo-metrik sensör verileri, etnik köken/cinsel yönelim/siyasi görüş vb.) ilişkin tutumları ve davranışsal verilerine ilişkin tutumları, günlük internet kullanım sıklığından, kişisel verilerine ilişkin tutumlarından daha fazla etkilenmektedir.

Kişisel verilere ve hassas verilere ilişkin tutumlar, uzmanlık düzeyinden etkilenmezken, davranışsal verilere ilişkin tutumları uzmanlık düzeylerinden etkilenmektedir. Bulgulara göre, sıradan internet kullanıcılarının, davranışsal verilerine ilişkin endişe düzeyleri, orta düzeyde ve yüksek düzeyde uzmanlığa sahip internet kullanıcılarının endişe düzeylerinden anlamlı bir şekilde farklılaşmaktadır. Orta düzeyde ve yüksek düzeyde uzmanlığa sahip kullanıcılar arasında ise, davranışsal verilerine ilişkin endişe düzeyleri bakımından farklılaşma tespit edilmemiştir. Bunun sebebinin, davranışsal verilerin kullanıcıların gizliliğine ve mahremiyetine ilişkin ne türden ihlallere sebebiyet verebileceğine dair bilincin, sıradan internet kullanıcılarında yüksek olmaması ile ilişkili olduğu düşünülmektedir.

Araştırma sonucunda, örneklemin çoğunluğunun, cinsiyet, etnik köken, siyasi görüş, cinsel yönelim ve dini inanç gibi bilgilerinin çevrimiçi platformlar tarafından ulaşılabildiğini gösterecek davranışsal profilleme stratejilerini fark ettikleri görülmüştür. Örneklemin geneli, beğeni ve tercihlerine uygun reklam ve gönderilerin kendilerine sunulmasını ifade eden, hedefli reklamcılık stratejilerinden, rahatsızlık duyduklarını ifade etmişlerdir. Örneklemin neredeyse tamamının, verilerinin gözetim stratejileriyle ilişkili olarak depolandığının farkında oldukları görülmüştür. Ancak davranışsal veri gizliliklerini koruma, anonim hesap kullanma ve gizlilik ayarlarını düzenleme alışkanlığının, örnekleminde yaygın olmamasından yola çıkarak, gözetim stratejilerinin mevcut tehlikelerine ilişkin farkındalığın düşük olduğu yorumu yapılabilmektedir. Çünkü, söz konusu tehlikelere ilişkin farkındalık geliştirebilmek için, bireylerin teknoloji ile ilişkili güncel tartışmalara ilgi duyması,

internette güvenilir bilgiye ulaşabilecekleri dijital okur-yazarlığa ve gerekli gizlilik düzenlemelerini yapabilecekleri dijital becerilere sahip olmaları gerekmektedir.

Bu bağlamda, araştırmanın üçüncü hipotezi ile kullanıcıların veri gizliliklerini koruma konusundaki farkındalık düzeyleri ile dijital becerileri arasında ilişki aranmıştır. Çalışmanın hipotezi, güvenilir bilgiye ulaşma aracı olarak interneti kullanan katılımcıların, kişisel verilerini koruma konusunda daha temkinli olduğunu öne sürmektedir. Kişisel verileri koruma konusundaki temkinliliği ölçen 11 soru sorulmuştur. Katılımcıların güvenilir bilgiye ulaşma becerileri ile kişisel verileri koruma konusundaki temkinlilikleri arasındaki ilişki test edildiğinde, güvenilir bilgiye ulaşma becerileri yüksek olan katılımcıların, kişisel verilerini koruma konusunda daha da temkinli olduğu sonucu çıkmıştır.

Araştırma bulgularında katılımcıların, website ve uygulama sağlayıcılarının, kimliklerine dair ayırt edici özellikleri çıkarabileceklerine ilişkin bilincin, düşük olduğu gözlemlenmiştir. Katılımcılar, kendileri hakkında toplanan verilerin gerçeğe uygun çıkarımlar yapmak için yeterli olmayabileceğini düşünme eğilimindedirler. Bunun sebebi, büyük veri teknolojilerinin analiz kapasitesinin ne kadar gelişmiş olduğuna dair bilinci geliştirebilecek fırsatlarının olmaması olarak değerlendirilebilir. Benzer şekilde Rader (2014, p.61)'in araştırmasının ortaya çıkardığı üzere, internet kullanıcıları Facebook'ta tıkladıkları bağlantılar yoluyla kim olduklarına dair ayırt edici bilgilere ulaşılabilceğini fark etmiş olsalar da Google'da tıkladıkları bağlantıların yalnızca arama kelimelerinden yola çıkarak önerilerde bulunduğunu düşünme eğilimindedirler. Oysaki Google, dünyadaki en büyük veri zengini şirketler arasındadır ve kazancının büyük bir kısmını veri analitiği ve hedefli reklamcılık hizmeti sunarak kazanmaktadır.

SONUÇ

Bu araştırmada amaçlanan, büyük veri teknolojilerinin yarattığı ileri veri analiz teknikleri kapsamında, kullanıcıların veri gizliliklerine ve mahremiyetlerine ilişkin endişe düzeylerini, veri gizliliklerini sağlama konusunda farkındalık düzeylerini, veri gizliliklerine verdikleri önem düzeylerini belirlemektir. Bu unsurların, toplanan veri türlerine, internet kullanım alışkanlıklarına ve teknoloji kullanım uzmanlık düzeylerine göre farklılık gösterip göstermediği analiz edilmiştir. Araştırmanın konusu belirlenirken, uluslararası literatürde en güncel tartışmalardan biri olan büyük veri teknolojilerinin ortaya çıkardığı toplumsal problemlerin, ulusal literatürde kapsamlı bir tartışmaya açılmamış olması etkili olmuştur.

Araştırmanın bulguları bölümünde, 307 kişiye uygulanan anket verilerine ilişkin betimsel analiz bulguları incelenmiş ve araştırma hipotezleri analiz edilmiştir. Kullanıcıların veri gizliliklerine ve güvenliklerine önem vermeleri için öncelikle veri gizliliklerine yönelik tehditlerin farkında olmaları gerekmektedir. Söz konusu tehditlerin farkında olmayan bir kullanıcının, veri gizliliğinden endişe etmek için de bir sebebi olmayacaktır. Bu farkındalığın edinilebilmesi için ise, teknolojik ürünlere erişim sağlayabilmek, dijital becerilere sahip olmak, devamlı olarak dijital

platformları kullanıyor olmak, internet aracılığı ile güvenilir bilgiye ulaşabilecek dijital okur-yazarlığa sahip olmak önem arz etmektedir.

Araştırmanın özgünlük taşıdığı bağlam, kullanıcı verileri içerisinde “kişisel veriler” ve “davranışsal veriler” arasında bir ayrım gözetmesidir. Kişisel verilerin, kullanıcılara ait demografik bilgileri, konum bilgileri ve parolalar gibi bireylerin çevrimdışı dünyada da gizlilik ve mahremiyet kapsamında korumaya aldıkları bilgiler olduğu göz önüne alınmalıdır. Çünkü bu durum, bireylerin dijital platformda bu bilgilerinin gizliliğine ilişkin duyduğu endişeyi sürdürmesine ve bu tür verilerin güvenliğini sağlama konusunda daha bilinçli olmalarına sebep olabilecektir. Davranışsal veriler ise, bireylerin internete bağlı oldukları her an, sürekli olarak ürettikleri ve çoğu zaman ürettiklerinin dahi farkında olmadıkları verilerdir. Büyük verinin ileri analiz kapasitesi ile değer ve anlam kazanmış olan bu veri türü, kullanıcıların internet kullanım alışkanlıklarına dair örüntülerden yola çıkılarak, bir sonraki davranışlarının öngörülmesine yardımcı olmaktadır.

KAYNAKÇA

Aydın, M., Berkay. (2021). Dijital Sosyoloji Üzerine Notlar. A. Zinderen (Der.), *Dijital Sosyoloji Çalışmaları* içinde (ss.1-16). Nobel Yayıncılık.

Ayverdi, İlhan (2008). *Misalli Büyük Türkçe Sözlük*. Kubbealtı Yay.

Bellman, S., Johnson, E. J., Kobrin, S. J., ve Lohse, G. L. (2004). International Differences in Information Privacy Concerns: A Global Survey of Consumers. *The Information Society*, XX (5), ss.313-324.

Castells, M. (1996). *The Rise of the Network Society. The Information Age, Volume1: Economy and Society*, Wiley Blackwell Inc.

Culnan, M. J. (1995). Consumer awareness of name removal procedures: Implications for direct marketing. *Journal of direct marketing*, IX (2), 10-19.

Dyer-Witheyford, N. (2005). Cognitive capitalism and the contested campus. *European Journal of Higher Arts Education*, II (2), 71-93.

Europe, C. (2017). *Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data*. <https://rm.coe.int/16806ebe7a>. (Erişim Tarihi 10.05.2022).

Foucault, M. (2005). *Büyük Kapatılma*, Ayrıntı Yay.

Fuchs, C. (2003). The Role of the Individual in the Social Information Process. *Entropy*, IV (1), 34-60.

Fuchs, C. (2011). An alternative view of privacy on Facebook. *Information*, II (1), 140-165.

Fuchs, C. (2015). Surveillance and Critical Theory. *Media and Communication*, III (2), 6-9.

Fuchs, C. (2020). The Ethics of the Digital Commons. *Journal of Media Ethics*, 35 (2), 1-15.

Fuchs, C., & Chandler, D. (2019). *Digital Objects, Digital Subjects: Interdisciplinary Perspectives on Capitalism, Labour and Politics in the Age of Big Data*. University of Westminster Press.

Fuchs, C., & Fisher, E. (2015). Introduction: Value and labour in the digital age. In *Reconsidering Value and Labour in the Digital Age*, Springer, 3-25.

Golding, P. (2000). Forthcoming features: information and communications technologies and the sociology of the future. *Sociology*, I (34), 165-184.

Gökalp, B. & Sütüoğlu, T. (2021). Dijital Eşitsizliğin Yeni Yüzleri: Covid19 Pandemisinin Düşündürdükleri. A. Zinderen (Der.), *Dijital Sosyoloji Çalışmaları* içinde (ss.19-43). Nobel Yayıncılık.

Graeff, T. R., & Harmon, S. (2002). Collecting and using personal data: consumers 'awareness and concerns. *Journal of consumer marketing*. 19 (4), 302-318.

Handbook on European Data Protection Law. (2018). Luxemburg: Publications Office of the European Union.

Harvey, D. (1989). *1989: The condition of postmodernity: an enquiry into the origins of cultural change*. Blackwell Inc.

Harvey, D. (2008). *Umut Mekânları*, İstanbul: Metis Yayınları

Harvey, D. (2017). *Marx, Capital, and The Madness of Economic Reason*, New York: Oxford University Press.

Joseph Phelps, Glen Nowak, & Ferrell, E. (2000). Privacy Concerns and Consumer Willingness to Provide Personal Information. *Journal of Public Policy & Marketing*, I (19), 27-41.

Karaman, G. (2021). Çevrimiçi Öğrenme Toplulukları. A. Zinderen (Der.), *Dijital Sosyoloji Çalışmaları* içinde (ss.235-249). Nobel Yayıncılık.

Kişisel Verilerin Korunması Kanunu, (2016). <https://www.mevzuat.gov.tr/mevzuatmetin/1.5.6698.pdf> (Erişim Tarihi: 10.05.2022).

Neuman, W. L. (2006). *Toplumsal Araştırma Yöntemleri: Nitel ve Nicel Yaklaşımlar I, S. Özge (Çev)*. Yayın Odası.

Pasquinelli, M. (2009). Google's PageRank algorithm: A diagram of cognitive capitalism and the rentier of the common intellect. Konrad Becker and Felix Stalder (Eds), *Deep search: The politics of search beyond Google* içinde (152-162). London: Transaction Publishers.

Rader, E. (2014). *Awareness of behavioral tracking and information privacy concern in Facebook and Google*. Paper presented at the 10th Symposium On

Usable Privacy and Security (SOUPS 2014).
<https://www.usenix.org/system/files/conference/soups2014/soups14-paper-rader.pdf> (Erişim Tarihi: 10.05.2022).

Sadowski, J. (2019). When data is capital: Datafication, accumulation, and extraction. *Big Data & Society*, 6(1), 1-12. Schiller, H. (1973). *The Mind Managers*. Boston: Beacon Press.

Zinderen, A. (2021). Dijitalleşen Dünyada Gözetim Toplumunu Anlamak: Kanıksama ve Kabul. A. Zinderen (Der.), *Dijital Sosyoloji Çalışmaları* içinde (ss.47-67). Ankara: Nobel Yayıncılık.

Zinderen, İ.E. (2021). Yeni İletişim Teknolojileri Bağlamında Kimliğin Dönüşümü: Sanal Kimlik. A. Zinderen (Der.), *Dijital Sosyoloji Çalışmaları* içinde (ss.72-89). Ankara: Nobel Yayıncılık.

Spiekermann, S., Grossklags, J., & Berendt, B. (2001). *E-privacy in 2nd generation E-commerce: privacy preferences versus actual behavior*. Paper presented at the Proceedings of the 3rd ACM conference on Electronic Commerce. https://www.researchgate.net/publication/2480871_E-privacy_in_2nd_Generation_E-Commerce_Privacy_Preferences_Versus_actual_Behavior. (Erişim Tarihi: 10.05.2022).

Vercellone, C. (2007). From formal subsumption to general intellect: Elements for a Marxist reading of the thesis of cognitive capitalism. *Historical materialism*, I (15), 13-36.

Webster, F. (2014). *Theories of the information society*. London: Routledge.