Süleyman Demirel Üniversitesi Sosyal Bilimler Enstitüsü Dergisi Yıl: 2023/1, Sayı: 45, s. 189-235
Journal of Süleyman Demirel University Institute of Social Sciences Year: 2023/1, Number: 45, p. 189-235
Alınış/Recieved: 22.08.2022 Kabul/Accepted: 04.11.2022 Online Yayın/Online Published: 30.04.2023

BÜYÜK VERİDE MAHREMİYETE YÖNELİK ETİK TARTIŞMALARA GÖSTERGEBİLİMSEL YAKLAŞIM: "THE ENTIRE HISTORY of YOU"

Şehriban KAYACAN[1]
Deren BAYSAL[2]

ÖZET

Bu çalışma, büyük veri teknolojisinin gelişerek hayatımızın her alanına girdiği ve mahremiyet tartışmalarını da beraberinde getirdiği günümüzde, büyük veri tabanlı ürünlerin mahremiyet üzerine yol açtığı veya açabileceği etik problemleri sorgulamak ve geleceğe yönelik öngörüler ortaya koyabilmek amacıyla yapılmıştır. Bu doğrultuda, geleceği yansıtabilen bilim kurgu film ve dizilerinden hareketle Black Mirror dizisinin "The Entire History of You" bölümünden seçilen 8 sahne, Sassure ve Barthes'in göstergebilimsel çözümleme yöntemlerine göre analiz edilmiş, büyük veride mahremiyet üzerine getirilen etik tartışmalar bağlamında incelenmiştir. Bu analize göre, dizide yer alan arttırılmış gerçeklik ve nesnelerin interneti özellikleri taşıyan büyük veri ürünün kişi ve kişisel bilgi mahremiyeti ihlallerine yol açtığı görülmüştür. Ortaya konulan bu ihlallerin gelecek büyük veri çalışmalarında mahremiyetin etik boyutu anlamında katkı sağlayacağı düşünülmüştür.

Anahtar Kelimeler: *Büyük Veri, Mahremiyet, Etik, Arttırılmış Gerçeklik, Nesnelerin İnterneti*

A SEMIOTIC APPROACH of ETHICAL DISCUSSIONS ON PRIVACY in BIG DATA: "THE ENTIRE HISTORY of YOU"

ABSTRACT

This study has been carried out in order to question the ethical problems that big data-based products cause or may cause on privacy, and to reveal redictions for the future, in today's world where big data technology has developed and entered every area of our lives and brought privacy discussions with it. In this direction, 8 scenes selected from the "The Entire History of You" episode of the Black Mirror series, based on science fiction films and TV series that can reflect the future, were analyzed according to the semiotic analysis

[1] Şehriban Kayacan, Doktorant, Ege Üniversitesi, sehribankayaacan2017@gmail.com, ORCID: 0000-0001-5664-7928, (Sorumlu Yazar).
[2] Deren Baysal, Doktorant, Ege Üniversitesi, derenbaysall@gmail.com, ORCID: 0000-0002-6438-2904.

methods of Sassure and Barthes, and were examined in the context of ethical discussions on privacy in big data. According to this analysis, it was seen that the big data product with augmented reality and internet of things features in the series caused violations of personal and personal information privacy. It is thought that these violations will contribute to the ethical dimension of privacy in future big data studies.

Keywords: *Big Data, Privacy, Ethics, Augmented Reality, Internet of Things*

1. GİRİŞ

Kendini sürekli yenilemekte olan günümüz teknolojisi sınırları olmayan bir olgu haline gelmektedir. Teknoloji olgusunun bu yapısı insan için sayılamayacak faydalar getirse de aynı zamanda bazı tartışmaları da beraberinde getirmektedir. Son yıllarda teknolojik ilerlemeler içerisinde büyük veri (big data) ve büyük veri ile birlikte yapay zeka, nesnelerin interneti (IoT) ve arttırılmış gerçeklik en çok tartışılan konular arasında yer almaktadır. Bu akıllı teknolojilerin artışı, büyük veri kavramının ortaya çıkmasında etkili olmuştur. Terim olarak büyük veri, 2005'de çok büyük miktarlardaki veriyi ifade etmek üzere O'Reilly Media'dan Roger Magoulas tarafından bilgisayar dünyasına girmiştir. Veri tabanı yönetim sistemlerinin geleneksel yapısının yeterli olamadığı yüksek hacim, hız ve çeşitlilikteki akışkan verilerin saklanıp işlenmesi, analizi ve bunlardan ihtiyaç duyulan bilgiyi çıkarmaya dair süreci açıklayan büyük veri taşıdığı zorluklara rağmen getirdiği fırsatlar sebebiyle kurum ve kuruluşlar tarafından kullanılmaktadır (Dülger, 2016: 503).

Büyük veri kullanımının şirketler için ekonomik anlamda fayda sağladığı kabul edilmekle beraber kişisel verilerin toplanması, kullanımı, işlenmesi ve yönetilmesi gibi noktalar, güvenlik ve etik anlamında önemli sorunların doğmasına sebep olmuştur. Örneğin; 2018'de, Facebook hesapları aracılığıyla milyonlarca kullanıcıdan edinilen verilerin Donald Trump'ın ABD başkanlığına seçilmesi ve İngiltere'nin Brexit Referandumu gibi olaylarda bireylerin verecekleri oylar üzerinde yönlendirme yapmak için kullanıldığı iddia edilmiştir (Fuller, 2019: 14). Veri ihlali skandalına neden olan Facebook ve Cambridge Analytica şirketleri, kamuoyunda gizlilik standartları ve etik konusunda tartışmalara yol açmıştır (Spyratos vd, 2018: 3). Diğer yandan veri toplama, saklama, işleme amaçlı edinilen kişisel veriler sadece internet ortamı olan web veya sosyal medya üzerinden değil, akıllı gözlükler, akıllı saatler, sanal gerçeklik teknolojileri, akıllı oyuncaklar, dijital asistanlar, sanal eğitim platformları ve robot yardımcılar gibi ileri teknoloji ürünlerinden de elde

edilerek toplandığı, işlendiği veya ifşalara maruz kaldığı görülebilmektedir.

2. BÜYÜK VERİ ve NESNELERİN İNTERNETİ

2.1. Büyük Veri

Dijital dünyanın hızla gelişmesi ve bu hıza bağlı olarak yeni yöntemlerin ortaya çıkması büyük verinin, yapay zekanın ve insanların iletişim kurma şeklini değiştirmektedir. İnternetin kullanım alanlarının artması ve kullanım sıklığının fazlalaşmasıyla veri miktarında artış yaşanmaktadır. Geleneksel yöntemlerle verilerin işlenmesi, saklanması ve analiz edilmesinin zorlaşması ile büyük veri kavramı ortaya çıkmıştır. Fotoğraf, ses ve video belgeleri, mobese kayıtları, internet istatistikleri, blog ve mikrobloglar, ağ günlükleri, web sunucularının log dosyaları, sosyal medya yayınları, GSM operatörleri, hastane kayıtları, tanıma sistemleri, hava durumu sensörleri, DNA dizilişlerinin analizi, sosyal medya paylaşımları, iklim algılayıcıları gibi veri kaynakları büyük veri araçları ile işlenerek anlamlı hale gelmektedir (Işıklı, 2014: 93). Büyük verinin çok büyük boyutlarda olması verinin ölçülmesini, saklanmasını, işlenmesi ve analiz edilmesini zorlaştırmaktadır. Verileri kullanabilmek ve onlardan fayda sağlayabilmek için geleneksel yöntemleri kullanmak yetersiz kalmaktadır. Her geçen gün büyük veriyi kullanılabilir hale getirmek için yeni teknolojik yöntemler ve araçlar geliştirilmektedir. Geliştirilen araçların birçoğu Google, Amazon, Facebook ve Linked-In gibi şirketlerin çok büyük verileri saklamak, işlemek ve analiz etmek için geliştirdiği teknolojilerden oluşmaktadır (Cackett, 2013: 14).

Büyük veriyi daha iyi anlayabilmek için büyük verinin bünyesindeki temel bileşenler açıklanmalıdır. Bu bileşenler; verinin hacmi (volume), hızı (velocity) ve çeşitliliği (variety) olarak 3V başlığı altında yerini almıştır (McAfee ve Brynjolfsson, 2012: 5). Hacim (Volume), teknolojinin gelişmesine bağlı olarak gelişen dijital araç ve yöntemler sayesinde veri miktarında çok sayıda artış olmaktadır. Sosyal medya kanalları, videolar, fotoğraflar, sensörler, akıllı uygulamalar, kameralar gibi birçok araç veri üretmekte ve bu veriler saklanan veri hacmini de genişletmektedir (Akıncı, 2019: 7). Çeşitlilik (Variety), verilerin türünü ifade etmektedir. Değişik formatlarda yer alan veriler sadece yapılandırılmış değil aynı zamanda yarı yapılandırılmış ve yapılandırılmamış veriden de meydana gelmektedir (Aktan, 2018: 4). Hız (Velocity), verinin üretilmesindeki hızı ifade eden bir kavram olarak açıklanmaktadır. Bu kadar hızlı üretilen veriler de aynı hızda analiz edilebilir ve işlenebilir olmalıdır (Demirtaş ve Argan, 2015: 7). Büyük verinin temel bileşenleri; verinin hacmi (volume), hızı (velocity) ve

çeşitliliği (variety) olarak açıklanan 3V' ye ek olarak büyük verilerin diğer boyutlarından da söz edilmektedir. Bu boyutlar; doğruluk (veracity), değişkenlik (variability) ve değer (value) olarak açıklanmaktadır. Doğruluk (veracity) birçok kaynakta 4V olarak geçer. Bilgilerin kesinlik derecesi olarak açıklanan doğruluk sosyal medyadan çekilen veriler gibi birçok kaynaktan alınan belirsiz ham verilerin sorunlara neden olabileceğini savunmaktadır. Değişkenlik (variability), zamanla veride meydana gelebilecek değişim olarak açıklanabilir. Son olarak, değer (value) ise büyük verinin tüm işlemlerin sonucunda bir değer yaratıyor olması gerektiğini belirtmektedir (Gandomi ve Haider, 2015: 139).

2.2. Yapay Zeka

Teknolojik gelişmelerin artmasına bağlı olarak yapay zeka konusu üzerine yapılan çalışmalarda da artış görülmeye başlanmıştır. Teknolojinin durmaksızın ilerlemesi ile bu çalışmaların artacağı ön görülmektedir. Farklı alanlarda yapılan çalışmalar sebebiyle her disiplin kendine göre yapay zekâ tanımlamaları yapmaktadır. Yapay zekanın ortaya çıkması çok eskiye dayanmadığı için insanların zihninde ne olduğu, nasıl etkileyeceği, ne kadar gelişeceği gibi konularda soru işaretleri oluşturmaktadır. Şimdiden söylenebilecek kesin bir yargı varsa o da yapay zeka, dijitalleşme gibi teknolojik gelişmelerin insanları daha az düşünmeye ittiği gerçeğidir. İnsanlar günlük hayatlarında en basit şeyleri bile çözmeye çalışken ilk olarak bunu yapabilecek makinalara yönelmektedir. Örneğin, matematiksel bir işlem yapmak gerektiğinde zihinden çözmeye kendilerini zorlamadan ya akıllı telefonlardan ya da hesap makinalarından yardım alınmaktadır (Yücel ve Adiloğlu, 2019: 56). Yapay zeka, temel amacının makinaları daha akıllı ve faydalı hale getirmek için insan zekasının yapabileceği davranışları makinaların da yapmasının sağlanması olarak tanımlanabilir (Tektaş vd., 2012: 2). Yapay zekanın geliştirilmesi için insan zekasının nasıl düşündüğünü kavrayarak makinalarında benzer şekilde çalışmalarını sağlayacak bilgisayar işlemlerini geliştirmek gerekmektedir.

Yapay zekanın kullanım alanları; sürücüsüz araç geliştirmeleri, çevrim içi arama motorlarının hedefe yönelik arama sonuçları sunmaları, sosyal medya kurumlarının fotoğraflarda yüzleri tanımaları ve haber akışlarını filtrelemeleri, medya şirketlerinin kullanıcılarına kitap veya etkinlik önermeleri, perakendecilerin alışveriş yapanlar için kişileştirilmiş çevrimiçi alışveriş deneyimleri yaratmaları, lojistik firmalarının teslimatlar için en iyi güzergâhları seçmeleri, hükümetlerin salgınları önceden tahmin etmeleri, pazarlama uzmanlarının müşterilerine gerçek

zamanlı son derece kişiselleştirilmiş içerikler sunmaları, sanal yardımcıların tüketicilerle etkileşim kurmak için ses-kontrollü doğal bir dil kullanmaları (IIA, 2017: 5-15) olarak sıralanmaktadır.

Kullanım alanları da düşünüldüğünde yapay zekanın insanlara tehdit olarak gelmediği fayda sağlayıcı olarak geldiği ve geliştirildiği söylenebilir. Başlıca yapay zeka yöntemleri; uzman sistemler, bulanık mantık, genetik algoritma ve yapay sinir ağlarıdır (Gönül vd., 2015: 105). Bu yapay zeka yöntemlerine de bağlı olarak bazı bilimler yapay zekayı sahiplense de gelişen teknolojiye bağlı olarak birçok alanı ilgilendiren bir kavram haline gelmiştir.

2.3. Nesnelerin İnterneti

Nesnelerin interneti kavramı ilk olarak 1999 yılında Procter&Gamble şirketi için hazırlanmış bir sunumda Kevin Ashton tarafından kullanıldığı bilinmektedir (Kutup, 2011: 1-5). Nesnelerin interneti (Internet of Things / IoT), en kısa tanımı ile nesnelerin birbirleri ile iletişim halinde olmaları olarak tanımlanmaktadır (Aktaş vd., 2016: 43). Dünyada gelişen teknoloji ve dijitalleşme ile birlikte birçok alanda kullanılmaya başlanan bu kavram Türkiye'de de gün geçtikçe daha fazla kullanılmaktadır.

Veri üretimi ve paylaşımı yapan akıllı nesneler geleceğin interneti olarak anılmaktadır ve Her şeyin İnterneti, Akıllı Nesneler, Şeylerin İnterneti veya Nesnelerin İnterneti olarak isimlendirilmektedir (Söğüt ve Erdem, 2017: 1-2). Nesnelerin interneti cihazların herhangi bir veri girişi ya da insan yardımı olmadan birbirleri ile iletişim kurduğu, veri topladığı ve bu verileri kullanabildiği bir ağ sistemidir (Aktaş vd., 2016: 43). Gündüz, M., Z. ve Daş, R. nesnelerin interneti için şu örnekleri vermiştir (Gündüz ve Daş, 2018: 328).

- Buzdolabında sütün bittiğini haber verip arabanın GPS'sini en yakın markete yönlendirilmesi ve bu noktada telefonla ödeme yapılabilmesi,
- Arabaları takip eden sistemler ile herhangi bir kaza anında bunu algılayıp yardım çağrılabilmesi,
- Kapıları kilitleyen, alarmı kuran ve bu aygıtları açıp kapatabilen ev araçları uygulamaları,
- Televizyonlar, ev sunucu ve depoları, panjur sistemleri, bebek monitörleri vb. cihazların çevrimiçi kontrolü,

- Sağlık uygulamaları ile hastaya ve doktoruna ihtiyacı olan bilgilerin aktarılması ve hastanın sağlığı ile ilgili olumsuz durumların önceden belirlenmesi.

Nesnelerin İnterneti (Iot) ve World Wide Web (www.) zaman zaman birbirlerinin yerine kullanılmaktadır ancak birbirlerinden farklı kavramlardır. İnternet anahtarlar, yönlendiriciler ve diğer ekipmanlardan oluşan fiziksel katman veya ağdır. Temel işlevi bilgiyi bir noktadan diğerine hızlı, güvenilir ve güvenli bir şekilde taşımaktır. Web ise internetin üstünde çalışan bir uygulama katmanıdır. Birincil rolü, İnternet üzerinden akan bilgilerin kullanılabilir olmasını sağlayan bir arayüz sağlamaktır (Evans ve Dave, 2011: 5). Nesnelerin İnterneti, nesnelerin bir veri ağı veya İnternet üzerinden izlenmesini, koordine edilmesini veya kontrol edilmesini sağlayan fiziksel nesnelere yerleştirilmiş sensörlerin, aktüatörlerin ve veri iletişim teknolojisinin kullanılmasını ifade eder (Khalil ve Özdemir, 2018: 320). Nesnelerin İnterneti uygulamalarında üç adım vardır: Nesneden veri yakalama (örneğin, basit konum verileri veya daha karmaşık bilgiler), bu bilgileri bir veri ağında toplama ve bu bilgilere göre hareket etme ve anında işlem yapma (Manyika vd., 2013: 52).

Nesnelerin İnternetinin uygulama alanları gün geçtikçe genişlemektedir. Günlük hayatımızın her alanına ulaşabilen internetin uygulama alanlarının aşağıdaki gibi sıralandığı görülmektedir (Weinberg vd., 2015: 615-624).

- Giyilebilir teknoloji (eğlence, fitness, akıllı kol saatleri, konum izleme),
- Sağlık uygulamaları (uzaktan izleme, ambulans uzaktan izlemesi, ilaç takibi,
- Hastane malzeme takibi, erişim kontrolü),
- Bina/ev otomasyonu (erişim kontrolü, Isı & elektrik kontrolü, enerji optimizasyonu önleyici, onarım, birbirine bağlı aletler),
- Akıllı üretim (akış optimizasyonu, gerçek zamanlı envanter, kaynak izleme, çalışan güvenliği),
- Akıllı şehirler (akıllı şehir ışıklandırması, trafik kontrolü, gaz kaçağı kontrolü, güvenlik kameraları, bağlı ve merkezi sistem kontrolü)
- Otomotiv sanayi

Nesnelerin İnterneti için literatürde yer alan ilk örneklerden birisi kahve makinası uygulamasıdır (Bozdoğan, 2008: 5). Cambridge

Üniversitesinde laboratuvarda çalışan yaklaşık 15 akademisyen tek bir adet kahve makinasını kullanmaktadır. Ofislerinden çıkıp kahve almak istediklerinde çok sayıda merdiven çıkıyor ve kahve makinasını boş görüyorlardı. Durumdan sıkılan akademisyenler kahve makinasının bulunduğu yere kamera koyarak internete bağlamışlardır. Oturdukları masadan bilgisayardan kahve olup olmadığını kontrol ederek nesnelerin internetini de ilk kullanan kişilerden olmayı başarmışlardır (Gündüz ve Akyüz, 2017: 234).

2.4. Arttırılmış Gerçeklik

Son yıllarda sıklıkla kullanılan artırılmış gerçeklik ve sanal geçeklik kavramlarının anlamlarının tam olarak bilinmemesi çeşitli anlam karmaşalarına yol açabilmektedir. Bu iki kavram kimi zaman birbiriyle karıştırılabilirken kimi zaman da birbirinin zıttı gibi görülmektedir. Sanal gerçekliğin amacı, gerçek hayattan tamamen koparak sanal bir ortam oluşturmaktır. Artırılmış gerçeklikte hedeflenen ise gerçek dünyayı sanal verilerle desteklemektir (Köroğlu, 2012: 1-4). Arttırılmış gerçeklik teknolojileri, bu sistemleri deneyimleyen kullanıcıları sanal bir evrenin içinde yaşıyormuş hissi içine sokmaktadır. Kullanıcılar gerçek zamanlı olarak gerçek dünyayı ve sanal dünyayı birleştirerek algılamaktadır (Bingöl, 2018: 46). Dolayısıyla arttırılmış gerçeklik var olan dünyayı değiştiren teknolojiler değil tamamlayan teknolojiler olarak tanımlanabilir. Teknolojinin hızlı değişimi nedeniyle arttırılmış gerçeklikle ilgili tanımlarda zamanla değişiklik göstermektedir.

Aynı alanda bir arada var olduğu görülen arttırılmış gerçeklik teknolojileri gerçekliğin güçlendirilmesini de sağlamaktadır (Somyürek, 2014: 67). Artırılmış gerçeklik ile ilgili yapılan ilk uygulamalar; başa takılan görüntüleyiciler, simülatörler, basit düzeyde giyilebilir araçlar, cep bilgisayarları, masaüstü bilgisayarlar ve onlara dışarıdan entegre edilmiş kameralar olduğu söylenebilse de internet çağı ile birlikte hızla çeşitli alanlarda yaygınlaşmıştır (Bingöl, 2018: 48). Arttırılmış gerçeklik dijital çağın getirdiği olanaklar sayesinde eğitim, müze, sağlık, gezi, tasarım, imalat, doğal afet, sanat, reklam, eğlence, güvenlik, mühendislik alanında ve askeri alanda kullanılmaktadır (İçten ve Bal, 2017: 403).

Arttırılmış gerçeklik uygulamalarının insanlara muazzam bir keyif vermesinden dolayı oldukça hızlı bir biçimde kullanımı artmaktadır. Bu kullanımın artması ile zaman zaman mahremiyet ve etik problemlerde de artış görülmektedir. Yüz tanıma ve kullanıcı tanıma sistemleri gibi arttırılmış gerçeklik uygulamaları sosyal mecralarda var olan bireylerin günlük hayatta kolayca erişime açık hale gelmiş olmalarına neden olmaktadır (Bingöl, 2018: 54). Temel amacı insanların hayatını

kolaylaştırmak olan arttırılmış gerçeklik uygulamalarının gelecekte insan bedenine takılacak çip benzeri cihazlarla olacağı düşünülmektedir. Dolayısıyla, insanların bu cihazları bedenlerine yerleştirmek isteyip istememeleri durumu etik problemleri de beraberinde getirecektir.

3. Büyük Veri Üzerine Etik Tartışmalar

Günümüzde büyük veri kullanımı insanlık adına inkâr edilemez birçok fayda sağlamaktadır. Örneğin; büyük veri sayesinde şirketler müşterileriyle olan ilişkilerini kuvvetlendirebilmekte, tedarik zinciri yönetimlerini daha doğru yönetebilmekte ve ürün satışlarından edindikleri verilerle daha sağlam ve kullanıcı dostu ürünler oluşturabilmektedir (Kılıç vd., 2019: 291). Bankalar, dolandırıcılık ihtimali olan işlemleri tespitte veya kredi verme işlemlerinde büyük veriden yararlanırken, Croll (2012)'a göre hükümetlere de bütçe oluşturma, kaynakların etkili kullanımı konusunda ve hükümet-vatandaş ilişkisinin demokratikleşmesi üzerine yarar sağlama imkânı tanımaktadır. Öte yandan büyük veri, sağlık alanında hastalıkların tedavisine ve hatta hastalıkların önlenmesinde önemli bir potansiyele sahip olmakla birlikte genetik bilimin kök hücre çalışmalarının geliştirmesinde ve kişiye özgü gen haritalarının oluşturulmasında getirdiği olanaklarla insan sağlığı anlamında güçlü gelişmelere yol açabilmektedir (Kurşun, 2021: 931).

Tüm bu faydalarının yanında büyük veri, taşıdığı risklerle ve dolayısıyla etik anlamda kaygılarla aşağıdaki birçok soruyu da beraberinde getirmektedir (Işıklı, 2014: 106).

- Geniş çaplı veri araştırmaları, daha iyi araçlar, hizmetler ve mallar üretmeye yardım edecek mi?
- Büyük veriye mahremiyetin ihlâl ve istila eden pazarlama dalgasının eşlik etmesi önlenebilir mi?
- Büyük veri analizleri, çevrim içi iletişimi veya siyasi hareketleri anlamaya, analiz etmeye ve öngörmeye yardımcı olabilir mi?
- Büyük veri, örneğin protestocuların izini takip etmek ve ifade özgürlüğünü baskı altında tutmak için kullanılır mı?
- Geniş nitel veriler, insani iletişim ve kültür araştırmalarını nasıl dönüştürecek veya dar araştırma paletleri seçeneklerinde araştırmanın anlamı ne olacak? (Danah Boyd, 2012: 663).
- Sosyal tabakalar ve kuşaklar arasında yeni türden bir ayrımı yol açabilir mi?

- Bilgi ve gündelik yaşama dair kritik değişimlere yol açar mı?

Verilerin toplanma amaçlarının ya da toplanma amaçlarından sapmasının doğurabileceği olumsuz sonuçlar yani kişisel verilerin kötüye kullanım ihtimali ya da gözetimi arttıran durumu insanlık için potansiyel bir mücadele alanına sebep olma riski taşımaktadır (Eyüpoğlu vd., 2017: 179). Örneğin; bir bireyin web aramasına göre edinilen herhangi bir sağlık sorunu verisi, sigorta şirketlerinin elinde farklı anlamlar kazanabilme, sosyal ağlardaki gezinti verisi suç işlemese dahi suça eğilimli sınıfına alınabilme ya da genetik verisi işe alım sürecini etkileyebilme gibi ihtimallere sahiptir (Derinözlü, 2017: 3-4).

Taşıdığı risklerden ötürü büyük veri etik sorgulamalarla "Büyük veri, büyük tehlike midir?" şeklinde yaklaşımlara sebep olmuştur. Işıklı (2014)'nın deyimiyle "Büyük verinin altını oyan etik içerimler", tartışılması gereken bir konudur. Bu etik durumları birkaç başlık altında toplayan Işıklı, dijital telif hakları kanunlarının belirsizliğine vurgu yaparak, dijital etik ilkelerden bahsetmenin güçlüğünü ortaya koymuştur. Bu anlamda dijital alanlarda araştırmalar yapan uzmanların kamuya açık verileri bilgilendirme veya izin olmadan inceleme hakkına sahip olup olmadıklarını sorgulamıştır. Bu tarzda araştırmalar başkalarına zarar verme ihtimali taşıyabilir ve zarar görme durumunda zarardan sorumlu tutulacaklar belirsizdir (Ergen, 2018: 63). Bir başka durum; halka açık verilerin, herkese açık veya erişilebilir oluşu sebebiyle kullanılabilir olduğu algısının ne kadar etik olduğudur. Günümüzde bilgi bir kapital değeri taşımaktadır ancak bilgilerin bu şekilde edinimi ve başka amaçlar için kullanılma ihtimali karşısında veri sahiplerinin hakları göz önünde tutulmalıdır (Eroğlu, 2018: 134-135). Diğer sorun, veri yığını halindeki kişisel veriler dolandırıcılık alanını genişletme imkânı sunabilmektedir (Öz ve Kılıç, 2020: 209).

Büyük verinin mahremiyet ihlaline sebebiyet veren yapısı geleneksel etik anlayışının yetersiz bırakmaktadır. İnternet ortamının sağladığı kolaylıkla büyük veri başlangıçta kişisel bilgileri içermese de ikincil kullanımı etik açıdan sorunlu hale gelmekte ve bireylerin kişisel birçok dijital iz bırakmasını sağlamaktadır (Özcan, 2021: 12). Bu düzenin dijital fişlemeye, izin kaydına, sürekli gözetlenmeye olanak sağlaması ve bunlara özgü önlemlerin var olmayışı güvenlik anlamında problem olarak karşımıza çıkmaktadır. Bireylerin rızası olmadan kişisel kayıtlarına dayanan reklam, öneri veya mesaj gibi kişiselleştirmeler hem bireyleri meşgul ederek zamanının hem de kişisel bilgisinin istismarı olarak değerlendirilebilmektedir (Kalaman, 2019: 583). Sadece izlenmenin

ötesine geçerek özgür iradeyi kısıtlama ve kişileri bıraktığı izlere göre suçlu potansiyeli yorumuyla karşı karşıya bırakma riski taşımaktadır. Suç işlememiş ancak dijital izlerine göre suçlu potansiyeli olan kişiler ne anlamda değerlendirilecek ve hukuksal karşılığı ne olacak, şeklindeki sorular yine etik açıdan zorunlu bir değerlendirmeye itmektedir.

Diğer bir sorun ise şirketlerin kötü amaçlarla veri işlemeleri, güç uğruna kullanmaları ve buna yönelik yasal düzenlemelerin eksik oluşudur (Işıklı, 2014: 106-110). Büyük veriye etik açıdan yaklaşan Davis ve Patterson'a göre kişiler ve kuruluşlar için önemli dört faktör ortaya çıkmaktadır: kimlik, mahremiyet, mülkiyet ve itibar. Bu anlamda Davis ve Patterson, kimlik ile çevrimiçi/çevrimdışı kimlikler arasındaki ilişkinin ne olduğunu, mahremiyet ile verilere erişimi kimin kontrol edebileceğini sorgulamışlardır. Verilere kimin sahip olduğu, verilerin devredilebilir olup olmadığı ve veri sağlayanlarla kullanacak kişilerin sorumluluklarının neler olduğuyla mülkiyet faktörüne işaret etmişlerdir. (Davis ve Patterson, 2012: 3-18).

Dijital hayatın yükselişi; gizlilik, güvenlik, mahremiyet gibi yapıların anlamlarına yönelik yorumlamalara ve bu yapıların etik açıdan küresel düzeyde zedelenmesine yönelik eleştirilere tabii tutulmasına sebep olmuştur. Dijital hayatın insanları sarmalamasıyla bir yandan özgürlük fırsatı sunan bu düzen, diğer yandan insanları güvenlik ve özgürlük arasında bir yol ayrımına iterek mahremiyet alanının da daralmasına etki etmektedir (Çalık ve Toker, 2016: 9). İnternet üzerindeki hareketleriyle insanlarda mahremiyet algısının değişmesine de yol açtığı görülmektedir. Büyük veri kullanımını kolaylaştıran bu durum, mahremiyete dönük tehlikeler arz etmektedir.

Mahremiyet, bireylerin başkalarıyla ne zaman, nerede ve nasıl ilişki kurabileceklerine dair kendi iradeleriyle karar verebildikleri alanı ve bu alan üstünde sahip oldukları hakkı ifade etmektedir (Yüksel, 2003: 182). Taşıdığı bu özelliklerle mahremiyet temel insan hakları arasında yer almaktadır. Kültürden kültüre, kuşaktan kuşağa hatta kişiden kişiye göre değişiklik gösterebilen mahremiyet kavramının açıklanması zor olsa da hukuki açıdan bakıldığında "bedensel, bölgesel, bilgi ve iletişim gizlilikleri" üzerine çalışılmaktadır (Eroğlu, 2018: 132).

Mahremiyetle ilgili sorunları dörtlü sınıflandırma ile ortaya koyan Daniel J. Solove ilk sınıf olarak; gözetim ve sorgulama sorunlarını doğuran bilgi toplama, ikinci sınıf olarak da bilgi işlemi ortaya koymuştur. Bilgi işlem, verilerin saklanmasını, analizini ve manipülasyonunu ifade etmektedir. Kişisel verilerin kötüye kullanımına karşı bireylerin savunmasızlıklarının artması gibi örneklerle açıkladığı

güvensizlik, verilerinin kullanım biçimlerine erişememe ve üzerinde söz sahibi olamama gibi örneklerle açıkladığı dışlama ve bireylere ait bilgilerin amaçları dışında kullanım ihtimaliyle açıkladığı ikincil kullanım gibi alt sorun kategorilerini de barındırmaktadır. Üçüncü olarak bilgi yayılması sınıfı ile gizliliğin ihlali, ifşa, teşhir, erişilebilirliğin artışı, şantaj, çarpıtma yollarıyla kişisel verilerin başkalarına aktarılma ihtimalini öne sürmektedir. Solove'un mahremiyet sorunlarına dair sınıflandırmasından sonuncusu mahremiyet istilası ise kişisel verilere izinsiz erişimi ve keyfi müdahaleler gibi sorunları ortaya koymaktadır (Solove, 2008: 757-759).

Mahremiyetle ilgili sorunların yanı sıra sorunlara yol açan ihlallerin neler olduğu da mücadele ve alınacak tedbirler anlamında önemlidir. Bunlar; arka plan bilgileri ve dolayısıyla gerçekleşen kimlik ifşası, hassas veri ifşası ve üyelik ifşası olarak adlandırılmaktadır (Fung vd., 2010:292-293; Canbay vd., 2017: 63-64).

- Arka plan bilgileri, mahremiyet ihlallerine sebep olan faktörlerde başı çekmektedir. Eşleştirmelerle yapılan saldırılarla ortaya çıkan ihlallerden biri kimlik ifşası; kimliksizleştirilmiş verileri hedef saldırganın arka plan bilgilerini kullanarak, halka açık kimlik bilgilerinin olduğu veri tabanları ile yayınlanmış kimliksiz verileri bazı yarı tanımlayıcılarla eşleştirerek mağdurun kimliğini ifşa etmesi olarak açıklanmaktadır.
- Üyelik ifşası ise saldırganın mağdurun büyük veri içinde var olup olmadığını öğrendiğinde bir ifşa yapamayacağını; ancak yayınladığı veriye göre çıkarımlar yaparak yayınlanan veride yer alıyorsa bunu yayınlayanla ilişkisini ortaya koyarak, ifşasını gerçekleştirebilmesini ifade etmektedir.
- Veri kümesindeki bilgilerin homojen şekilde dağılım hali, saldırganın bundan faydalanarak veri bağlama yapmadan, paylaşılan veri kitlesi içinde mağdurun varlığını bilmesiyle, hangisinin mağdura ait olduğunu bilmese bile hassas verilerin aynılığından mağdurun hassas verilerini ifşa etmesini sağlayabilmektedir. Bu da öznitelik (hassas veri) ifşası olarak bilinmektedir

Mahremiyet ihlallerinin ve ifşaların doğmasına en çok maruz kalan ortamlarından biri bulut bilişimdir. Bulut bilişim; büyük çaptaki dağıtık verilerin depolanmasını, sanallaştırmasını, işlenmesini sağlayan kapasitesi ayarlanabilen dijital aygıtladır (Eyüpoğlu, 2018: 21). Bulut bilişim; ucuz, kolay uygulanabilir ve erişilebilir yapısı sayesinde mali yükten kurtararak ekonomik anlamda, ihtiyaç duyulan miktarda alan

yaratarak esneklik anlamında ve güvenlik, yedekleme ve kesintisiz hizmet sağlayarak hizmet kalitesi anlamında şirketlere avantaj sağlamaktadır (Orka, 2017: 15-20). Diğer yönden güvenlik ve mahremiyet ihlali riskine açık olabilmekte ve gizlilik endişelerini beraberinde getirmektedir. Örneğin; Bulut Güvenlik Birliği (Cloud Security Alliance-CSA), bulut konusundaki güvenlik risklerini araştırmış ve 2019 yılında "Bulut Bilişime En Önemli Tehditler" başlığıyla yayınladığı raporda bu tehditleri; veri ihlalleri, yanlış yapılandırma ve yetersiz değişim kontrolü, bulut güvenliği mimarisi ve stratejisi eksikliği, yetersiz kimlik, kimlik bilgisi, erişim ve anahtar yönetimi, hesap korsanlığı, iç tehdit, güvensiz arayüzler ve API'ler, zayıf kontrol düzlemi, meta yapı ve uygulama yapı hataları, sınırlı bulut kullanımı görünürlüğü, bulut hizmetlerinin suistimali ve kötüye kullanımı olarak sıralamıştır (CSA, 2019: 5).

Bulut teknolojisine karşı yapılan saldırılar literatürde; hizmet hırsızlığı, hizmet aksatma, veri temizliği, müşteri manipülasyonu, veri sızıntısı, buluta kötücül yazılım enjekte etme, çapraz-sanal makine yan kanallar, sanal makine kaçışı, sanal makine atlama, kötücül sanal makine oluşturma, güvensiz sanal makine göçü, sanal ağların kandırılması, hedeflenmiş paylaşılan hafıza, kimlik avı, botnetler, sesli steganografi ve sanal makine geri alma olarak görülmektedir (Karabey Aksakallı, 2019: 15-17). Dolayısıyla; global düzeyde bireysel ve kurumsal olarak kullanılan bulut bilişim veri gizliği ve güvenliği anlamında hem kişiler hem de kurumlar için mahremiyet ihlali gibi birtakım risklere açık olabilmektedir.

Mahremiyeti korumak ve ihlalleri önlemek amaçlı bilgisayar tabanlı yöntemler geliştirilmiştir. İfşa riskini azaltan, veri silme veya bozma sağlayan kimlik tanımlanmasını önleme (de-identification) olarak bilinen anonimleştirme tekniği; genelleştirme, baskılama, anatomi, permütasyon ve pertürbasyon gibi yollarla gerçekleştirilmektedir. Anonimleştirme tekniğinden iyi sonuçlar elde edebilmek için K-anonimlik, L-çeşitlilik, T-yakınlık gibi mahremiyet modelleri kullanılmaktadır (Victor vd., 2016: 65-67). Anonimleştirme her ne kadar bir çözüm olarak görülse de örneğin; 2006'da yayın ve DVD satışına yönelik faaliyet gösteren Netflix'in kullanıcılarına dair film önerisi sunmak için düzenlediği bir yarışmadaki büyük veri kullanımıyla aslında bu çözümün de kırılabileceğini göstermiştir (Gözüküçük, 2014: 89). Netflix kişisel bilgilerini yayınlamasa dahi yüzlerce abonesini sayısal film puanlamasıyla ilgili verilerini yayınlamıştır ve bu da kullanıcı kimliklerinin açığa çıkmasına yol açabilecek bir durumu ortaya

koymuştur. Austin Üniversitesi 'den bazı araştırmacılar, Netflix'in yayınladığı veriler ile İnternet Film Veritabanı (IMDB) üzerinden yapılan film puanlamaları eşleştirerek kullanıcıların kimliklerinin açığa çıkarılabileceğini göstermişlerdir (Narayanan ve Shmatikov, 2008: 1-3). Çünkü büyük veri kümesinde herhangi bir kullanıcının kimliğine dair tanımlayıcı veriler verilmese dahi o kullanıcının birkaç filmi puanlamasına göre bile kimliği hakkında çıkarım yapabilmektedir. Kısacası, mahremiyeti koruma yollarından olan anonimleştirmenin de büyük veri yöntemleriyle etkisiz hale gelebilme ihtimali söz konusudur. Kişisel verilere, mahremiyete yönelik bu ihlaller, dünyada bu konuya dair hukuki düzenlemelerin de yapılmasına neden olmuş böylelikle büyük verinin getirdiği risklerin de önüne geçilmeye çalışılmıştır. Ekonomik İşbirliği ve Kalkınma Örgütü, 2013 yılında kişisel verileri korumaya ve işlenirken dikkat edilecek hususlara dair, sınırlılık, kalite, amaca özgülük, kullanım sınırlaması, güvenlik, açıklık, bireyin rızası ve hesap verilebilirlik gibi temel prensiplerin benimsenmesi gerektiğini ortaya koymuştur (OECD, 2013: 14-15). Türkiye'de özel hayat gizliliği anayasada ceza ve medeni kanunda düzenlemelerin var olmasının yanı sıra, 2003'deki Bilgi Edinme Kanunu 2016'daki "6698 sayılı Kişisel Verilerin Korunması Kanunu" nun oluşturulmasıyla kişisel veri mahremiyetini korumaya yönelik hukuki çalışmalar yapılmıştır (Eroğlu, 2018: 134-135). Yapılan birçok araştırmaya göre; insanların, çevrimiçi eylemleri sırasında taşıdıkları endişelerin arttığı ortaya konmuştur. Örneğin; kullanıcı baz alınarak yapılan bir araştırmada 1500 internet kullanıcısının %91'i web sitelerini kullanırken izlendiklerine yönelik kaygı taşırken, %81'i web sitelerinde e-postalarını paylaşmaktan endişe duymaktadır (Karlıdağ, 2014: 105). Aralık 2018'de yapılan bir araştırmaya göre; Amerikalı kullanıcıların %67'si veri gizliliğini korumak üzerine hükümetin daha fazlasını yapması gerektiğini düşünmekte (Cary, 2018); diğer yandan Şubat 2019'daki bir ankete göre çevrimiçi kullanıcıların %66'sı kendi hükümetleri nedeniyle çevrimiçi mahremiyetlerine yönelik kaygı taşımaktadır (Clement, 2019). Mart 2019'da McAfee tarafından yapılan bir ankete göre tüm dünyadaki kullanıcıların %40'ından fazlası kişisel verileri üzerinde kontrol sahibi olmadıklarını düşünmekte ve ebeveynlerin de 1/3'nin çevrimiçi güvenlik risklerini çocuklarına nasıl açıklayacağını bilmediklerini ortaya koymaktadır (The Manifest, 2019)

4. Metodoloji

4.1. Araştırmanın Amacı ve Önemi

Çalışmanın amacı, sahneleme örneğinden yola çıkılarak gelecekte kullanılacak bu tarz büyük veri nitelikli ürünlerin etik anlamdaki sorunlarını ortaya koymaktır. Araştırmanın önemi ise, bu sorgulamaların büyük verinin gelecekte yaratabileceği etik sorun ve sorgulamalara dolayısıyla alınabilecek önlemlere katkı sağlayacağının düşünülmesidir.

4.2. Araştırmanın Yöntemi

Göstergebilim, anlamı anlamak, anlamın nasıl oluştuğunu çözmek ve en anlamın olmasını sağlamak için yapılmaktadır. Anlam üzerine kurulmuş olan göstergebilimsel analizin iki farklı açıdan yorumlayan kurucusu bulunmaktadır. Sassure'un göstergebilim modelinde gösterge, bir gösteren ve gösterilenden oluşmaktadır. Sassure göstereni, göstergenin algılanan imgesi olarak tanımlarken gösterileni, gösterenin göndermede bulunduğu zihinsel kavram olarak tanımlamaktadır. Göstergenin iki düzlemli zihinsel bir süreç olduğunu söyleyen Sassure, kavram ve sözcüğün birbirinden ayrılamayacağını vurgulamaktadır. Göstergeleri inceleyen bilim dalının diğer bir öncüsü olan Barthes ise dil kavramının diğer kavramlardan önde olduğunu savunmaktadır. Sassure'dan farklı olarak göstergebilim ve dilbilimin birbirini kapsayıp kapsamadığı üzerinde düşünmektedir. Sonuç olarak da göstergebilim dilbilimin bir bölümüdür düşüncesini savunmaktadır. Barthes göstergeleri düz ve yan anlamıyla çözümler düz anlam görünen yan anlam ise mitsel anlatıyı içermektedir.

Araştırma için Sassure ve Barthes'in göstergebilimsel çözümleme yöntemleri kullanılarak, dizi bölümünde 8 sahne analiz edilmiş, büyük veri ve mahremiyet bağlamında anlamlar inşa edilmiştir. Mahremiyet ve etik üzerine incelemeler, büyük veriye etik açıdan yaklaşan Davis ve Patterson'un kişiler ve kuruluşlar için önemli olarak "kimlik, mahremiyet, mülkiyet ve itibar" şeklinde ortaya koyduğu faktörlerden özellikle 'mahremiyet' üzerinden değerlendirilmiştir. Dizi bölümü, araştırmacılar tarafından defalarca izlenerek, üzerinde notlar alınmış, çözümlenecek sahneler bu şekilde seçilmiştir.

4.3. Araştırmanın Örneklemi

Araştırmada büyük veri ile ilgili tüm film veya dizilere ulaşmak yani tüm evrene ulaşmak mümkün değildir. Bu yüzden örneklem olarak, amaçlı örnekleme çeşitlerinden tipik durum örneklem yöntemine göre, Black Mirror dizisinin birinci sezonunun üçünde bölümü olarak

18.11.2011 yılında yayınlanan "The Entire History of You" isimli bölümü seçilmiştir. Bu örneklem seçimdeki amaç; bölümde, bireylerin hayatının her anını kaydeden büyük veri teknolojili (yapay zeka, IoT ve arttırılmış gerçeklik tabanlı) fütüristtik bir ürünün kullanılmasıyla ortaya çıkan mahremiyet ihlallerinin sahnelenmiş olmasının, gelecekte olabilmesi muhtemel büyük veri teknolojileri ve bu teknolojilerin doğurabileceği etik soruların incelenebilmesidir.

5. Göstergebilimsel Açıdan "Black Mirror" Dizisinin 'The Entire History of You' Bölümünün Çözümlemesi ve Bulgular

Görsel 1: Dijital Ekran ve Uygulamalarını Kullanılabildiği Taksi

Kaynak: Welsh, B. (Director), **The Entire History of You**. Channel 4, 2011.

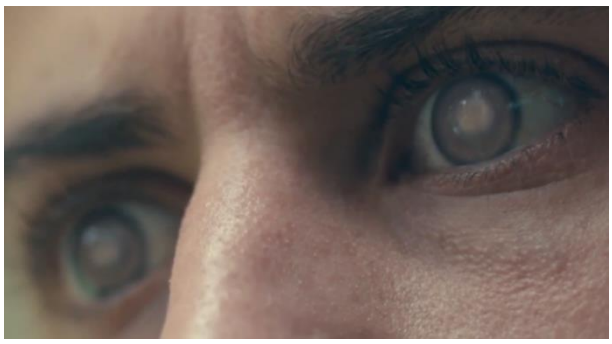
Görsel 2: İnsanın Her Gördüğünü ve Her Anını Kaydeden ve Kulak Arkasına Deri Altına Takılan Çip

Kaynak: Welsh, B. (Director), **The Entire History of You**. Channel 4, 2011.

Görsel 3: Çipin Dijital Uygulamasındaki Zaman Çizelgesi

Kaynak: Welsh, B. (Director), **The Entire History of You**. Channel 4, 2011.

Görsel 4: Çipin Kullanımı Sırasında Gözlerin Görünümü



Kaynak: Welsh, B. (Director), **The Entire History of You**. Channel 4, 2011.

Sahne-1: (02:13 – 03.34 dk.) Liam, iş görüşmesinden çıkıp havaalanına gitmek üzere taksiye binmiştir. Takside var olan teknolojik cam ekran sayesinde iş görüşmesi kayıtlarını tekrar izlemek için bellek çipini ekrana bağlantılandırmıştır. Bu arada bellek çipi cihazı hakkında bilgiler verilerek tanıtımı yapılmıştır.

Gösterge	**Gösteren**	**Gösterilen**
Mekan	Taksi	İçinde büyük teknoloji barındıran, sadece ulaşım amacına ek olarak içinde bireylerin dijital ekran ve uygulamalarını kullanılabildiği ortam.

Düz anlam olarak ulaşım sağlayan ve dijital uygulamaların kullanılabildiği taşıt ortamı şeklinde verilen mekan, yan anlamıyla;

taksinin sadece ulaşım amacına hizmet eden bir taşıt değil, içinde dijital uygulamaların da kullanılabilmesine de hizmet eden ortam haline gelmiş olduğunu göstermektedir. İçinde araçla bağlantılı bir şekilde dijital uygulamaların dahi kullanılabildiği, günümüz taksi kullanımının salt ulaşım amaçlı kullanımından öteye geçecek düzeyde gelişmiş bir teknolojinin varlığının ortaya konmakta ve bu da yüksek teknolojik gelişmelerin insanların günlük yaşamındaki basit ortamlarına dahi eklemlendiğini göstermektedir.

Gösterge	**Gösteren**	**Gösterilen**
Nesne	Çip kumandası	Basit bir ulaşım aracı olan takside bile sadece ekrana temas ettirilerek kullanılabilen, çip kullanımını sağlayan kolay taşınabilir teknolojik araç

Çip kumandası düz anlamıyla, dijital bir uygulama kullanımını sağlayan taşınabilir teknolojik aracı ifade etmekteyken; yan anlamıyla, bedende taşınan teknolojik bir çipin, her yerde, basit taşınabilir bir araçla kullanımına olanak sağlayan ileri bir teknolojinin varlığını göstermektedir.

Gösterge	**Gösteren**	**Gösterilen**
Nesne	Çip	İnsanın her gördüğünü ve her anını kaydeden, kulak arkasına deri altına takılan, insan beyni ile bağlantılandırılmış yüksek teknolojili ürünü dijital alet ve bu aletin tanıtımı.

Düz anlam olarak deri altına takılan, insanın gördüklerini kaydeden teknolojik ürün şeklinde öne çıkan çipin taşıdığı yan anlam; insanın özel veya değil tüm kişisel yaşantısını, her anını, her gördüğünü kaydeden ileri teknoloji üretimi bir aracın günlük yaşamın bir parçası haline gelmiş şekilde kullanımı ifade etmekteyken aynı zamanda, insanların kendi vücudunda implant şeklinde, her anlarını kayıt altında tutan, biyoteknolojik bir bellek taşımalarının kabulünü de orya koymaktadır. Bu durum bir nevi insan tarafından robotlaşmanın kabulünü ve yüksek teknolojinin insanların günlük yaşam pratiği haline geldiğine işaret etmektedir.

Gösterge	Gösteren	Gösterilen
Nesne	Cam ekran	Dijital uygulamalara izin veren, bu uygulamalar aracılığıyla kişisel verilerin yansıtılıp incelendiği araç. Her insanın kullandığı bir taşıt içinde, her insanın kendi verilerini yansıtıp görebildiği herkes tarafından ortak şekilde çip uygulamasını açmak ve kişisel verilerini yansıtmak için kullanılan araç.

Düz anlamıyla kişinin bilgilerini yansıtıp incelediği dijital aracı ifade eden cam ekran, yan anlam olarak insanların kişisel bilgilerini, taksi gibi herkesçe kullanılan bir taşıtta bulunan, yine herkesin kişisel verilerini yansıttığı bir ekranda inceleyebilmesini sağlayan teknolojik gelişme durumu ortaya koymaktadır. Bu da başka insanlar da kişisel verilerini aynı yere yansıtarak inceleyebilmesine rağmen, bireylerin durumu kabul ederek kişisel verilerini endişe duymadan o ortak alanlara yansıtıp inceleyebilmesini göstermektedir.

Gösterge	Gösteren	Gösterilen
Dijital program	Çipin dijital uygulamasındaki zaman çizelgesi	İnsanın her anını kayıt altına alan çipin, insanlara geçmiş zamanlara ulaşma olanağı tanıdığı ve bu zamanları tarih tarih bir çizelge halinde ortaya koyabilen bir dijital uygulama

Zaman çizelgesi, düz anlam olarak bellek çipinin uygulaması içinde var olan geçmişe dönük ve geriye zaman çizelgesini gösterirken, yan anlam olarak ise insanların bellek çipi uygulamasındaki zaman çizelgesi aracılığıyla geçmiş bir tarihlerdeki her anısına ulaşıp izleyebilmesini göstermekte, dolayısıyla insanın geçmişini kaydeden çip ile istenilen her an insanların zaman çizelgesi üzerinden kendi geçmişine geri dönüp olanın tüm ayrıntılarına ulaşabilmesini sağlayan teknoloji varlığını ortaya koymaktadır. Diğer yandan geçmişe geri dönüp geçmiş zamanı izlemeye olanak sağlayan bu teknolojik durum sayesinde, insan için "unutmak" kavramının bir nevi ortadan kalkması ve her anın kontrol edilebilmesini göstermektedir.

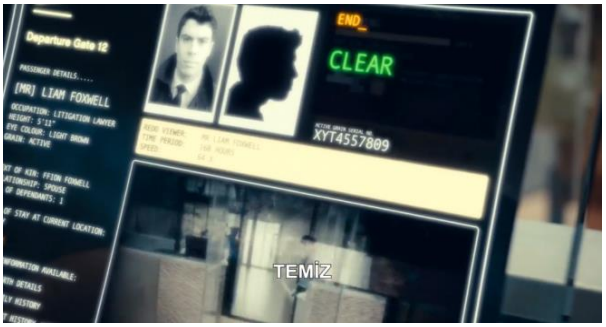
Gösterge	Gösteren	Gösterilen
İnsan	Erkek birey	Biyolojiyi ve teknolojiyi bütünleştiren yüksek teknoloji ürününü kullanan insan.

Erkek birey düz anlamıyla çipi kullanan kişi olarak gösterilirken, yan anlamıyla bireyin, deri altına takılan bu teknolojik ürünü kullanımı kabulü ve bunun günlük yaşamına yerleşmiş olmasını göstermektedir. Bu sayede birey iş görüşmesini tekrar izleyerek, görüşmecilerin onu işe alıp almadığı konusunda tahmin yürütmeye çalışmaktadır.

Gösterge	Gösteren	Gösterilen
Organ	Gözler	Bellek çipinin kullanımında her anın kayıt edilmesinin gözler aracılığıyla sağlanması. Çip sayesinde geçmiş zaman izlenirken gözlerin, perde inmiş gibi bir hale gelmesi. Kullanım sırasında gerçek yaşamdan kopup sadece görüntülerin izlenmesi, gerçek dünyanın görülememesi.

Bireyin gözleri, düz anlamıyla çipin kayıt edeceği verileri göz organının görme işlevi aracılığıyla elde etmesi göstermekteyken, yan anlam ise göz organı ile teknolojinin bütünleştirilmesi, bir anlamda robotlaşmayı ve kişisel dünyanın kaydı teknolojisi ile gözlerin adeta bir cihaz haline gelmesini göstermektedir.

Görsel 5: Havaalanındaki Güvenlik Önlemleri



Kaynak: Welsh, B. (Director), **The Entire History of You**. Channel 4, 2011.

Görsel 6: Güvenlik Bilgisayarları

Kaynak: Welsh, B. (Director), **The Entire History of You**. Channel 4, 2011.

Görsel 7: Havaalanı Güvenliğinden Sorumlu İnsanlar

Kaynak: Welsh, B. (Director), **The Entire History of You**. Channel 4, 2011.

Görsel 8: Havaalanında Kişisel Verilerin ve Günlük Yaşam Kayıtlarının Görevliler Tarafından İzlenebilmesi

Kaynak: Welsh, B. (Director), **The Entire History of You**. Channel 4, 2011.

Sahne-2: (03:45 – 04:16 dk.) Liam seyahat etmek için havaalanına gelmiştir. Havaalanındaki güvenlik önlemlerinin dijital sistemler üzerine kurulu olduğu ve üst düzey nitelikte olduğu görülmektedir. Güvenlik görevlileri bilgisayar üzerinden Liam'ın kişisel bilgilerini incelerken, aynı zamanda bellek kaydındaki son 24 saat ve 1 haftalık kişisel yaşantısın kayıtlarını isteyerek incelemektedirler. Güvenlikler, Liam'ın uçuş için tehlike arz edebilecek biri olup olmadığını tespit etmeye çalışmaktadırlar. Ancak bu incelemede, Liam'ın yaşı, milliyeti gibi kişisel bilgilerinin yanı sıra, aile hayatı, eşi, çocuğu ve iş görüşmesine dair kayıtları hızlandırılarak güvenlik tarafından izlendiği ve hatta iş görüşmesindeki bireylerin kimlik bilgilerine kadar ulaşıldığı da görülmektedir.

Gösterge	**Gösteren**	**Gösterilen**
Mekân	Havaalanı	İçinde çok insanın olduğu ve bu yüzden güvenli tutulması gerektiği için teknoloji aracılı yüksek güvenlik önemleri ile korunan yer.

Havaalanı düz anlamda, seyahat için kullanılan ve genel olarak içinde her zaman insan yoğunluğunun olduğu yer olarak görülmekteyken; yan anlamda ise insan yoğunluğunun sürekli bir halde olduğu halka açık bir yerin, risklere karşı yüksek teknoloji aracılığıyla korunduğunu ve teknolojinin, günlük hayattaki mekanlara da derin bir şekilde girdiğini göstermektedir.

Gösterge	**Gösteren**	**Gösterilen**
Nesne	Güvenlik Bilgisayarları	Havaalanında güvenlik önlemi olarak kullanılan dijital sistemlerde, yolcuların kişisel bilgilerinin ve günlük hayat kayıtlarının, üzerine aktarılarak güvenlikler tarafından incelenebildiği araç Havaalanındaki bireylerin, herhangi bir güvenlik tehdidi arz edip etmediğinin ortaya konulmasında kullanılan araç

Düz anlamda bilgisayarlar havaalanında güvenlik önlemi için kullanılan aracı göstermektedir. Yan anlamda ise havaalanına giren her bireyin tüm kişisel bilgilerinin ve çip sayesinde kayıt altına aldıkları yaşamlarının her anının güvenlik amaçlı da olsa üçüncü kişiler tarafından bilgisayar aracılığıyla görülüp incelenebildiğini ortaya koymakta,

bireylerin kişisel bilgileri ve hayat kayıtlarının incelenmesi sayesinde, bireylerin güvenlik tehdidi yaratıp yaratmayacağına karar verildiğini göstermektedir.

Gösterge	**Gösteren**	**Gösterilen**
Bilgi	Kişisel veriler, kişisel hayat kayıtları	Havaalanındaki bireylerin tüm kişisel verilerinin ve günlük yaşam kayıtlarının üçüncü kişiler tarafından izlenebilmesi

Kişisel veriler, düz anlamda kişinin sadece kendisine ait tüm bilgi ve kayıtları ifade ederken, yan anlamda bireylerin kişisel bilgi ve kişisel hayat kayıtlarının güvenlik sebepleriyle ortaya dökülebilmesi ihtimalini göstermektedir. Havaalanı güvenliğinin sağlanması için güvenlik önlemleri teknoloji ile üst düzeyde tutulurken, yolcuların yakın geçmiş kayıtlarında var olan bireylerin bile kimlik bilgilerine ulaşılarak belki de olması gerekenden fazla kişisel bilginin toplanıldığını, belli yönlerden, kişilerin mahremiyet sınırlarının delinmesi ile bir anlamda gözetim toplumu oluşturulduğu göstermektedir.

Gösterge	**Gösteren**	**Gösterilen**
İnsan	Erkek birey, uçak yolcusu	Havaalanında güvenlik için, bireyin tüm kişisel veri ve kayıtlarını vermek durumunda olması

Düz anlamda uçak yolculuğu için havaalanına gelen birey gösterilirken, yan anlamda bireyin, havaalanı güvenliği için tüm kişisel bilgilerini ve bellek kayıtlarını sunma zorunluluğu, güvenliğin sağlanması adına bireyin tüm kişisel bilgi mahremiyetini güvenliklerle paylaşma zorunluluğunu göstermektedir.

Gösterge	**Gösteren**	**Gösterilen**
İnsanlar	Güvenlik görevlileri	Teknoloji aracılığıyla, havaalanına gelen yolcuların tehdit arz edip etmediğini saptayan görevliler.

Güvenlik görevlileri, düz anlamıyla havaalanı güvenliğinden sorumlu insanları, yan anlamıyla ise bu görevlilerin, yolcuların herhangi bir tehdit oluşturup oluşturmadığını teknolojik bir sistemle saptarken, insanların tüm kişisel bilgilerini görüp kayıtlarını izleme yetkilerinin

bulunmasını göstermektedir. Ayrıca bu güvenlik görevlilerinin üçüncü kişiler olarak yolcuların kişisel verilerinin her detayını görebilmesi ile oluşan mahremiyet ihlalini de göstermektedir.

Görsel 9: İş Görüşmesi Üzerine Değerlendirme Yapmak İsteyen Arkadaş Grubu

Kaynak: Welsh, B. (Director), **The Entire History of You**. Channel 4, 2011.

Görsel 10: İş Görüşmesinin Ekrana Yansıtılması

Kaynak: Welsh, B. (Director), **The Entire History of You**. Channel 4, 2011.

Görsel 11: Arkadaş Grubuna Yeni Katılan ve Mahremiyetini Korumak İçin Özel Bilgilerini Vermek İstemeyen Birey

Kaynak: Welsh, B. (Director), **The Entire History of You**. Channel 4, 2011.

Sahne-3: (07:28 – 08:14 dk.) Liam'ın eşi Fi, eski arkadaşlarının evine gitmiş, Liam da yanlarına geçerek onlarla tanışmıştır. Liam'ın yeni tanıştığı bu kişiler, birlikte salonda otururlarken, Liam'a iş görüşmesinin nasıl geçtiğini sormuş ve kaydını ekrana yansıtarak iş görüşmesi üzerinde değerlendirme yapmak istemişlerdir. Arkadaş gurubunun değerlendirme yapmak üzerine olan ısrarcı yaklaşımı karşısında Liam, bu kaydını paylaşmak istememiş, durumdan rahatsız olmuş; ancak bu isteği güçlü bir şekilde geri çevirememiştir. Liam'ın köşeye sıkışarak baskı altında hissettiği sırada, Fi'nin arkadaşı Jonas olaya dahil olarak, Liam'ın durumdan rahatsızlığını ortaya koymuş ve arkadaşlarını, bunu yapmaktan vazgeçirmiştir.

Gösterge	**Gösteren**	**Gösterilen**
Mekân	Ev salonu	Arkadaşların birlikte oturup sohbet ettiği alan

Düz anlamıyla ev salonu arkadaşların birlikte vakit geçirdiği alanı göstermekteyken, yan anlamıyla birbirleriyle arkadaş olan insanların ev ortamında bir araya gelip evin ortak toplanma alanı olan salonda yani rahat bir ortamda sohbet etmesini güzel vakit geçirmesini göstermektedir.

Gösterge	Gösteren	Gösterilen
İnsanlar	Kadın ve erkek arkadaşlar	Aralarına yeni birinin girdiği bir arkadaş grubu, Yeni kişinin iş görüşmesi konusunda sorular soran ve görüşmesini değerlendirmek için kişinin iş görüşmesi kaydını ekrana yansıtmasında ısrar eden arkadaş grubu

Düz anlamda aralarında yeni tanıştıkları birinin olduğu, kadın ve erkeklerden oluşan arkadaşları göstermekteyken, yan anlamda ise daha önceden tanışan bir arkadaş grubuna eşi sebebiyle yeni birinin katılmasını, arkadaş grubunun yeni bireye iş görüşmesini ekrana yansıtması konusunda çoğunluk olmalarından güç alarak ısrar etmesini, bireyin karşısında ısrarcı çoğunluğun olmasıyla istekleri doğrultusunda bireyi sıkıştırmalarını ve bireyin paylaşmak istemediği kişisel kaydına, yani mahremiyetine müdahale etmeye çalışan ısrarcı bir grubun varlığını göstermektedir.

Gösterge	Gösteren	Gösterilen
İnsan	Salonda, eşi dolayısıyla yeni tanıştığı arkadaş grubuyla oturan erkek birey	Ortamdaki yeni tanıdığı kişilerin kişisel kaydını göstermesi istemi sonucunda bunu paylaşmak istemediği için çoğunluk karşısında köşeye sıkışmış baskı altında kalmış birey

Düz anlamda daha önceden birbirlerini tanıyan bir arkadaş grubuna yeni katılan erkek birey gösterilmekteyken, yan anlamda da bireyin, paylaşmak istemediği kişisel kaydı konusunda grup baskısına maruz kalması, bunu kolayca reddedememesi, bireyin mahremiyetini koruma isteği karşısında, çoğunluk bir grubun, bu mahremin ortaya konması ve üzerinde değerlendirme yapılması istemiyle bireyin zor durumda kalması ve bireyin çoğunluk karşısında baskı altında ve tek kalmış hissetmesi ortaya konmuştur.

Gösterge	Gösteren	Gösterilen
Nesne	Çip uygulamasının dijital bir şekilde yansıtılabildiği cam ekran	Çip uygulaması kayıtlarının ev ortamında da televizyon gibi ekranlara kolayca yansıtılabilmesini ve herkes tarafından aynı anda izlenebilmesini sağlayan araç

Düz anlamda bireylerin kayıtlarını yansıtabildiği, ev salonunda duran televizyon benzeri cam ekran, yan anlamıyla bireylerin kişisel kayıtlarının ev ortamında TV gibi ekranlara kolayca yansıtılabilmesini, bireylerin birbirlerinin kişisel kayıtlarını ya da mahremiyetlerini paylaşmasıyla insanların bunu tıpkı film, dizi izler gibi paylaşıp izleyebilmesini göstermektedir. Aynı zamanda bu durumun, paylaşmak istenildikten sonra herkesçe normal olarak kabulü ortaya konulurken, bireylerin kişisel kayıtlarını yansıtmasıyla herkes tarafından aynı anda rahatça izlenebilmesi ve bunu sağlayan teknolojik gelişmişliği de göstermektedir.

Görsel 12: Kulak Arkasından Çalınan Çipin Konuşulduğu Sofra

Kaynak: Welsh, B. (Director), **The Entire History of You**. Channel 4, 2011.

Görsel 13: Kulak Arkasından Çalınan Çipin Gösterilmesi

Kaynak: Welsh, B. (Director), **The Entire History of You**. Channel 4, 2011.

Görsel 14: Geçmişteki Eğlenceli Günlerin Ekrana Yansıtması

Kaynak: Welsh, B. (Director), **The Entire History of You**. Channel 4, 2011.

Sahne-4: (11:40 – 12:54 dk.) Arkadaşlar hep beraber yemek yiyip sohbet etmektedirler. Aralarından Hallam'ın çipi olmadığı ortaya çıkmış ve Hallam çipinin kesilip ondan çalındığını yani gaspa uğradığını anlatmıştır. Herkes bu duruma şaşırırken, bunu kimin neden yaptığını merak etmişler, Hallam ise zengin bir sapığın yapmış olabileceğini düşündüğünü belirtmiştir. Üstelik kayıtlarının da şifresiz olduğunu ifade etmiştir, dolayısıyla herkesin onun tüm özel kayıtlarını görebileceği anlaşılmaktadır. Jonas çipin nasıl kesilip çalındığını sorgularken, Hallam'ın çipin çıkarıldığı yerdeki yara izine bakmak istemiştir. Diğer yandan sohbet ilerledikçe, aralarından başka bir arkadaşları, kendi bellek kayıtları arasında olan, bu gruptaki bazı arkadaşların birlikte eğlendikleri

geçmiş kayıtlarını duvardaki ekranlara yansıtmış, hep beraber o zamanları izleyip anılarını yad etmişlerdir.

Gösterge	**Gösteren**	**Gösterilen**
Mekân	Evin yemek odası	Arkadaşların birlikte sohbet edip yemek yedikleri rahat ortamın varlığı

Düz anlamda arkadaş grubunun beraber yemek yedikleri ortamı gösteren yemek odası yan anlamda, arkadaşların birlikte güzel vakit geçirdikleri, kendilerine ait olayları paylaştığı ve anıları yad ettikleri rahat ve samimi bir ortamda olduklarını göstermektedir.

Gösterge	**Gösteren**	**Gösterilen**
Nesne	Yemek masası	İnsanların birlikte yemek yemesi, samimi ve sohbetli bir ortam oluşması

Düz anlamda insanların yemek yedikleri yeri gösteren yemek masası, yan anlamda ise insanları bir araya getiren birlikte güzel vakit geçirmelerini sağlan bir buluşma noktasını göstermektedir.

Gösterge	**Gösteren**	**Gösterilen**
İnsan	Yan yana oturan biri esmer diğerleri sarışın 3 kadın birey	Bir kadının dinlediği olaya şaşırması, olayı anlatan ve olayı bilen kadının üzülmesi

Düz anlamda yaşadığı bir olayı anlatan bir arkadaşlarını dinleyen 2 kadını gösterirken, yan anlamda ise olayı bilerek duruma üzülen ve olayı duyup şaşıran arkadaşları göstermektedir.

Gösterge	**Gösteren**	**Gösterilen**
İnsan	Esmer kadın birey	Bireyin deri altındaki çipinin kesilip çalınması sebebiyle kulak arkasında kalan yara izini oradaki arkadaşına göstermesi Çip gaspına uğrayan kadın

Yaşadığı olayı anlatan esmer kadın birey düz anlamla görülürken, yan anlamda ise kadının gaspa uğradığı, çipinin kesilerek ondan çalındığı,

kişi ve kişisel bilgi mahremiyetine yönelik saldırı yaşadığı gösterilmektedir.

Gösterge	**Gösteren**	**Gösterilen**
İnsan	Yara izi	Bireyin implant çipinin oyulup çalınmasıyla kalan iz Bireyin çipinin zorla ondan alınması ve bireyin şiddet görmesi Bireyin kişisel bilgi ve kişi mahremiyetine yönelik saldırıya uğraması Kişisel verilerin zor kullanılarak başka ellere geçebileceği riski

Düz anlamda yara izi, kadının vücuduna aldığı bir zararı gösterirken, yan anlamıyla kadının mahremiyetine yönelik yaşadığı tecavüzü, şiddet görmüş olmasını göstermektedir. Aynı zamanda kişisel verilerin zor kullanılarak istenmeyen başka ellere geçebilme riskinin de olduğunu göstermektedir.

Gösterge	**Gösteren**	**Gösterilen**
Organ	Erkek birey elleri	Bireyin çipi oyulan arkadaşının yara izine dokunması, normalde çip olması gereken yerdeki çipin artık olmadığını hissetmeye çalışması Kadınla flört etmesi

Düz anlamda kadının yarasına dokunan erkeği gösteren eller, yan anlamıyla herkeste olan çipin, olmadığı bir kişiyi görünce çipsiz oluşu yadırgamasını ve çipsiz yeri hissetmeye çalışmasını göstermektedir. Aynı zamanda adamın kadının yara izine dokunma bahanesiyle, kadınla flört ettiğini göstermektedir.

Gösterge	**Gösteren**	**Gösterilen**
İnsan	4 kadın 4 erkek birey, arkadaşlar	İnsanların, arkadaşların birlikte samimi bir ortamda bir araya gelip beraber sohbet etmesi, kendileriyle ilgili konuları paylaşması, güzel vakit geçirmesi

Düz anlamda beraber sohbet eden yemek yiyen arkadaşları gösteren insanlar, yan anlamıyla ise arkadaşların beraberce güzel vakit geçirmesini, birbirleriyle paylaşımlarda bulunmasını göstermektedir.

Gösterge	**Gösteren**	**Gösterilen**
Nesne	Duvarda asılı 3 cam ekran	Arkadaş ortamında birinin ekranlara geçmişteki eğlenceli günlerini yansıtması,

Düz anlamıyla televizyona benzeyen cihazları gösteren ekranlar, yan anlamıyla insanların anılarını paylaşmalarını, eğlenmek için geçmiş anıların dijital bir yöntemle izlenmesini ve ekranların film dizi gibi sebeplerle değil, kolayca yansıtılması sebebiyle, geçmiş anıların izlenmesi için kullanılıyor olmasını göstermektedir.

Görsel 15: Çipin Dudak Okuma Özelliği

Kaynak: Welsh, B. (Director), **The Entire History of You**. Channel 4, 2011.

Görsel 16: Eşi Tarafından Aldatıldığını Kayıtlardan İzlemesi

Kaynak: Welsh, B. (Director), **The Entire History of You**. Channel 4, 2011.

Sahne-5: (24:04 – 24:16 dk.) Liam'ın, eşi Fi'nin Jonasla aralarındaki iletişim dikkatini çekmiş, Jonas'a olan tavırlarından şüphelenmiş, ondan bir şeyler sakladığını düşünmüştür. Bu nedenle onları konuşurken gördüğü anı tekrar incelemek için geçmiş kayıtlarını izlemek istemiştir. Onları uzaktan gördüğü bir anın kaydında, aralarında geçen konuşmaları öğrenebilmek için bellek çipi uygulamasının dudak okuma özelliğini kullanarak konuşmalarını deşifre etmiş ve aralarında onu daha da şüpheye sokacak konuşmalar duymuştur.

Gösterge	**Gösteren**	**Gösterilen**
İnsan	Koca	Bireyin, eşinin ondan bir şeyler sakladığını düşünüp şüphe duyması ve bunu araştırırken geçmiş kayıtlarını izleyerek durumu anlamaya çalışması

Düz anlamıyla geçmiş kayıtlarını izleyen bir erkeği gösterirken, yan anlamda ise eşinin ondan bir şeyler sakladığını düşünen bir kocanın şüphesinin üstüne gitmesini, eşiyle ilgili gerçekleri bellek kaydından ipuçları arayarak öğrenmeye çalışmasını göstermektedir.

Gösterge	**Gösteren**	**Gösterilen**
Dijital program	Çip uygulamasının dudak okuma özelliği	Çip uygulamasının dudak okuma özelliği sayesinde eşi tarafından aldatılma şüphesi taşıyan bireyin, eşi ve diğer bir kişi arasında geçen konuşmaları açığa çıkarması,

Düz anlamıyla bireyin çip uygulamasının dudak okuma özelliğini kullanmasını göstermektedir. Yan anlamda ise eşinden şüphelenen kocanın, eşi ve arkadaşı arasındaki konuşmaları açığa çıkarmasıyla; uygulamanın sahip olduğu dudak okuma teknolojisi sayesinde iki kişi arasındaki diyalogların deşifre edilebileceğini, dolayısıyla kişilerarası özel konuşmaların da deşifre edilerek mahremiyet ihlalinin doğabileceğini göstermektedir.

Görsel 17: Kayıtların Silinmesi İçin Şiddete Başvurulması

Kaynak: Welsh, B. (Director), **The Entire History of You**. Channel 4, 2011.

Görsel 18: Kişisel Kayıtların Zor Kullanılarak Elinden Alınması

Kaynak: Welsh, B. (Director), **The Entire History of You**. Channel 4, 2011.

Sahne-6: (34:50 – 36:02 dk.) Liam, eşinin bir zamanlar Jonasla bir şeyler yaşadığını öğrendikten sonra, Jonas'ın önceki akşam yemeğinde seviştiği kadınların kayıtlarını tekrar izlediğini anlatması

kaydını defalarca izlemiştir. Bunları düşünürken fazlaca alkol alan Liam, sarhoş bir şekilde bir sabah erkenden Jonas'ın evine gitmiş ve onunla tartışmaya başlamıştır. Kavgaya dönen tartışma sonucu bir içki şişesini kırıp Jonas'ın boğazına dayayan Liam, Jonas'ı onun kayıtlarında olan eşiyle ilgili kısımları silmesi konusunda tehdit etmiştir. Jonas bu tehdit altında, Fi'nin olduğu kayıtların tamamını ekrana yansıtarak silmiştir.

Gösterge	**Gösteren**	**Gösterilen**
İnsanlar	İki erkek arasındaki kavga	Bireyin eşinin onu aldattığını düşündüğü adamla, adamın eşine ait kayıtlarını silmesi için kavga etmesi.

Düz anlamda iki erkeğin ettiği kavga görülmekteyken, yan anlamda ise eşinin onu aldattığını düşünen kocanın, kendini kaybetmesini, eşinin onu aldattığı kişiye baskı ve zor kullanarak eşine dair kayıtları sildirtmesini ve kavga ettiği adamın kendi evinde onun kişi mahremiyetine ve kişisel bilgi mahremiyetine saldırmasını göstermektedir.

Gösterge	**Gösteren**	**Gösterilen**
Nesne	Kırık içki şişesi	Bireyin, kendi eşine ait kayıtları, eşi tarafından onunla aldatıldığını düşündüğü adamın bellek kaydından sildirmek için bir içki şişesini kırarak adamın çipini kesip alma ile tehdit etmesi.

Düz anlamda kırık içki şişesi tehdit aracı olarak görünmekteyken, yan anlamda eşinin kendisini onunla aldattığını düşünen kocanın, o adamın çipini sökme tehdidini, canına kastını, adamın kişi mahremiyetine ve kişisel veri gizliliğine tecavüzünü göstermektedir. Ayrıca insanların kişisel kayıt verilerinin zor kullanarak ellerinden alınabileceğini, şiddet ile mahremiyetlerinin ifşa edilebileceğini ve başkaları tarafından el konulabileceğini de göstermektedir.

Görsel 19: Arkadaki Tablodan Kendi Evinde Aldatıldığını Öğrenmesi

Kaynak: Welsh, B. (Director), **The Entire History of You**. Channel 4, 2011.

Görsel 20: Bellek Kayıtlarının Ekrana Yansıtılması

Kaynak: We Welsh, B. (Director), **The Entire History of You**. Channel 4, 2011.

Sahne-7: (38:34 – 39:12 dk.) Liam, Jonas'ın evine gidip ona zorla kayıtları sildirirken, gözüne Jonas'ın kayıtları arasındaki eşi Fi'nin görüntüsü takılmıştır. Görüntü, 18 ay öncesine ait kendi yatak odalarında eşinin yarı çıplak halde olduğunu göstermektedir. Liam, artık eşinin onu aldattığından emin olmuştur. Üstelik görüntüdeki tablo, kendi yatak odalarındakiyle aynı tablodur. Eşi tarafından kendi evinde aldatıldığını öğrenen Liam'ın gösterdiği görüntüleri izleyen Fi, şaşkınlık içinde kalmıştır.

Gösterge	**Gösteren**	**Gösterilen**
İnsanlar	Kadın erkek Evli eşler,	Kocanın, eşinin onu aldattığını kişisel kaydından kanıtlaması.

Düz anlamda kayıtları izleyen karı-koca gösterilmekteyken, yan anlamda teknoloji sayesinde bellek kaydı görüntülerine dayanarak, kocanın, eşi tarafından aldatıldığını kanıtlaması ve aldatılışını karısının yüzüne vurmasını göstermektedir. Karısının da bunun ortaya çıkabileceğini daha önce düşünmemiş olduğunu, ortaya çıkmasına olan şaşkınlığı ve üzüntüsünü göstermektedir.

Gösterge	**Gösteren**	**Gösterilen**
Nesne	Tablo	Kayıtlardaki tablonun kendi evlerindeki yatak odasındaki tabloyla aynı olması, Kadının eşini kendi evlerinin yatak odasında aldattığının, kocasının bellek kaydındaki görüntülerindeki tablodan ortaya çıkması.

Düz anlamda kadının yatak odasında önünde durduğu tablo ile görüntüdeki tablonun aynı oluşu gösterilirken, yan anlamı ise kayıtlardaki ve kendi yatak odalarındaki tablonun aynı oluşu sebebiyle kadının kocasını, kendi yatak odalarında aldattığını göstermektedir.

Gösterge	**Gösteren**	**Gösterilen**
Görüntü	Bellek kayıtlarının ekrana yansıtılması, kayıtlarda bireyin karısının görüntüsü	Erkeğin karısının onunla aldattığı adama bellek kaydını sildirirken, karısının görüntüsünü görmesi Kocanın eşinin onu 18 ay önce aldatmış olduğunu öğrenmesi.

Düz anlamda bellek kayıtlarında 18 ay öncesine ait kadının görüntüsü gösterilirken, yan anlamda bu görüntü, uygulamanın zaman çizelgesi sayesinde erkeğin 18 ay önce eşi tarafından Jonasla aldatıldığını göstermektedir. Kocanın kendi belleğine kaydolan Jonas'ın kişisel kayıtlarını karısına göstermesi, başkalarının kişisel kayıtlarının da görüldüğü anda bir başkasının hafızasına kaydolabilmesini, bu kişisel bilgi mahremiyetinin başkaları tarafından dağıtılabileceğini veya

başkalarına gösterebileceğini dolayısıyla mahremiyet ihlali riskini de göstermektedir.

Görsel 21: Aldatılan Kocanın Kayıtları Görmek İstemesi

Kaynak: Welsh, B. (Director), **The Entire History of You**. Channel 4, 2011.

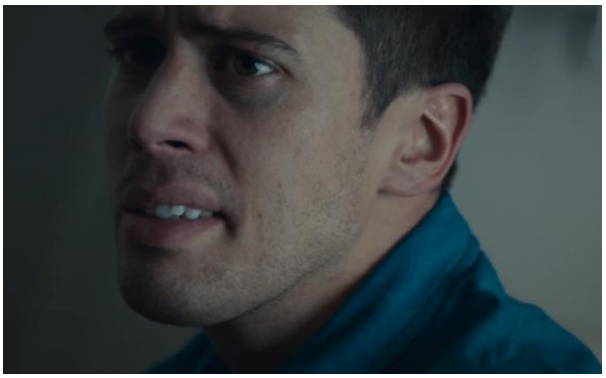
Görsel 22: Kadının Aldatma Kayıtlarına Bakamaması

Kaynak: Welsh, B. (Director), **The Entire History of You**. Channel 4, 2011.

Görsel 23: Aldatmaya Ait Bellek Kaydı Görüntüleri

Kaynak: Welsh, B. (Director), **The Entire History of You**. Channel 4, 2011.

Görsel 24: Aldatıldığını Öğrenen Kişinin Hayal Kırıklığı



Kaynak: Welsh, B. (Director), **The Entire History of You**. Channel 4, 2011.

Sahne-8: (41:33 – 43:21 dk.) Eşinin kendisini aldattığı kesinleşen Liam, bu sefer de çocuğunun kendinden olup olmadığı konusunda şüpheye düşmüş ve Fi'ye prezervatif kullanıp kullanmadığını sormuştur. Fi, kullandığını söylese de ona inanmayan Liam, zorla Fi'nin kayıtlarını açtırmıştır. Kayıtlarını açmak zorunda kalan Fi, pişmanlık ve utanç içinde kendi görüntülere bakamayarak kayıtlarını açmıştır.

Gösterge	Gösteren	Gösterilen
İnsanlar	Tartışan evli kadın erkek	Aldatıldığını öğrenen kocanın, eşinin kayıtlarını görme istemesi sebebiyle tartışan evli çift, karısının kayıtlarını göstermek istememesi ve bunu ağlayarak reddetmesi

Düz anlamda ağlayarak birbiriyle tartışan evli kadın ve erkek görülmekteyken, yan anlamda ise aldatıldığını öğrenen adamın çocuğunun kendisinden olup olmadığı hakkındaki gerçekleri güçlü bir şekilde görme öğrenme isteğini, karısının ise bunu saklama ve bundan kaçınma davranışında olduğunu göstermektedir.

Gösterge	Gösteren	Gösterilen
İnsan	Kadın (Eş)	Kocasını aldatan kadının kocasının baskısıyla kayıtlarını açmak zorunda kalması

Düz anlam olarak kadının kişisel kayıtlarını çip kumandası ile ekrana yansıtması ve bu kayıtlara bakamaması görülürken; yan anlamda ise kadının, kocasının yoğun baskısıyla altında kayıtlarını açmak zorunda kaldığını ve kocasını aldattığı kişiyle olan görüntülerini göstermek istemeyen kadının, kayıtlarını açmak zorunda kaldığında ekrana dahi bakamaması, onun utancını, çaresizliğini ve üzüntüsünü göstermektedir. Yan anlam olarak başka bir nokta ise aldatılan kocanın, o anı görebilmek için zorla eşine kişisel kayıtlarını açtırtması; dijital alanda duran ve paylaşılmak istenmeyen kişisel bir bilginin baskıyla elde edilebileceğini de göstermektedir.

Gösterge	Gösteren	Gösterilen
Görüntü	Bellek kaydı görüntüleri	Kadının kocasını aldattığı anın görüntü kayıtlarını açması, kocasını kiminle aldattığının ve onunla yaşadığı ilişkinin görünmesi

Kadının açtığı kişisel bellek kaydı görüntüleri düz anlam olarak görülmekteyken, yan anlam olarak kadının eşini aldattığı erkekle olan cinsel ilişkisinin kendi bellek kaydındaki görüntülerinin hala duruyor olması ve bunların baskı altında ortaya çıktığı görülmektedir. Dolayısıyla yalan söylenmiş olduğunu ve saklama davranışında bulunulduğunu da göstermektedir. Kadının, kocasını aldattığı kişiyle olan görüntüleri hala saklıyor olması, o ilişkiyi yaşadığı kişiden kopamayışını, belki de

istediğinde tekrar izleyebilme fırsatına sahip olma isteğini ve onunla olan paylaşımlarını anılarında tutma isteğini göstermektedir. Teknolojinin, ikili ilişkilerde hem saklamaya hem de ortaya çıkarmaya hizmet ettiği görülmektedir.

Gösterge	**Gösteren**	**Gösterilen**
İnsan	Soyunan erkek	Kadının, kocasını aldattığı kişi Kadının bellek kaydı görüntülerindeki, kocasını aldattığı kişinin cinsel ilişki yaşamadan önceki soyunma anı Cinsel ilişkinin gerçekleşeceği yer

Düz anlamda bellek kaydı görüntüsünde olan soyunan erkek, yan anlamda kadının aldatma anını ve cinsel ilişkinin başlangıç anını göstermektedir. Bu aynı zamanda, çip teknolojisinin getirdiği kişisel kayıtlardaki var olan kişilerin, belli durumlar altında başkalarına ifşa olabileceğini de göstermektedir.

Gösterge	**Gösteren**	**Gösterilen**
İnsan	Erkek (Koca)	Kocanın, eşinin kendisini aldattığını eşinin kişisel kayıtlarından görmesi, Hayal kırıklığı

Koca, düz anlamda, karısının ihanet kayıtlarını izleyen kişi olarak görülürken, yan anlamda ise teknolojiden yararlanarak gerçekleri ortaya çıkaran bireyin, artık şüphesi son bulsa da aldatılmış olduğu gerçeğiyle yüzleştiğini, bu yüzden büyük hayal kırıklığına uğradığını, üzüntü ve çaresizlik içinde olduğunu göstermektedir.

Çalışma kapsamında olan dizi bölümündeki büyük veri teknolojili ürün ve beraberinde getirdiği mahremiyet ihlali risklerinden de görüldüğü gibi, günümüzde kullanılan ve gelecekte üretilebilecek bu tarz ileri teknoloji ürünlerinin de mahremiyet ihlalleri ve dolayısıyla etik problemlere yol açabileceği düşünülmektedir. Örneğin; 2017 yılında Sypral Toys'un ürettiği, Iot teknolojisi bir ürün olan Cloudpets oyuncakları, 800 binden fazla kullanıcısının kimlik bilgilerini ve 2 milyon ses ve mesaj kaydını üçüncü kişiler ile paylaşması, dijital teknolojilerde mahremiyet ihlalini ortaya koymaktadır (Dijital Medya ve Çocuk, 2017). Diğer yandan Çin'de, suçluların yakalanmasında

kullanılan yüz tanıma gözlüğü ve yapay zekalı kameralar sayesinde Pekin yönetimi 1.4 milyarlık nüfusunun izini sürmekte, sokaklara yerleştirilmiş olan büyük ekranlarda ise bir utandırma aracı şeklinde hafif suçlar işlemiş kişilerin de fotoğrafları ve kimlik bilgileri gösterilmekte yani insanların mahremiyetini ortaya dökerken, bir anlamda da tekno-faşizm yaşatmaktadır. Özellikle Müslüman Uygur azınlığı ve aralarındaki ilişkileri geniş gözetleme teknolojileriyle izleyen Çin yönetimi, Uygur halkına cep telefonu taşımayı zorunlu hâle getirmiş, telefondaki tüm yazışmaları ve görüşmeleri kaydetmekte, güvenlik güçlerinin veri tabanına yüklemekte ve dolayısıyla birçok anlamda Uygur halkının mahremiyetini ihlal etmektedir (Beldeniz ve Büyükkaya, 2019). Bu örneklerden de anlaşılacağı üzere büyük veri teknolojili bu ürünlerin bugün dahi kişisel veri mahremiyetine saldırma riski varken, gelecekte üretilebilecek daha gelişmiş bir teknoloji tabanlı büyük veri ürünleri faydasının yanında, kişisel veriler için daha riskli ve daha zarar verici durumlara sebebiyet verme ihtimalini de taşımaktadır.

6. TARTIŞMA ve SONUÇ

Dijital çağın hızla gelişmesi ile birlikte artırılmış gerçeklik son zamanlarda oldukça ilgi çeken çalışmalar arasındadır. Teknolojik gelişmelerin gün geçtikçe hızına yetişemeyecek kadar ilerlemesi bu teknolojiye uygun cihazların gelişimini de beraberinde getirmiştir. Bu cihazlar ile internet kullanımı daha da yaygınlaşmış ve internetin kullanım şekli yön değiştirmeye başlamıştır. Önceden bilgiye kolayca erişim sağlamak için kullanılan internet zamanla üç boyutlu görüntülerin ve sanal ortamların oluşmasını sağlayan artırılmış gerçeklik sistemleri etkin bir şekilde kullanılmaya başlanmıştır. Artırılmış gerçeklik teknolojisinin sanal ortamda gerçeklik hissi sağlama ve farklı deneyim oluşturma, gibi hedefleri bulunmaktadır. Bu nedenle artırılmış gerçeklik teknolojisi eğitim, müze, sağlık, gezi, tasarım, imalat, doğal afet, sanat, reklam, eğlence, güvenlik, mühendislik ve askeri gibi birçok alanda kullanılmaktadır. Arttırılmış gerçeklik uygulamaları şu anda kullanılan birçok cihazın yerini alarak yeni bir devri başlatacağı söylenebilmektedir. Ancak diğer yandan da bugünün veya yakın geleceğin teknolojileri veri gizliliği gibi sorunsalları da içermektedir. Bu sorunsalların başında mahremiyet gelmektedir.

Çalışmada da ele alındığı gibi bu tür bilim kurgu film veya dizilerinin teknolojik anlamda geleceği yansıtabildiği düşünülmektedir. Geçmiş zamanlarda film ya da dizilerde yer alan ancak o günün şartlarında var olmayan teknolojik ürünler, zaman içinde teknolojik gelişmeler sonucu artık bir kurgu değil gerçek yaşamın bir parçası haline

gelebilmektedir. Bu çalışma kapsamındaki göstergebilimsel çözümlemesi yapılmış dizi bölümünde de benzer çıkarımların yapılabileceği düşünülmektedir. Örneğin, bu dizi bölümünde bireylerden birinin bellek çipinin zorla bedeninden sökülüp çalındığı görülmektedir. Birey kişisel bilgi mahremiyetiyle birlikte vücuduna aldığı zararla kişi mahremiyeti anlamında da saldırıya uğramıştır. Diğer yandan bellek çipindeki kayıtların zor yoluyla veya baskıyla üçüncü kişiler tarafından ele geçirilebildiği yani kişisel bilgi mahremiyeti ifşasının da yaşandığı görülmüştür. Görüldüğü gibi ileri teknoloji akıllı ürünler de web, sosyal medya gibi ortamlarda olduğu kadar kişisel veri toplamaya ve bunları işlemeye oldukça açık bir potansiyel taşımaktadır. Bu anlamda denilebilir ki; akıllı cihazlar insanlığın hayatını büyük ölçüde kolaylaştırsa da kişisel verileri içinde toplayan bu cihazlar, sadece casus yazılımlar gibi sebeplerle kişisinin kişisel verilerini ele geçirme riskini değil aynı zamanda baskı veya zorbalıkla ele geçirilebilme riskini de taşımaktadır. Sadece kişisel bilgi mahremiyetine değil, kişi mahremiyetine yönelik saldırı ihtimallerini yanında taşıyabileceği düşünülmektedir. Bu sebeple, insanlık için üretilen veya üretilebilecek günümüz ve gelecekteki teknolojik ürünler için üretim aramasından, üretim sonrası kullanım aşamasındaki süreçlere kadar kişilerin her türlü mahremiyetini korumaya veya muhtemel etik sorunları bertaraf etmeye yönelik yazılım veya uygulamalar geliştirilmesi önerilmektedir. Bu uygulamaların sadece mühendislik anlamında değil, aynı zamanda günümüz düzenlemelerinden daha ayrıntılı ve geniş çaplı hukuki düzenlemelerle desteklenmesi önerilmektedir. Hatta belki de bu konu üzerine, mühendislik ve hukuk alanlarının eş zamanlı çalışmalar yürütme olanağının yaratılabilmesi, mahremiyeti koruma çabaları anlamında fayda sağlayabileceği düşünülmektedir.

Sonuç olarak büyük veri, insan adına sağlık, pazarlama, güvenlik, ekonomi ve daha birçok alanda fayda getirdiği gibi aynı zamanda kişisel veya özel olanı ortaya döken, sivil özgürlükleri kısıtlama riskine sahip, gözetim olgusunu ve algısını arttıran birçok endişe, etik sorun ve yeniden düzenleme alanlarını da yanında getirmektedir. Bir anlamda insanlığa yüzünü gülen büyük verinin etik açıdan sorgulanmasının, yine insanı tehdide ve tehlikeye maruz bırakma ihtimaliyle arkadan iş çevirme potansiyelini öngörebilmek ve önlem alabilmek için büyük önem taşıdığı aşikardır.

KAYNAKÇA

Akıncı, A. N. (2019). Büyük veri uygulamalarında kişisel veri mahremiyeti, (Uzmanlık Tezi). 7. Retrieved from

https://www.sbb.gov.tr/wp-content/uploads/2019/04/Büyük-Veri-Uygulamalarında-Kişisel-VeriMahremiyeti.pdf, Erişim Tarihi: 01.09.2022.

Aktan, E. (2018). Büyük Veri: Uygulama Alanları. Analitiği ve Güvenlik Boyutu. *Bilgi Yönetimi Dergisi*, 1(1), 4. https://doi.org/10.33721/by.403010

Aktaş, F. Çeken, C. ve Erdemli, Y. E. (2016). Nesnelerin Interneti Teknolojisinin Biyomedikal Alanındaki Uygulamaları. *Düzce Üniversitesi Bilim ve Teknoloji Dergisi,* 4(1), 43. Retrieved from https://dergipark.org.tr/tr/pub/dubited/issue/24381/258447

Bingöl, B. (2018). Yeni Bir Yaşam Biçimi: Artırılmış Gerçeklik (AG). *Etkileşim*, (1), 44-55 . DOI: 10.32739/etkilesim.2018.1.8

Bozdoğan, Z. (2015). Nesnelerin İnterneti İçin Tasarım Mimarisi, Üniversitesi Fen Bilimleri Enstitüsü (Yüksek Lisans Tezi), Düzce.

Cackett, D. (2013). Information Management and Big Data, A Reference Architecture. White paper. Redwood Shores: Oracle Corporation, 14. Retrieved from https://www.oracle.com/technetwork/topics/entarch/articles/info-mgmt-big-data-ref-arch-1902853.pdf

Cary, NC. (2018). *SAS Survey: 67 Percent of US Consumers Think Government Should Do More to Protect Data Privacy*, Erişim adresi: https://www.sas.com/en_us/news/press-releases/2018/december/data-management-data-privacy-survey.html, Erişim Tarihi: 22.12.2021

Clement, J. (2019). *Online Privacy - Statistics & Facts*, Erişim adresi: https://www.statista.com/topics/2476/online-privacy/, Erişim Tarihi: 22.12.2021

Cloud Security Allience (2019). CSA Releases New Research, *Top Threats to Cloud Computing: Egregious Eleven*, Erişim adresi: https://cloudsecurityalliance.org/press-releases/2019/08/09/csa-releases-new-research-top-threats-to-cloud-computing-egregious-eleven/, Erişim tarihi: 19.11.2021

Çalık, D. ve Toker, G. (2016). Ekran Çağı İnsanı ve Dijital Toplum. *XXI. Yüzyılda Türkiye'de İnternet Konferansı*, 03-05.

Danah Boyd ve K. Cukier. (2012). Critical Quastions for Big Data Information, *Communication and Society,* 15(5), 662-679. http://dx.doi.org/10.1080/1369118X.2012.678878

Dave, E. (2011). The Internet of Things: How the Next Evolution of The Internet is Changing Everything. Cisco, 5.

Davis, K. (2012). *Ethics of Big Data: Balancing Risk and Innovation.* " O'Reilly Media, Inc.".

Demirtaş, B. ve Argan, M. (2015). Büyük Veri ve Pazarlamadaki Dönüşüm: Kuramsal Bir Yaklaşım. *Pazarlama ve Pazarlama Araştırmaları Dergisi,* 15, 7. Retrieved from https://dergipark.org.tr/tr/pub/ppad/issue/61006/906046

Derinözlü, C. (2017). Büyük Veri ve Mahremiyet. *1.Ulusal Bulut Bilişim ve Büyük veri Sempozyumu,19-20 Ekim*, Antalya.

Dülger, Ü. (2016). Büyük Veri Nedir?, *Yeni Türkiye Dergisi*, 22(88), 503-508.

Eroğlu, Ş. (2018). Dijital Yaşamda Mahremiyet (Gizlilik) Kavramı ve Kişisel Veriler: Hacettepe Üniversitesi Bilgi ve Belge Yönetimi Bölümü Öğrencilerinin Mahremiyet ve Kişisel Veri Algılarının Analizi, *Hacettepe Üniversitesi Edebiyat Fakültesi Dergisi,* 35, 2. https://doi.org/10.32600/huefd.439007

Ergen, Y. (2018). Büyük Veri, Sosyal Medya ve Etik: Facebook Örneğinde Bir Değerlendirme. *Ege Üniversitesi İletişim Fakültesi Yeni Düşünceler Hakemli E-Dergisi,* (10), 53-64. Retrieved from https://dergipark.org.tr/en/pub/euifydhed/issue/41830/485812

Eyüpoğlu, C. , Aydın, M. A. , Sertbaş, A. , Zaim, A. H. ve Öneş, O. (2017). Büyük Veride Kişi Mahremiyetinin Korunması. *Bilişim Teknolojileri Dergisi*, 10(2), 177-184. DOI: 10.17671/gazibtd.309301

Eyüpuğlu, C. (2018). Büyük Veride Etkin Gizlilik Koruması İçin Yazılım Tasarımı, (Doktora Tezi), İstanbul Üniversitesi Fen Bilimleri Enstitüsü, İstanbul.

Fuller, M. (2019). Big Data and The Facebook Scandal: Issues and Responses. *Theology*, 122(1), 14-21. https://doi.org/10.1177/-0040571X18805908

Fung, B. C., Wang, K., Fu, A. W. C., ve Philip, S. Y. (2010). *Introduction to Privacy-Preserving Data Publishing: Concepts and Techniques.* Chapman and Hall/CRC.

Gandomi A. ve Haider M. (2015). Beyond The Hype: Big Data Concepts, Methods and Analytics, *International Journal of Information Management*, 35(2), 139. https://doi.org/10.1016/j.ijinfomgt.2014.10.007

Gönül Y., Ulu Ş., Bucak A. ve Bilir A. (2015). Yapay Sinir Ağları ve Klinik Araştırmalarda Kullanımı. *Genel Tıp Dergisi,* 105. https://doi.org/10.15321/geneltipder.2015313147

Gözüküçük, M. (2014). Veri İşleme Süreçlerinde Tartişmali Bir Çözüm: Veri Anonimleştirmesi. (Yüksek Lisans Tezi) Bilgi Üniversitesi Sosyal Bilimler Enstitüsü. İstanbul.

Gündüz K. A. Akyüz, E. T. (2017). Nesnelerin Interneti ve Hayvancılık Alanındaki Uygulamalar, *Selçuk Üniversitesi Sosyal ve Teknik Araştırmalar Dergisi*, 14, 234.

Gündüz, M. Z. ve Daş, R. (2018). Nesnelerin Interneti: Gelişimi, Bileşenleri Ve Uygulama Alanları. *Pamukkale Üniversitesi Mühendislik Bilimleri Dergisi*, 24(2), 328. Retrieved from https://dergipark.org.tr/tr/pub/pajes/issue/36922/419740

Işıklı, Ş. (2014). Büyük Veri, Epistemoloji ve Etik Tartışmalar. *Online Academic Journal of Information Technology*, 5(17), 90-122. DOI: 10.5824/1309-1581.2014.4.006.x

İç Denetçiler Enstitüsü, (2017). Küresel Bakış Açıları ve Anlayışlar: Yapay Zekâ – İç Denetim Mesleğine İlişkin Dikkate Alınması Gerekenler, *Küresel Bakış Açıları: Yapay Zekâ I*, AI Kısım I, 5-15, Erişim adresi: https://www.tide.org.tr/file/documents/pdf/GPAI-Artificial-Intelligence-Part-I-Revised.pdf. Erişim Tarihi: 05.01.2020.

İçten T. Bal G. (2017). Artırılmış Gerçeklik Teknolojisi Üzerine Yapılan Akademik Çalışmaların İçerik Analizi, *Bilişim Teknolojileri Dergisi*, 10(4), 403. https://doi.org/10.17671/gazibtd.290253

İlkdoğan, H. (2017). Göstergenin Toplum Düzlemindeki Yeri: Toplumsal Göstergebilim. *İdil Dergisi,* 6(39), 3147-3164. DOI: 10.7816/idil-06-39-10

Kalaman, S. (2019). Yeni Medya ve Dijital Gözetim: Türkiye'deki Sosyal Medya Kullanıcıları Üzerine Bir Araştırma. *Yönetim ve Ekonomi Dergisi,* 26(2), 575-594. DOI: 10.18657/yonveek.556868

Karabey Aksakallı, I. (2019). Bulut Bilişimde Güvenlik Zafiyetleri, Tehditler ve Bu Tehditlere Yönelik Güvenlik Önerilerinin İncelenmesi, *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi*, 5(1), 8-34. https://doi.org/10.18640/ubgmd.544054

Karlıdağ, S. (2014). Yeni İletişim Teknolojileri ve Mahremiyet: E-Belediyeler Kişisel Bilgileri Koruyor Mu? *Erciyes İletişim Dergisi*, *3*(4),102-120. https://doi.org/10.17680/akademia.v3i4.5000012420

Khalil, E. A. ve Özdemir, S. (2018). Nesnelerin İnternetine Genel Bir Bakış: Kavram, Özellikler, Zorluklar ve Fırsatlar. *Pamukkale Üniversitesi Mühendislik Bilimleri Dergisi*, 24(2), 311-326. DOI: 10.5505/pajes.2017.60343

Kılıç, H. , Atalay, E. ve Yurtsever, A. E. (2019). Büyük Veri (Bıgdata) ve Müşteri İlişkileri Yönetimi (Crm) İşbirliğinin Pazarlama İletişimi Stratejilerindeki Rolü: Büyük Ölçekli Özel Bir Banka Örneği. *Stratejik ve Sosyal Araştırmalar Dergisi*, 3(2), 289-310. DOI: 10.30692/sisad.574133

Köroğlu, O. (2012). En Yaygın Iletişim Ortamında Artırılmış Gerçeklik Uygulamaları. Türkiye'de 17. Internet Konferansı. İstanbul. Retrieved from https://www.academia.edu/19633002/Augmented_reality_applications_in_the_most_common_communication_medium, Erişim Tarihi: 15.11.2019.

Kurşun, A. (2021). Büyük Veri Ve Sağlık Hizmetlerinde Büyük Veri İşleme Araçları. *Hacettepe Sağlık İdaresi Dergisi,* 24(4), 921-940. Retrieved from https://dergipark.org.tr/en/pub/hacettepesid/issue/67142/912677

Kutup, N. (2011). Nesnelerin Interneti; 4H, Her Yerden, Herkesle, Her Zaman, Her Nesne ile Bağlantı. *16. Türkiye'de İnternet Konferansı inet-tr'11.1-5.*

Manyika, J. Chui, M. Bughin J. Dobbs, R. Bisson P. ve Marrs A. (2013). Disruptive Technologies: Advances That Will Transform Life, Business, and The Global Economy. *McKinsey Global Institute,* 52.

McAfee, A. ve Brynjolfsson, E. (2012). Big Data: The Management Revolution. *Harvard Business Review*, 90(10), 60-6,5.

Narayanan, A., ve Shmatikov, V. (2008). Robust De-Anonymization of Large Datasets (How To Break Anonymity of The Netflix Prize Dataset). *2008 IEEE Symposium on Security and Privacy*, University of Texas at Austin.

OECD (2013). The Oecd Privacy Framework, *1. Oecd Guidelines Governing The Protection Of Privacy and Transborder Flows of Personal Data*, Erişim adresi: https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pd, Erişim Tarihi: 26.12.2021.

Orka, Ö. T. (2017). Bulut Bilişim Uygulamaları Ve Büyük Veri Analizinin Özellikle Müşteri İlişkileri Yönetimi Ve Pazarlama Stratejilerinin Belirlenmesindeki Etkileri, (Yüksek Lisans Tezi), TOBB Ekonomi ve Teknoloji Üniversitesi Sosyal Bilimler Enstitüsü, Ankara.

Solove, D. J. (2008). I've Got Nothing to Hide and Other Misunderstandings of Privacy. *San Diego L. Rev.*, 44, 745.

Somyürek S. (2014). Öğrenme Sürecinde Z Kuşağının Dikkatini Çekme: Artırılmış Gerçeklik, *Eğitim Teknolojisi Kuram ve Uygulama*, 4(1), 67. https://doi.org/10.17943/etku.88319

Söğüt E. ve Erdem O. A. (2017). Günümüzün Vazgeçilmez Sistemleri: Nesnelerin Haberleşmesi ve Kullanılan Teknolojiler, *AB 2017 Akademik Bilişim Konferansları*. Erişim adresi: https://docplayer.biz.tr/45117792-Gunumuzun-vazgecilmez sistemleri-nesnelerin-haberlesmesi-ve-kullanilan-teknolojiler.html, Erişim Tarihi: 09.12.2021

Spyratos, S., Vespe, M., Natale, F., Weber, I., Zagheni, E., ve Rango, M. (2018). Migration Data using Social Media. *JRC Science Hub*.

Tektaş M., Akbaş A. ve Topuz V. (2012). Yapay Zeka Tekniklerinin Trafik Kontrolünde Kullanılması Üzerine Bir İnceleme, *I. Uluslararası Trafik ve Yol Güvenliği Kongresi*, Retrieved from http://www.trafik.gov.tr/icerik/bildiriler/pdf/C4-7.pdf, Erişim Tarihi: 5.01.2021.

The Manifest (2019). "*Data Privacy Concerns: An Overview for 2019"*, Erişim adresi: https://medium.com/@the_manifest/data-privacy-concerns-an-overview-for-2019-2ccea79aa6f8, Erişim Tarihi: 22.12.2021

Öz, M. ve Kılıç, D. (2020). Kişisel Verilerin Çevrimiçi Mahremiyet İle İlişkisinin İçerik Analizi Yöntemiyle İncelenmesi . *Karamanoğlu Mehmetbey Üniversitesi Sosyal ve Ekonomik Araştırmalar Dergisi*, 22(39), 206-224. Retrieved from https://dergipark.org.tr/en/pub/kmusekad/issue/58846/792665

Özcan, A . (2021). Büyük Veri: Fırsatlar ve Tehditler. *TRT Akademi Dergisi*, 6(11), 10-31. DOI: 10.37679/trta.818569

Victor N., Lopez D. ve Abawajy J. H., (2016). Privacy Models for Big Data: A Survey, *International Journal of Big Data Intelligence*, 3(1), 61-75.

Weinberg, B. D., Milne, G. R. ve Andonova, Y. G. (2015). Internet of Things: Convenience vs. Privacy and Secrecy. *Business Horizons*, 615-624. https://doi.org/10.1016/j.bushor.2015.06.005

Welsh, B. (2011). The Entire History of You. Erişim adresi: https://www.imdb.com/title/tt2089050/

Yücel, G. & Adiloğlu, B. (2019). Dijitalleşme - Yapay Zeka ve Muhasebe Beklentiler. *Muhasebe ve Finans Tarihi Araştırmaları Dergisi*, (17), 47-60. Retrieved from https://dergipark.org.tr/en/pub/muftad/issue/46942/589319.

Yüksel, M. (2003). Mahremiyet Hakkı ve Sosyo-Tarihsel Gelişimi. *Ankara Üniversitesi SBF Dergisi*, *58*(01). https://doi.org/10.1501/SBFder_0000001619