...::KENT AKADEMİSİ | URBAN ACADEMY

Volume: 15 Issue: 3 - 2022 | Cilt: 15 Sayı 3 - 2022

ARTICLE INFO | MAKALE KÜNYESİ
Review Article | Derleme Makalesi
Submission Date | Gönderilme Tarihi: 19.07.2022
Admission Date | Kabul Tarihi: 22.09.2022

CITATION INFO | ATIF KÜNYESİ
Gülpınar Demirci, V. (2022). Dijital Reklamcılıkta Makine Öğrenmesi ve Veri Gizliliği, *Kent Akademisi Dergisi*, *15*(3):1455-1474.
https://doi.org/10.35674/kent.1145325

Dijital Reklamcılıkta Makine Öğrenmesi ve Veri Gizliliği

Machine Learning and Data Privacy in Digital Advertising

Vildan Gülpınar Demirci[1]

Öz

Dijital reklamcılık düşük reklam maliyetleri, hızlı ve etkili tüketici geri bildirimi, artan verimlilik ve ayrıntılı müşteri tabanı oluşturma avantajlarından dolayı şirketler için giderek daha önemli hale gelmektedir. Geleneksel reklamcılıkta daha çok sezgiye ve tecrübeye dayanan içerik üretme, dijital reklamcılıkta veriye dayalıdır. Böylece tüketicilerin dijital izlerine göre kişiselleştirilmiş hedef reklamlar sunulmaktadır. Hedef reklamcılık, dijital reklamcılığın odağına yerleşirken, bu alanda geliştirilen yöntemler hem şirketler hem de araştırmacılar için yeni ufuklar açmaktadır. Dijital reklamcılıkta hedefli reklamların sunulmasında teklif verme makineleri veya kişiye özel fiyat ve promosyon sunan fiyatlandırma motoru, genel olarak gelişmiş bir makine öğrenmesi algoritmasıyla gerçekleştirilmektedir. Makine öğrenmesi, şirketlere reklam üzerinde daha fazla kontrol gücü verirken, en önemli tartışma konusu ise reklamların kişiselleştirilmesi ve bunun sonucu olarak veri gizliliği ihlallerinin yaşanabilmesidir. Bu makale, makine öğrenmesi algoritmaları ile hedef reklamcılığın işletmelere sağladığı faydalar yanında, veri gizliliği endişelerine de odaklanarak konuyu bütüncül bir yaklaşımla ele almaktadır. Makalede hedef reklamcılığın getirdiği yüksek karlılığı korurken, tüketicilerin veri gizliliği endişesiyle satın alma davranışından vazgeçmelerini engelleyecek adımların neler olduğu tartışılmıştır. Sonuç olarak tüketici verilerinin dijital reklamcılıkta kullanılmasının önemi ortaya çıkmıştır. Bununla birlikte makine öğrenmesi algoritmaları ile kişiye özgü veri gizlilik ayarlarının yapılarak mahremiyetin, tüketicinin gizlilik sınırları çerçevesinde yapılandırılması gerektiği vurgulanmaktadır. Böylece şirketlerin hem kârlılığı koruması hem de veri gizliliği nedeniyle tüketici kayıplarının önüne geçmesi mümkün olacaktır.

Anahtar Kelimeler: Makine Öğrenmesi, Veri Gizliliği, Dijital Reklamcılık, Hedef Reklamcılık, Yapay Zekâ.

ABSTRACT

Digital advertising provides great advantages such as lower advertising costs, fast and reliable feedbacks from customers, increased efficiency, and the ability to create detailed databases of customers, which make it increasingly more important for companies. Production of contents is mainly based on intuition and experience in conventional advertising, while it is based on data in digital advertising. This makes it possible to offer targeted advertisements that are customized according to the digital trails of consumers. Targeted advertising has become the focus of digital advertising, and methods that have been developed in this field open new horizons both for companies and researchers. To provide targeted advertisements for digital advertising, bidding machines or pricing engines that offer customized prices and promotions are typically generated by means of a machine learning algorithm. Machine learning provides companies with more power to control advertisements; but the most important issue of debate is the customization of advertisements and therefore the possibility that data privacy is compromised. This paper discusses the issue with a holistic approach by focusing on the concerns of data privacy in addition to the benefits of targeted advertisements and machine learning algorithms for businesses. This paper also discusses the steps that would prevent consumers from not proceeding with a purchase due to concerns about data privacy, while maintaining the high level of profitability gained thanks to targeted advertisements. As a result, the importance of using consumer data in digital advertising was emphasized. However, privacy should be configured within the limits of consumer privacy by making personal data privacy settings with machine learning algorithms. Thus, it will be possible for companies both to protect their profitability and prevent consumer losses due to data privacy.

Keywords: Machine Learning, Data Privacy, Digital Advertising, Targeted Advertising, Artificial Intelligence.

[1] **Corresponded Author:** Aksaray Üniversitesi, İİBF, İktisat Bölümü, vildangulpinar@aksaray.edu.tr, http://orcid.org/0000-0002-8824-5154

GİRİŞ

Yeni dijital teknolojiler, dijital medya aracılığıyla şirketlerin tüketicilerle iletişim ve etkileşim kurma şeklini önemli ölçüde değiştirmiştir (Lee ve Cho, 2020, s.332). Dijital reklam, müşterileri yalnızca pasif alıcılar olmaktan çıkarmış, onları aynı zamanda içeriğin aktif dağıtıcıları, katkıda bulunanları ve hatta yaratıcıları konumuna getirmiştir. Diğer taraftan çevrimiçi reklam, şirketlerin reklam maliyetlerini düşürmek, verimliliği arttırmak, büyük ve ayrıntılı bir müşteri tabanı oluşturmak ve dolaylı olarak daha fazla gelir elde etmek için en önemli araçlardan biri haline gelmiştir (Shah vd., 2020, s.2). Bu nedenle dijital reklamcılık alanında geliştirilen yeni teknikler, şirketlerin ve araştırmacıların giderek daha fazla ilgi gösterdiği alanlar olmuştur.

Dijital reklamcılıkla ilgili temel eğilimler; veriye dayalı pazarlama iletişimine geçiş, yapay zekâ ve yapay zekanın alt bir alanı olan makine öğrenmesinin reklam üretimi üzerindeki etkisine odaklanmaktadır. Bu eğilimlerin özellikle gelecekte dijital reklamcılığın yönetiminde ve tüketicilere hedefli reklamlar sunmada önemli birer araç olacağı öngörülmektedir (Lee ve Cho, 2020, s.332).

Çevrimiçi bir ortamda kullanıcılar, daha önce ilgilendikleri bir ürün veya hizmetin reklamı ile sıklıkla karşılaşırlar. Kullanıcıların arka planını göremedikleri bu sürecin çoğu otomatik sistemler tarafından yönlendirilir. Arama sonuçları, reklam verenlerin teklif verme makineleri kullanılarak, otomatik olarak oluşturulan tekliflerle gelişmiş bir Google sıralama sistemi tarafından oluşturulur. Web sitesi geçişi yoluyla, web sitelerindeki içerik kullanıcı profiline göre özelleştirilir. Burada kullanıcı soruları aslında sohbet robotları (chat-bots) tarafından yanıtlanır. Benzer şekilde, kullanıcıların okuduğu incelemeler bir değerlendirme algoritması tarafından faydalı olduğu düşünüldüğü için öne çıkarlar ve tekrar tekrar gördüğü reklamlar, yeniden hedefleme algoritmaları aracılığıyla teklif olarak yayınlanır. Bu şekilde kişiselleştirilmiş fiyat sunan promosyon kuponu, firmanın fiyatlandırma motoru tarafından sunulur. Son olarak, sosyal medyadaki gönderiler sosyal dinleme motorları tarafından toplanır ve duyarlılık ve geri bildirim için analiz edilir. Bunlar genellikle son teknoloji makine öğrenmesi algoritmaları kullanılarak gerçekleştirilebilen eylemlerdir (Ma ve Sun, 2020, s.482).

Makine öğrenmesi, insanların karar verme sistemlerini taklit ederek geliştirilmiş, geçmiş veriler yardımıyla örneklerden ve gözlemlerden anlamlı ilişkileri ve örüntüleri otomatik olarak öğrenmeye çalışan bir tekniktir. Makine öğrenmesine dayalı teknikler temelde örüntü tanıma, sınıflandırma, kümeleme ve tahmin yaklaşımlarını içermektedir. Bu teknikler pazarlama, mühendislik, finans ve tıbbi uygulamalar gibi çok çeşitli alanlarda başarıyla uygulanmaktadır. Shah vd. (2020), reklamcılıkta yapay zekâ ve makine öğrenmesi tekniklerini kullanan Facebook, Twitter ve YouTube gibi belirli platformlara yatırım yapan Starbucks, Dell, Ikea, Dove, BMW gibi farklı sektörlerdeki şirketlerin potansiyel müşteriler kazanmada önemli bir büyüme sağladığını kanıtlamışlardır (s.12). Örneğin, Apple, Facebook'ta web sitelerini ve markalarını pazarlamak ve tanıtmak için Tıklama Başına Ödeme (PPC) yöntemini kullandığı kampanyada, 1000'den fazla Facebook kullanıcısını bir araya getiren çevrimiçi Facebook promosyonunu geliştirmiş ve müşterilerden büyük ilgi görmüştür. Benzer şekilde VirWoX Pazarlama için sosyal ağ tabanlı kampanya için Facebook'u kullanarak, bazı kampanyalarda 730'dan fazla beğeni ve reklam oluşturmuştur. Literatürde şirketlerin dijital veri akışını değerli tüketici iç görülerine dönüştürmek için dijital reklamcılıkta makine öğrenmesi algoritmalarının nasıl kullanılacağı sıklıkla araştırılmıştır (Shah vd., 2020; Perlich vd., 2014).

Yapay zekâ teknolojileri, özellikle dijital reklamların optimizasyonu konusunda, çevrimiçi reklamcılık için geleneksel uygulamalara göre rekabet avantajı sağlar. Makine öğrenmesi algoritmaları, kullanıcı verilerine dayalı olarak kullanıcılar için en ilgili reklamları tahmin eder ve böylece hedeflemenin doğruluğunu artırır. Makine öğrenmesi ve veri odaklı yaklaşımlardaki bu tür yenilikler, kullanıcı deneyimini önemli ölçüde geliştirirken, reklam verenlerin karşılaştığı zorlukların azaltılmasına yardımcı olur (Choi ve Lim, 2020, s. 176). Makine öğrenmesinin sağladığı avantajlara rağmen Facebook'un adının karıştığı Cambridge-Analytica skandalında olduğu gibi dijital reklamcılıkta veri gizliliği ihlalinin yaşanmasına sebep olabilmektedir. Reklamcılığın bu yeni uygulamalarındaki ciddi zorluk, kullanıcıların hedef reklamcılıkta gizlilik haklarının korunduğuna emin olma beklentileridir. Bu nedenle bu alanda

çıkarılacak yasalar, bu yasaların uygulanması ve makine öğrenmesi teknolojilerinin doğru kullanımı oldukça etkili olmaktadır (Shah vd., 2020, s.2).

Bu noktadan hareketle bu makalede; dijital reklamcılıkta makine öğrenmesi algoritmalarının kullanımıyla derin müşteri iç görülerinin elde edilmesi ve hedefli reklamların sunulmasının avantajlarının yanı sıra en önemli dezavantajlarından biri olan veri gizliliği ihlalleri ele alınmıştır. Daha sonra dijital reklamcılıkta veri gizliliği ihlallerinin nasıl çözümlenebileceğine yönelik güncel teknikler tartışılmıştır.

1. Makine Öğrenmesi

Sharma vd. (2019) e-posta, sosyal medya, web siteleri, arama motorları, mobil uygulamalar, web siteleri ve bağlı kuruluş programları aracılığıyla iletilen promosyon reklamlarını ve mesajlarını içeren dijital reklamcılığı, bir ürünün veya markanın dijital ortam aracılığıyla reklamını yapma süreci olarak tanımlamaktadır. Pazarlamada geleneksel olarak kullanılan istatistiksel modellerin aksine makine öğrenmesi yöntemleri, büyük ölçekli ve yapılandırılmamış (ham) verilerden öğrenebilen ve geleceğe yönelik tahmin yapabilen esnek yapılara sahiptir (Ma ve Sun, 2020, s.482). Makine öğrenmesi, çeşitli görevleri ele almak için çok sayıda yöntemi kapsayan geniş ve hızla gelişen bir alandır.

Şekil 1'de gösterildiği gibi, Ma ve Sun (2020) pazarlama literatüründe kullanılan temel makine öğrenmesi görev ve yöntemlerini özetlemişlerdir. Burada görev ve yöntemler kısaca açıklanmıştır.

Makine Öğrenmesi		
Denetimli öğrenme	**Denetimsiz Öğrenme**	**Takviyeli Öğrenme**
Klasik teknikler	**Klasik teknikler**	• Çok kollu haydut (Multi-armed bandit)
• K- en yakın komşu	• Kümeleme	• Dinamik programlama
• Destek vektör makineleri	• K-ortalamalar	• Q öğrenme
• Naive Bayes	• Hiyerarşik	• Derin Q Ağları
• Karar Ağaçları	• DBSCAN	
• Yapay Sinir Ağları		
Son gelişmeler	**Son gelişmeler**	
• Topluluk yönetimi	• Konu modelleme	
• Rastgele orman	• Temsili öğrenme	
• Gradyan destekli ağaçlar	• Otokodlayıcı	
• XGBoost	• Kelime yerleştirme	
• Olasılıksal grafiksel modeller	• Ağ yerleştirme	
• Derin Sinir Ağları		
• Evrişimli sinir ağları		
• Tekrarlayan sinir ağları		

Şekil 1. Makine Öğrenmesi Görev ve Teknikleri (Ma ve Sun, 2020).

1.1. Denetimli Öğrenme

Denetimli öğrenmede her örnek için hem girdi (X) olarak belirtilen bir değişkenler kümesi ve bir hedef değişken olan çıktı (Y) gözlemlenecek şekilde bir eğitim veri kümesi sağlanır. Denetimli öğrenme, bir girdi verildiğinde çıktıyı tahmin etmek için bu eğitim veri kümesinden Y = f (X) bir fonksiyon öğrenmeyi amaçlar. Öğrenme performansını ölçmek için veri kümesi eğitim ve test seti olmak üzere bölünür. Eğitim seti ile değişkenler arası örüntüler ortaya çıkarılırken, test seti ile bu ilişkinin doğrulanması

hedeflenir. Ayrıca, eğitim ve doğrulama için eğitim veri setinin farklı bölümleri yinelemeli olarak kullanılarak, çapraz doğrulama gerçekleştirilir (Ma ve Sun, 2020, s.484). Klasik denetimli öğrenme algoritmaları aşağıda açıklanmıştır.

K-en yakın komşu (kNN) algoritması, örnek veri noktasının ait olduğu sınıfı, veri noktasına en yakın k adet komşunun sınıfına göre karar veren bir sınıflama tekniğidir. KNN algoritması örnek tabanlı öğrenme algoritmalarından biridir ve yeni bir örnek, eğitim setinde yer alan örneklerle arasındaki benzerliğe göre sınıflandırılır (Mitchell, 1997, ss.231-232).

Destek vektör makineleri, istatistiksel öğrenme teorisine dayalı olarak çalışmaktadır. Temelde iki sınıfı birbirinden en uygun şekilde ayırabilen n boyutlu bir hiper-düzlem oluşturulması esasına dayanmaktadır (Vapnik, 1995, s.133). Doğrusal hiper-düzlemler yetersiz olduğunda, orijinal girdi alanını daha yüksek boyutlu uzaylara eşleyerek, doğrusal olmayan sınıflandırma sınırları oluşturabilir (Ma ve Sun, 2020, s.485; Hsu ve Lin, 2002, s.424).

Naive Bayes, Bayes teoremini esas alan bir sınıflandırma tekniğidir. Sonsal olasılığı maksimize eden sınıfı seçen Bayes sınıflandırıcısı teorik olarak güçlü olmasına rağmen yüksek boyutlu girdi vektörleri için ampirik olarak mümkün değildir. Naive Bayes sınıflandırıcısı, bir tahmin edicinin (x) değerinin belirli bir sınıf (c) üzerindeki etkisinin diğer tahmin edicilerin değerlerinden bağımsız olduğunu varsayar. Bu varsayıma sınıf koşullu bağımsızlık denir. Bu varsayıma rağmen, NB güçlü bir sınıflandırıcıdır ve özellikle metin madenciliğinde yaygın olarak kullanılmaktadır (Ma ve Sun, 2020, s.485).

Karar Ağaçları, hem sınıflandırma hem de tahmin problemlerinde başarıyla uygulanan bir tekniktir. Karar ağaçlarında, değerlerin değişkenler arasında görülme sıklığına ve dağılımlarına bakarak, bir karar modeli oluşturulur. Ağaçtaki her bir düğüm bir soruya karşılık gelir ve soruya verilen her olası cevap, her seviyedeki yapraklar ile temsil edilir. Kökten yaprağa uzanan her bir yol, bir karar kuralını temsil eder. Bu karar kuralları takip edilerek, sınıflandırma gerçekleştirilir (Gülpınar Demirci ve Kaplan, 2020, s.259).

Yapay Sinir Ağları, büyük veri yığınları arasında gömülü ilişkilerin, yapıların ve örüntülerin ortaya çıkarılması amacıyla, herhangi bir matematiksel modele uymayan, gürültülü, eksik verilerin sınıflandırılmasında ve tahmininde de başarıyla uygulanan bir makine öğrenmesi yöntemidir (Gülpınar Demirci ve Altaş, 2020, s.167).

Rastgele Orman, eğitim veri kümesinden Boostrap tekniği ile örnekler seçilerek sınıflandırma ve regresyon ağaçları oluşturan bir tekniktir (Breiman, 2001, s.11; Onan vd., 2016, s.237). Algoritmada, sınıflandırıcının genelleme hatası, tek tek ağaçların gücüne ve ağaçlar arasındaki ilişkiye bağlıdır. Ağaç tümevarım sürecinde, modelin gürültülü veya alakasız verilerle başa çıkma yeteneğini artıran rastgele bir özellik seçimi kullanılır (Onan vd., 2016, s.237). Her bir ağaç için tespit edilen sınıflandırmalar arasında en çok tekrar edilen sınıf değeri seçilir.

1.2. Denetimsiz Öğrenme

Denetimsiz öğrenmede, eğitim veri kümesi yalnızca girdi değişkenlerini içerirken çıktı değişkenleri bilinmemektedir. Temel amaç, verilerdeki gizli kalıpları bulmak veya verilerden bilgi çıkarmaktır. Çıkarılan öznitelikler, orijinal verilerin anahtar bilgilerini taşır ve sonraki analizler için girdi olarak yorumlanabilir veya kullanılabilir. Çok sayıda denetimsiz öğrenme algoritmaları bulunmaktadır. Kümeleme analizinde, grup içi benzerliği ve gruplar arası farkı en üst düzeye çıkarmak için girdi örnekleri birden çok gruba ayrılır. Boyut azaltma görevinde, yüksek boyutlu veriler, orijinal verilerdeki bilgiler korunurken daha düşük boyutlu değişkenlere dönüştürülür. Görev, özellikler onları temsil etmek için giriş verilerinden çıkarılır (Ma ve Sun, 2020, s.484).

K-ortalamalar algoritmasında, veri kümesi, giriş parametresi olarak verilen k adet kümeye, küme içindeki nesnelerin birbirlerine maksimum düzeyde benzemesi, diğer kümelerdeki nesnelerden ise maksimum düzeyde farklılaşması sağlanarak bölümlenmektedir. K-ortalamalar algoritması rastgele

seçilen k adet merkez noktayla başlar. Veri kümesindeki her nokta uzaklık ölçüleri dikkate alınarak, kendisine en yakın merkez noktanın kümesine atanır. Küme merkezinin değeri kendine ait noktaların ortalaması alınarak hesaplanır. Merkezlerin değerleri değişmeyinceye kadar işlem devam eder (Gülpınar Demirci ve Kaplan, 2020, s.272). K-ortalamalar algoritması, bir ortalama uç değerlerden kolayca etkilendiği için aykırı değerlere duyarlıdır.

Hiyerarşik kümeleme yöntemleri, genellikle dendogram adı verilen bir ağaç yapısı aracılığıyla grafiksel olarak temsil edilen bir kümeler hiyerarşisi oluşturmaya dayanır. Bu hiyerarşi, artan benzerlik kümelerinin daha büyük olanları oluşturmak için birleştirilmesinden veya daha büyük kümelerin azalan farklılıklardan daha küçük olanlara bölünmesinden kaynaklanmaktadır (Marini ve Amigo, 2020, s.101). Bu nedenle hiyerarşik ayrışmanın nasıl oluştuğuna bağlı olarak birleştirici (agglomerative) ya da bölücü (divisive) olarak sınıflandırılabilir. Birleştirici hiyerarşik kümeleme, aşağıdan yukarıya (parçadan bütüne), bölücü hiyerarşik kümeleme ise yukarıdan aşağıya (bütünden parçaya) oluşturulur (Gülpınar Demirci ve Kaplan, 2020, s.272).

DBSCAN (Density-Based Spatial Clustering of Applications with Noise) ilk yoğunluk tabanlı kümeleme algoritmasıdır. Gürültü ve aykırı değerler içeren veri tabanlarında herhangi bir keyfi şekil ve boyuttaki kümeleri keşfedebilir (Khan vd., 2014, s.232).

Konu modelleme, makine öğrenmesinin yanı sıra doğal dil işleme ve bilgi çıkarımı süreçlerinde de yaygın şekilde kullanılan bir denetimsiz bir makine öğrenmesi tekniğidir. Bu teknikte amaç geniş ölçekli doküman koleksiyonlarından anlamsal bilgiye ulaşmaktır. Farklı konu modelleme algoritmaları bulunmaktadır (Ekinci vd., 2020, s.68).

Denetimli ve denetimsiz öğrenme arasında, çıktının verilerin yalnızca bir alt kümesi için bilindiği yarı denetimli öğrenme ve eldeki görev için farklı bir veri kümesinin kullanıldığı veya farklı bir amaç için eğitilmiş mevcut bir modelden yararlanıldığı transfer öğrenme modelleri yer almaktadır (Ma ve Sun, 2020, s.484; Pan ve Yang, 2009, s.1345).

1.3. Takviyeli Öğrenme

Takviyeli öğrenmede öğrenme aracısı, belirli bir amaç fonksiyonunu optimize etmek için eylemlerde bulunarak ve geri bildirimleri gözlemleyerek çevre ile sürekli olarak etkileşime girer (Sutton ve Barto, 2018, s.471). Bu görevler genellikle dinamik programlama modelleri kullanarak ileriye dönük davranışları araştıran pazarlama araştırmacılarının aşina olduğu bir yapı olan Markov karar süreci (MDP) olarak formüle edilir. Öğrenme algoritmasının hem ortamın özelliklerini öğrenmek hem de verilen durumlar için en uygun eylem politikasını oluşturmak için yapılacak eylemleri belirlemesi gerekir. Bu tür makine öğrenmesi görevleri, son metodolojik ilerlemeler ve otonom araçlardan geçiş yapan web sitelerine kadar sektördeki artan kullanımlar nedeniyle daha fazla ilgi görmüştür (Ma ve Sun, 2020, s.485).

Çok kollu haydut problemleri, vaka dağılımları ve trafik durumu gibi özellikleri tam olarak bilinmeyen ancak olasılıksal ifade edilebilen parametrelerin olduğu durumlarda, keşif ve istifade mekanizması ile öğrenme yapılmasını inceler (Şahin ve Yücesoy, 2019, s.1). Bir kumarbaz için çok kollu haydut sorunu, bir dizi denemede toplam ödülünü en üst düzeye çıkarmak için bir K-slot makinesinin hangi kolunu çekeceğine karar vermektir. Birçok gerçek dünya öğrenme ve optimizasyon problemi bu şekilde modellenebilir. Tüm bu durumlarda ortaya çıkan sorular, halihazırda edinilmiş bilgilere dayalı olarak ödül maksimizasyonunun dengelenmesi ve pekiştirmeli öğrenmede sömürüye karşı keşif değiş tokuşu olarak bilinen bilgiyi daha da artırmak için yeni eylemlere girişilmesi sorunuyla ilgilidir. Bu sorunun çözümünde Ɛ- Greedy stratejisi, soft-max stratejisi ve aralık tahmin stratejisi sıklıkla kullanılan çözüm yöntemleridir (Vermorel ve Mohri, 2005, s.437).

Dinamik programlama, çok sayıda karar değişkenin olduğu karmaşık problemleri, daha basit alt problemlere bölen bir optimizasyon yaklaşımıdır. Alt problemlerin her biri çözülür ve çözümler bellek tabanlı bir veri yapısı kullanılarak depolanır. Alt problemlerin çözümleri birleştirilerek, problemin

çözümünde aşağıdan yukarıya bir çözüm tekniği kullanılmış olur. Aynı alt problemin yeniden ortaya çıkması durumunda eski çözümler veri tabanından çağırılır ve kullanılır (Alzubi vd., 2020, s.16095).

Q Öğrenme, modelsiz takviyeli öğrenmenin bir şeklidir. Aynı zamanda bir asenkron dinamik programlama yöntemi olarak da görülebilir. Ajanlara, etki alanlarının haritalarını oluşturmalarını gerektirmeden eylemlerin sonuçlarını deneyimleyerek Markovian etki alanlarında en uygun şekilde hareket etmeyi öğrenme yeteneği sağlar. Öğrenme, zamansal farklılıklar yöntemine benzer şekilde ilerler. Bir ajan, belirli bir durumda bir eylemi dener ve sonuçlarını, aldığı ödül veya cezaya dayalı olarak tahmini açısından değerlendirir. Tüm durumlardaki tüm eylemleri tekrar tekrar deneyerek, hangilerinin genel olarak en iyi olduğunu öğrenir ve buna göre hareket eder (Watkins ve Dayan, 1992, ss.272- 292).

Derin Q ağları, genellikle Q-öğrenme ile aynı süreci izleyen, durumları ve eylemleri değerlere eşlemek için derin sinir ağlarını kullanan bir tekniktir. Takviyeli öğrenmede oldukça karmaşık olan durum uzayını ele almak için derin sinir ağları pekiştirmeli öğrenmeye dahil edilerek derin pekiştirmeli öğrenme yöntemleri kullanılmaktadır. Derin Q ağları bunların en iyi örneklerinden biridir. Çalışmalar, bu tür yöntemlerle eğitilen ajanların çok çeşitli oyunlarda insan seviyesindeki yetenekleri aşabileceğini göstermiştir (Ma ve Sun, 2020, s.487).

2. Makine Öğrenmesinin Dijital Reklamcılıkta Kullanımı

Makine öğrenmesi teknikleri dijital reklamcılıkta farklı alanlarda kullanılmıştır. Bu çalışmalardan bazıları aşağıda sıralanmıştır.

Wen vd. (2022), duygusal uyumun YouTube'daki müzik videolarının reklam yerleşimi üzerindeki etkilerini inleyerek, reklamın inandırıcılığını arttıran en belirleyici özellikleri incelemişlerdir. Analizler karar ağacı algoritmalarından CART (Classification and Regression Trees- Sınıflandırma ve Regresyon Ağaçları) algoritması kullanılarak gerçekleştirilmiştir. Buna göre algılanan ikna ediciliği tahmin etmek için algılanan reklam değeri, reklamın eğlenceli olarak algılanma düzeyi, reklamın bilgilendirici olarak algılanma düzeyi, reklam iritasyonu ve mesaj katılımı özellikleri kullanılmıştır. Elde edilen karar ağacının kök düğümü algılanan reklam değeri özelliğidir ve bu algılanan reklam değerinin, video reklamcılığının algılanan ikna ediciliğini etkileyen en önemli faktör olduğunu göstermektedir. Diğer bir deyişle, tüketicilerin ikna edilme olasılığı, reklamda ne kadar değer algıladıklarına bağlıdır. Çalışmada önemli karar kuralları elde edilmiştir. Örneğin bir karar kuralına göre algılanan reklam değeri 3,83'ten büyük ise ve reklamın bilgilendirici olarak algılanma düzeyi 5,5'ten büyük ise ve mesaj etkileşimi 5,25'ten büyük ise algılanan ikna edicilik en yüksek değeri almaktadır. Bu şekilde elde edilen karar kuralları ile reklamın inandırıcılığını etkileyen faktörler ortaya çıkarılmıştır. Çalışmada karar ağacı modelinden elde edilen tahmine dayalı sonuçlar, video paylaşım web sitelerinin reklam tasarımı ve değerlendirmesini sağlamak için önemli bilgiler sunmaktadır.

Sharma vd. (2019), çeşitli makine öğrenmesi tekniklerini kullanarak hedef kitleye ulaşma ve maliyet problemini optimize etme zorluğunu çözmek için hibrit bir sistem sunmuştur. Çalışmada belirli reklamları belirli bir grup insan veya hedef kitleye göstererek yayıncıya olduğu kadar izleyiciye de fayda sağlamak amaçlamıştır. Böylece izleyicinin reklamda gösterilen belirli ürünü satın alma şansını arttırmak hedeflenmiştir. Her bir reklam için veri toplanmış, tıklama oranı tahmin edilmiş ve yüksek tıklanma oranına sahip en iyi reklamlar seçilmiştir. Kullanıcıları farklı kategorilerde sınıflandırmak için popülasyon sınıflandırması yapılmıştır. Yeni bir kullanıcı yayıncının sitesini ziyaret ettiğinde, bir kullanıcı profili oluşturulur ve eğitilmiş makine öğrenmesi modeline dayalı olarak yeni kullanıcı sınıfı tahmin edilmiştir. Sonuçta geliştirilen sistemle, yüksek tıklanma oranlarından oluşan reklamların en uygun kitle grubuna gösterilmesi ve son kullanıcıların en alakalı ürünleri en az çabayla edinmesi sağlanmıştır. Görüntülü reklamlar için tıklanma oranı tahmin modellemesi yapan farklı bir çalışmada, çeşitli makine öğrenmesi regresyon teknikleri kullanılmıştır. Araştırma sonucunda destek vektör regresyonunun tıklanma oranlarını tahmin etmede diğer algoritmalardan daha başarılı sonuçlar verdiği görülmüştür (Avila ve Vijaya, 2016). Chapelle vd. (2014) de görüntülü reklamcılıkta tıklanma oranları tahmini için

lojistik regresyona dayalı bir makine öğrenmesi algoritması kullanmışlardır. Geliştirilen modelin, basit, ölçeklenebilir ve verimliliği yüksek olduğu sonucuna ulaşılmıştır.

Kuppusamy (2018) reklam bloklarını reklam dışı bloklardan ayırt edebilen çeşitli bir özellik kümesi kullanan makine öğrenmesi tabanlı bir reklam algılama sistemi tasarlamıştır. Yöntem, görme, bilişsel bozukluklar ve ışığa duyarlı epilepsi hastalarında sorunsuz tarama ve metin özetleme gibi erişilebilirlikle ilgili çeşitli özellikleri sağlamak için temel bir görev üstlenebilir. Önerilen özellik seti üzerinde eğitilmiş bir sınıflandırıcıdan elde edilen sonuçlar, reklamları tanımlamada yüzde 98.6 doğruluk elde etmektedir. Çalışmada rassal orman sınıflandırıcısı kullanılmıştır.

Ren vd. (2017), gerçek zamanlı teklif (GZT) ile reklam verenin kârını maksimize etmeyi amaçlayan bir teklif verme makine öğrenme algoritması önermiştir. GZT'ye dayalı görüntülü reklamcılığı, reklam verenlerin bir açık artırma yoluyla gerçek zamanlı olarak bireysel reklam gösterimleri satın almalarını sağlayan ve birden çok reklam veren arasında bireysel gösterimlerin değerlendirilmesini ve teklif verilmesini kolaylaştıran bir teknik olarak tanımlanmıştır. Çalışmada RTB'de reklamcıların, teklif stratejilerini optimize ederken tıklamalar gibi reklam gösteriminin faydasını tahmin etme, verilen reklamın piyasa değerini tahmin etme ve ilk ikisine dayalı olarak en uygun teklife karar verilmesi konusunda zorluklarla karşılaşıldığı ileri sürülmüştür. Çalışmada, tüm zorlukları birlikte çözen Teklif Makinesi (Bidding Machine) tekniği önerilmiştir. Sonuçta bu teknikle reklam kampanyalarının etkinliğinin ve karın büyük ölçüde arttırıldığı gösterilmiştir.

Perlich vd. (2014) hedeflenen görüntülü reklamcılık için çok aşamalı transfer öğrenme sisteminin tasarımını sundukları çalışmada, çeşitli transfer aşamalarının deneysel bir değerlendirmesini yapmışlardır. Buna göre reklamı gördükten sonra belirli bir ürünü ilk kez satın alma olasılığı en yüksek olan potansiyel çevrimiçi müşteriler belirlenerek, sayısız çeşitli eşzamanlı görüntülü reklam hedefleme kampanyası için otomatik olarak tahmine dayalı modeller oluşturulmuştur. Makalede, hedeflenen görüntülü reklamcılık için büyük ölçekli, gerçek dünya verilerini, makine öğrenmesi sistemiyle birleştirilen ayrıntılı problem formülasyonu sunulmuştur. Sistem, farklı "kaynak" örnekleme dağılımlarına ve eğitim etiketlerine sahip modelleri öğrenir ve ardından bu bilgiyi hedef göreve aktarır. Deneysel sonuçlar, eğitim için önyargılı proxy popülasyonlarının bilinçli kullanımının, verilerin yetersiz olduğu durumlarda model performansını iyileştirebileceğini göstermektedir. Diğer taraftan Makine öğrenmesi uygulamaları oluştururken hedef dağıtım dışındaki dağılımlardan veri çekmenin yanı sıra hedef etiketten farklı etiketler kullanmanın da performansı artırabileceği görülmüştür.

Shanahan ve Kurra (2011) istatistiksel makine öğrenmesi ve bilgi bilimi perspektiflerinden çevrimiçi reklamcılık alanını dönüştüren teknolojileri ve iş modellerini incelemişlerdir. Bu tekniklerden biri olan "davranışsal hedefleme" kullanıcının göz atma davranışına dayalı olarak reklamları hedefleyen bir yaklaşım sunar. Çalışmada makine öğrenmesi ve bilgi bilimi bakış açısının yardımıyla dijital reklamcılık alanının araştırma ve geliştirme açısından dinamik bir yapıya sahip olduğu ve kullanıcıların kişiselleştirme yoluyla reklam deneyimini optimize etmenin daha iyi yollarına ihtiyaç duyulduğu vurgulanmıştır.

3. Veri Gizliliği

Dijital formattaki kişisel bilgiler kolayca kopyalanabilir, iletilebilir ve entegre edilebilir hale gelmiş, bu da çevrimiçi pazarlamacıların bireylerin kapsamlı tanımlarını oluşturmalarına olanak sağlamıştır (Malhotra vd., 2004, s.338). Böylelikle dijital ortamlardan elde edilen büyük veriler, kullanıcıların görüşleri ve davranış örüntüleri hakkında paydaşlara çok yönlü içgörüler elde etmek için benzersiz fırsatlar sunmaktadır. Buna rağmen, dijital ortamlardan elde edilen büyük veriler, sunduğu fırsatların yanı sıra birtakım riskler de içermektedir (Wieringa vd., 2021, s.1). İnternetin küresel ve açık doğası, kişisel bilgilerin birden fazla tarafça kolayca toplanmasına, saklanmasına, işlenmesine ve kullanılmasına izin vermekte, böylece bilgi gizliliği endişelerini bilgi çağı için önemli bir sorun haline getirmektedir (Smith vd., 2011, s.990).

Veri ve bilgi kavramları literatürde sıklıkla birbirlerinin yerine kullanılmalarına rağmen, aralarında önemli farklılıklar mevcuttur. Veri (data), bilginin (information) ham maddesidir. Bilgi ise bilişin (knowledge) ham maddesidir (Zins, 2007, s. 479). Diğer bir deyişle bilgi, verinin işlenmiş halidir. Biliş ise bilginin deneyime dönüşmüş halidir. Genel olarak veri gizliliği, bireylerin kişisel bilgilerinin mahremiyetini ifade etmek için kullanılır. Literatürde veri gizliliği ile ilgili farklı tanımlar yer almaktadır. Westin (1967), gizliliği "bireyin kendisi hakkındaki hangi bilgilerin, kimlere ve hangi koşullar altında iletileceğine karar verme hakkı" olarak tanımlamıştır (s.7). Bu tanım şu varsayımlara dayanmaktadır (Wu vd., 2019, s.1):

- Bireylerin kendileri hakkındaki bilgiler, bireyler tarafından bilinmektedir ve şeffaftır.
- Bireylerin bilgilerinin başkalarına iletimi, bilgi yolculuğunun sonudur.
- Bireyler koşulları değerlendirmede yeteneklidir ve mahremiyet hakları konusunda rasyonel kararlar vermektedir.

Bu varsayımlar, dijital çağda özellikle sosyal ağlardaki veri gizliliği açısından tartışmalıdır (Wu vd., 2019, s.1). Özellikle sosyal ağ gibi ortamlarda bilgiler, farklı kişilerle paylaşılabildiği için bireylerin kendileri hakkındaki bilgilerin akış sürecini takip etmeleri oldukça zorlaşmıştır. Dolayısıyla bu sürecin şeffaf olduğunu iddia etmek de zordur. Benzer şekilde "mahremiyet paradoksu" tartışmaları ile sıklıkla gündemde tutulduğu gibi bireylerin ticari çıkarları söz konusu olduğunda mahremiyet hakları konusunda rasyonel davranıp davranmadıkları da tartışmalıdır.

Clarke (1999) "gizliliğin genellikle ahlaki bir hak veya yasal bir hak olarak düşünüldüğünü" belirtirken, gizliliğin dört boyutundan bahsetmiştir (s.60). Bunlar; bir kişinin (vücut bütünlüğü) mahremiyeti, kişisel davranış gizliliği, kişisel iletişim gizliliği ve kişisel veri gizliliğidir. Diğer taraftan gizlilik "kişinin, kişisel bilgilerini ikincil kullanımlara karşı kontrol etme yeteneği" olarak da tanımlanmıştır (Bélanger vd., 2002, s.249). İkincil kullanım, verilerin toplanma amacının dışında farklı amaçlarla kullanılmasını ifade etmektedir.

Bélanger ve Crossler (2011), kişisel iletişim ve veri gizliliğinin, bilgi ve iletişimin sayısallaştırılması göz önüne alındığında bilgi gizliliği yapısıyla birleştirilebileceğini ve böylece daha geniş gizlilik literatürünün bilgi gizliliği kavramına odaklanabileceğini savunmaktadır (s.1018). Bu düşüncenin temelinde teknolojinin bilgi gizliliğiyle ilgili birçok endişeyi tetiklemesi fikri yer almaktadır. Bu noktadan hareketle literatürdeki bilgi gizliliği tanımlarının ortak noktaları dikkate alındığında bilgi gizliliği, "bireylerin kendileriyle ilgili verileri kontrol etme veya en azından önemli bir etkiye sahip olma arzusu" olarak ifade edilmektedir (Bélanger ve Crossler, 2011, s.1017). Veri gizliliği, veri sorumluları tarafından toplanan verilerin hukuka ve etik kurallara uygun olarak işlenmesiyle veri öznelerinin korunmasıdır (Vural, 2018, s.22). Veri gizliliği bireylerin; kişisel bilgilerini ne zaman, nerede, nasıl, kiminle ve ne ölçüde paylaşacağını kontrol etme, verilere erişme, verileri düzenleme ve uygun şekilde imha etme hakkını içermektedir (Metheny, 2017, s.90). Gizlilik sıklıkla güvenlik kavramıyla birlikte ele alınır. Gizlilik ve güvenlik birçok açıdan örtüşmekle birlikte gizlilik; şeffaflık, bildirim ve seçim ilkelerini de içerdiğinden güvenlikten daha fazlası olarak görülmektedir (NIST, 2013).

Veri gizliliği ile doğrudan ilişkili bir diğer kavram ise veri sahipliğidir. Verilerin gerçekte kimin 'sahip olduğu' son yıllarda araştırmacıların ilgisini çekmiştir. Örneğin, Facebook'un, kullanıcıların verilerini Facebook'tan silemeyeceklerine dair duyurusu tartışmalara neden olmuştur. Hukuk teorisindeki baskın görüş ise "verilere sahip olunamayacağı" yönündedir. Veri sahipliği ile ilgili farklı yaklaşımlar söz konusudur: Bir tarafta bireysel vatandaşların kendi verileri üzerinde daha etkili kontrol sahibi olması gerektiğini benimseyenler bulunmaktadır. Buna göre mülkiyet hakları, kişisel verileri korumanın tek etkili yolu olarak görülmektedir İkinci grup ise, kişisel verilerin mülkiyet haklarıyla korunması gerektiği fikrini reddeder ve kişisel verilerin mahremiyet gibi insan hakları yoluyla korunmasını tercih eder. Burada mahremiyet toplu bir haktan ziyade bireysel bir hak olarak anlaşılmaktadır. Yeni Avrupa Birliği Genel Veri Koruma Tüzüğü (European Union General Data Protection Regulation- GDPR), veri

sahiplerine kişisel verilerini kontrol etme konusunda daha fazla hak vermesi anlamında çoğunlukla "bireysel kontrol" yaklaşımına dayanmaktadır (Prainsack, 2019, s.2). Hukuk teorisindeki baskın görüş, verilere sahip olunamayacağı yönündedir. Hummel vd., (2021) veri sahipliği ile ilgili literatürdeki temel görüşleri bir arada yorumladıkları çalışmalarında, verilerin pazarlanması ve metalaştırılmasıyla ilgili olarak, verilerin ekonomik potansiyelinden yararlanmak ve veri öznelerini verilerini satacak ve böylece ondan elde edilen değerden pay alacak bir konuma getirilmesi gerektiğini savunmuşlardır. Bunu yaparken verilerin ticari amaçlı paylaştıktan sonra veri sahipleri için kontrol kaygılarının ortaya çıkması endişesinin giderilmesi gerektiğidir.

Gizlilikle ilgili endişeler, tüketicilerin kişisel verilerinin ifşası ve işlenmesine yönelik tutumlarını ve endişelerini yansıtır. Bu noktadan hareketle Malhotra vd., (2004) internet kullanıcılarının bilgi gizliliği konusundaki endişelerini üç boyutla ilişkilendirmiştir (s.338). Bunlardan ilki veri toplamanın prosedüre uygun olup olmadığı, ikincisi kişilerin veriler üzerinde kontrole sahip olup olmadığı ve üçüncüsü farkındalık yani kişilerin, verilerinin kullanımı hakkında yeterince bilgilendirilip bilgilendirilmediğidir.

Veri gizliliğinin en güncel tartışmaları; sosyal medya üzerinden toplanan tüketici verilerinin, özellikle hedef reklamcılık alanında kullanılmak üzere elde edilmesi ve işlenmesidir. Her ne kadar bilişim teknolojilerindeki gelişmelere paralel olarak şifreleme yöntemleriyle kişisel verilerin paylaşılmasının önüne geçilmeye çalışılsa da kullanıcı bilgileri, ticari şirketlerin müşteri profillerini oluşturmaları için kullanılmaktadır. Google, tüketici verilerini Gmail, Calendar (Google Takvim), Docs (Google Dokümanlar), Maps (Google Haritalar) ve YouTube gibi çeşitli ürünlerindeki tüketicilerin profilini oluşturmak için birleştirip, reklam verenlere hedefleme fırsatları sunmaktadır (Bleier vd., 2020, s.1). Reklam verenler için benzersiz fırsatlar oluşturan bu alanlar tüketiciler için en önemli endişe kaynağı olabilmektedir. ABD'de Ponemon Enstitüsü'nün 786 Amerikalı tüketiciden oluşan bir örneklemle yaptığı araştırmada, katılımcıların yüzde 62'si gizli verilerinin kaybolduğu veya çalındığı konusunda bilgilendirildiklerini ve bu tüketicilerin yüzde 84'ü veri kaybı nedeniyle endişe duyduklarını belirtmişlerdir (Smith vd., 2011, s.90). En çok ziyaret edilen 50 web sitesinin kurumsal gizlilik uygulamalarını analiz eden bir çalışma, bu web sitelerinin çoğunun hedef reklamcılık için kişisel bilgileri kullandığını ve Google, Yahoo, Microsoft ve Facebook gibi çok sayıda saygın firmanın topladığı müşteri verilerini yüzlerce bağlı şirketle paylaştığını tespit etmiştir (Gomez vd., 2009).

Bleier vd. (2020), önümüzdeki yıllarda veri gizliliği sorununun çözümlenmemesi durumunda, veriye dayalı inovasyon ve pazarlamanın olumsuz etkileneceğine ve işletmelerin satışların azalması, veri kısıtlaması, dava riskleri ve gizlilik düzenlemesi nedeniyle stratejik kapsamın daraltılması sonuçlarıyla karşılaşacaklarına dikkat çekmiştir (s.2). Diğer taraftan, gizlilik endişeleri e-ticaretin büyümesini engelleyen önemli bir sorun olarak görülmekte ve tüketicilerin çevrimiçi kişiselleştirme hizmetlerinden yararlanmamalarına neden olmaktadır (Baruh vd., 2017, s.2). Dolayısıyla veri gizliliği sorunu, işletmelerin verilerle ilgili uygulamalarına daha katı gizlilik düzenlemeleri getirmelerini zorunlu kılmaktadır. Burada esas olan; hükümetlerin ve işletmelerin veriye dayalı yeniliği ve bireysel eylem belirleme stratejisini sağlarken, kullanıcıların veri gizliliğini de dikkate alarak başarılı bir düzenleyici ortamı oluşturabilmeleridir.

3.1. Veri Gizliliğine İlişkin Tüketici Endişeleri

Literatürde veri gizliliği endişelerinin çevrimiçi satın alma davranışına etki ettiğini öne süren çok sayıda araştırma mevcuttur (Bélanger vd., 2002; Eastlick vd., 2006; Bélanger ve Crossler, 2011). E-ticaret ilişkilerinde bilgi gizliliği konusu ise merkezde yer almaktadır. E-ticaret gerçekleştiren işletmeler, müşteri ihtiyaçlarını belirlemek ve kişiselleştirilmiş promosyonlar sunabilmek için web siteleri aracılığıyla müşteriler hakkında bilgi toplamaktadır. Ticari web sitelerinin rekabet stratejileri giderek büyük miktarda müşteri verisine dayanırken, işletmelere değer sağlayan aynı veri uygulamaları tüketiciler için gizlilik endişesini beraberinde getirmektedir (Culnan ve Armstrong, 1999, s.104). Buna rağmen, yaygın görüş işletmelerin ve hükümetlerin gizlilik endişelerini giderebilecek uygulamaları hayata geçirmesiyle, müşterilerin adil uygulamalar karşısında kişisel bilgilerini iş süreçlerinde

kullanılmak üzere paylaşmaya ikna olacağıdır (Culnan ve Armstrong, 1999; Miller ve Tucker, 2009; Pavlou, 2011).

Kişisel verilerin uygunsuz kullanımı, tüketici mahremiyetine iki şekilde zarar verebilir. Birincisi, kişisel bilgilerin uygunsuz kullanımıdır. Buna, istenmeyen e-postalar, kredi kartı dolandırıcılığı veya kimlik hırsızlığı örnek olarak verilebilir. Genel olarak uygun gizlilik ve güvenlik kontrollerinin olmaması kişisel verilerin uygunsuz kullanımına sebep olmaktadır. İkincisi ise, kişisel bilgilerin, alışveriş dışındaki amaçlar için tüketicinin rızası olmadan yetkisiz kullanımıdır. Buna göre, bilgi gizliliğine ilişkin endişeler, kişisel bilgilerin uygunsuz kullanımı, kişisel bilgilerin dış taraflara ifşa edilmesi ve kişisel bilgilerin bireyin rızası olmadan yetkisiz ikincil kullanımı ile ilgilidir (Pavlou, 2011, s.981). Bu nedenle araştırmalar, diğer faktörlerle birlikte bilgi gizliliğine ilişkin endişelerin, bireylerin çevrimiçi hizmetleri kullanma niyetlerini etkilediğini göstermektedir (Bélanger vd., 2002; Eastlick vd., 2006; Bélanger ve Crossler, 2011). Gizlilik endişeleri, ayrıca bireylerin kişisel bilgilerini web siteleriyle paylaşmaya daha az istekli olmalarına da yol açmaktadır (Bélanger ve Crossler, 2011, ss.1021-1022).

Bununla birlikte bilgi gizliliği endişelerinin çevrimiçi satın alma davranışı üzerinde çok düşük düzeyde bir etkisinin olduğunu ileri süren araştırmalar da vardır (Drennan vd., 2006; Chen ve Li, 2009). Bu bulguların literatürdeki diğer sonuçlarla çelişmesi güvenin rolü ile açıklanabilir. Çünkü güven, bilgi gizliliği ile birlikte bir faktör olarak düşünüldüğünde, internetten satın alma niyetlerini belirlerken gizlilikten daha önemli görülmektedir (Bélanger ve Crossler, 2011, ss.1021-1022). Bu nedenle birçok araştırmaya göre veri gizliliğine etki ettiği düşünülen kavramların başında tüketici güven tutumu gelmektedir (Bélanger vd., 2002; Dinev ve Hart, 2006; Eastlick vd., 2006; Bansal vd., 2010; Bélanger ve Crossler, 2011; Liao vd., 2019).

Tüketici güvenini tesis etmede en önemli adım, tüketicilerin kişisel bilgilerinin korunacağına dair güvence sağlamaktır (Bélanger vd., 2002, s.246). Buna ek olarak gizlilik ve güven arasındaki ilişkiye işletmenin itibarını da ekleyerek; güçlü bir firma itibarının, yalnızca tüketiciler arasında güven algısını ortaya çıkarmakla kalmayacağı, aynı zamanda gizlilik endişeleriyle ilişkili riskleri de azaltacağını öne sürmüşlerdir (Pavlou, 2011, s.981).

3.2. Veri Gizliliği Hakkında Hukuki ve Teknolojik Uygulamalar

Hükümetler, vatandaşların mahremiyetini korumak için küresel platformlar ve hizmetler arasındaki bilgi akışının düzenlenip düzenlenmeyeceği ve nasıl düzenleneceği konusunda mücadele etmektedir. İlgi alanlarının, tarihlerin ve kültürel bağlamların çeşitliliği göz önüne alındığında, ağlar arasında mahremiyetin ve kişisel veri akışlarının korunmasına yönelik karmaşık bir ulusötesi yasalar ve politikalar alanı ortaya çıkmıştır. Bazı bölgeler, Kanada'nın Kişisel Bilgilerin Korunması ve Elektronik Belgeler Yasası (PIPEDA) ve Avrupa Birliği'nin Genel Veri Koruma Yönetmeliği (GDPR) gibi kişisel bilgilerin toplanmasını, kullanılmasını ve ifşa edilmesini düzenleyen geniş ve nispeten katı yasaları seçmiştir. Ancak Amerika Birleşik Devletleri, yalnızca belirli kişisel bilgi türlerini ele alan yasalarla gizlilik mevzuatına daha sektörel bir yaklaşım sergilemektedir. Örneğin, Sağlık Sigortası Taşınabilirlik ve Sorumluluk Yasası (HIPAA) kişisel tıbbi bilgilerin korunmasını sağlar; Adil Kredi Raporlama Yasası, kişisel finansal verilerin toplanmasını ve akışını düzenler ve Video Gizliliğini Koruma Yasası, video kiralama kayıtlarının haksız yere ifşa edilmesini yasa dışı kılar (Wu vd., 2019, s.4).

AB ve Kanada, kişisel verilerin toplanması ve kullanılmasına ilişkin doğrudan ve önleyici düzenlemelere, "fazla" veri toplamanın yasaklanmasına, veri toplama ve kullanımının önceden belirlenen amaçlarıyla sınırlandırılmasına odaklanmıştır. ABD ise, çoğu veri toplamanın ve kullanımın hem kabul edilebilir hem de faydalı olması noktasından hareketle, düzenlemenin yalnızca belgelenmiş yanlış kullanım veya zarar durumlarını ele alması gerekliğine odaklanmıştır. Gizliliğe yönelik düzenleyici yaklaşımlardaki bu farklılık ve farklı yargı alanlarının veri öznelerinin haklarına yönelik görüşleri arasındaki temel görüş ayrılıkları, ulusötesi ağlar arasında ve sınırlar arasında artan kişisel bilgi akışı göz önüne alındığında daha da karmaşık hale gelmektedir. Google ve Facebook gibi internet şirketleri, veri işleme ve depolama tesislerinin eşit olarak dağıldığı, dünyanın dört bir yanından ürün ve hizmetlerine erişen müşterilere

sahiptir. Örneğin bir Kanada vatandaşı, Amerika Birleşik Devletleri'ndeki bir Google ürününe erişiyor olabilirken, belirli bilgi alışverişinin kaydı İrlanda'daki bir sunucuda saklanıyor olabilir. Her yargı yetkisi, paylaşılan ve depolanan herhangi bir kişisel bilginin işlenmesine atanan kendi karmaşık düzenlemelerine ve haklarına sahiptir (Wu vd., 2019, s.4).

Veri gizliliği hakkında teknolojik uygulamalar genellikle mahremiyetin korunması veya ihlali ile ilgili bireysel ve kurumsal eylemleri ve bu uygulamaları etkileyen çeşitli faktörleri araştırır. Bireysel bilgi gizliliği uygulamaları, bilgileri ifşa ederken dikkatli olmayı, gizlilik koruma yazılımını, kişisel bilgileri tahrif etmeyi, istenmeyen e-postaları filtrelemek veya silmek gibi pasif kısıtlamalar kullanmayı ve kimlik değişikliğini kullanmayı içerir. Bulgular, şirketlerin birçoğunun gizlilik politikalarına sahip olmaması nedeniyle hala tüketiciler için uygun gizlilik koruması sağlamadığını ve bunu yaptıklarında da genellikle FIP'e (Federal Information Processing Standard – Federal Bilgi İşleme Standartları) uymadıklarını göstermektedir. Buna rağmen, ABD şirketlerinin büyük olasılıkla bir gizlilik politikasına sahip olduğuna dair birçok çalışma bulunmaktadır (Bélanger ve Crossler, 2011, ss.1021-1022).

Bilgi gizliliği araçları ve teknolojileri üzerine araştırmalar, tipik olarak bilgi gizliliği korumasıyla ilgilenmek için yapay veya teknolojik çözümler sunar. Araştırma genellikle gizlilik tehditlerinin incelenmesiyle başlar ve daha sonra bu tehditleri ele almak için teknik veya kavramsal çözümler sunar. Tartışılan araçlar ve teknolojiler, hem mahremiyeti istila eden teknolojileri (PITS) hem de mahremiyeti artıran teknolojileri (PET'ler) içerir. Bu açıkça hem araştırma hem de pratik sonuçları olan bir alandır (Bélanger ve Crossler, 2011, ss.1022).

4. Dijital Reklamcılık ve Veri Gizliliği

Çevrimiçi izleme ve bağlı cihazlar, veri toplama ve analizi için yeni fırsatlar yaratmıştır. Çevrimiçi göz atma davranışı genellikle ürünleri ve reklamları hedeflemek için kullanılır. Örneğin Netflix, önerileri kişiselleştirmek ve son zamanlarda etkileşimli bölümler aracılığıyla yenilikçi içerik geliştirmek için milyonlarca müşterisinden görüntüleme bilgilerini toplamaktadır (Bleier vd., 2020, s.2). Dolayısıyla dijital veriler, firmaların tüketicilerin satın almaları, davranışları ve zevkleri hakkında büyük miktarda bilgi toplamasını ucuz ve kolay hale getirir. Bununla birlikte dijital verilerin hedef pazarlama ve reklamcılıkta kullanımı tüketicilerin veri gizliliği endişelerini oldukça arttırmıştır. Tucker (2015), dijital alanlarda gizlilik endişeleriyle ilgili en önemli alanları nesnelerin interneti, biyo-bilginin dijitalleşmesi ve konumsal mahremiyet olarak sınıflandırmıştır. Nesnelerin internetinde bir kullanıcının web kameralar, alarmlar gibi nesnelerin her biriyle nasıl etkileşime girdiği ölçülerek, veri analistlerinin yardımıyla kullanıcının davranışının eksiksiz bir resmi elde edilebilmektedir (s.558). Böylece bireyler, siber ortamda verilerini veya en azından izlerini bırakabilmekte ve bilgileri olmadan takip edilebilmektedir. Daha da endişe verici olanı, artık sadece kamu kurumlarının değil, aynı zamanda pazarlama işletmeleri gibi özel aktörlerin de bu kişisel verileri toplamakla ilgilenmeleridir (Weber, 2010, s.24). Biyo-bilginin dijitalleşmesi sonucunda ise kişisel sağlık bilgilerinin artık özel olmadığını görülmektedir. Sosyal medya platformları, giyilebilir fitness takip cihazları ve hamilelik ve ruh sağlığını yönetmeye yönelik uygulamaların tümü, tıbbi kayıtlara ve diğer tüketici bilgilerine eklenebilen sağlık verilerini toplamakta ve reklam amacıyla paylaşılabilmektedirler. Nitekim kadınların hamileliklerini ve doğumlarını takip etmek için kullanabilecekleri bir uygulama olan Ovia, bu tür verileri işverenlere kimliksiz biçimde gösteren ücretli hizmetler sunmuştur (Bari ve O'Neill, 2019, s.1). Son olarak mobil cihazlar yardımıyla kullanıcıların konum bilgilerinin izlenebilmesi önemli bir veri gizliliği sorunu doğurmaktadır.

Dijital verilerin en yoğun şekilde kullanıldığı alan dijital reklamcılıktır. Reklamcılığın tüm izleyicilere gelişigüzel yayınlandığı bir paradigmadan, her reklamın ayrı ayrı hedeflendiği bir paradigmaya doğru ilerledikçe, belirli bir tüketicinin davranışına odaklanması açısından medya endüstrisinde önemli bir değişim olmuştur. Bu noktada çevrimiçi reklamcılığının ayırt edici özelliği, bilgiyi hedeflenen bir kitleye iletme yeteneğidir. Hedeflemedeki bir artış, tüketici-ürün eşleşmelerinin toplam sayısında ve dolayısıyla reklamın sosyal değerinde bir artışa yol açar. Hedefleme aynı zamanda her pazarda reklam veren firmaların konsantrasyonunu da arttırır. Özellikle hedefleme, tüketici ile reklam mesajı arasındaki eşleşmenin kalitesini iyileştirir ve daha küçük işletmelerin daha önce dışlandıkları reklam pazarlarına

erişmelerini sağlar. Reklam verenler, reklam gösterimi alacak tüketicileri, Web'de gezinirken tıklama bazında ayak izlerini dikkate alınarak söz konusu tüketicilerin kişisel zevkleri ve eylemleri ile ilgili bilgilerine göre anonim olarak seçer (Tucker, 2015, s.545; Bergemann ve Bonatti, 2011, s.417). Mobil cihazların konum, durum ve kullanım bilgilerini izleyen sensörlerle donatılmaları da yeni veri türlerinin elde edilmesine ve reklam verenlere hedefli ürün ve özellikler sunma fırsatı sağlamıştır. Reklam verenler için benzersiz fırsatlar sunan bu teknolojik gelişmeler tüketiciler için yeni tür veri gizliliği endişelerini beraberinde getirmiştir. Örneğin, kişisel sağlık veya fitness izleyicileri, tüketici etkinliği gösterge tablolarını ve emsallerle karşılaştırmaları kolaylaştırmak için tüketici verilerini doğrudan kullanır. Bu veriler, amacı dışında yani sigorta veya kredi puanlama gibi fitness takibi dışında bir amaç için kullanılırsa, verilerin yeni bağlamı gizlilik endişelerini artıracaktır (Bleier vd., 2020, s.3).

Goldfarb ve Tucker (2011), çevrimiçi reklamcılığın etkinliğini araştırdıkları çalışmada, iki stratejiyi ele almışlardır. Bu stratejilerden biri, bir reklamı web kullanıcısının aradığı içerikle eşleştirmektir. Diğer strateji ise rahatsız edicilik yani reklam verenlerin, video ve sesi kullanarak, bir reklamı kullanıcının aradığı içeriğin üzerinde gezdirme veya devralma yeteneği dahil, rahatsız edici reklam özellikleridir. Çalışmada bir reklamı web sitesi içeriğiyle eşleştirmenin ve bir reklamın rahatsız ediciliğini artırmanın bağımsız olarak satın alma amacını artırdığını tespit etmişlerdir. Bununla birlikte hem hedeflemeyi hem de rahatsız ediciliği birleştirmeye yönelik girişimler, iki tekniğin tek başına sahip olduğu olumlu etkileri geçersiz kılar. Aynı rahatsız edici reklam, alakasız içeriğe sahip web sitelerinde alakalı içeriğe göre çok daha iyi sonuç verir. Bu sonucun olası bir açıklaması, bu reklamcılık tekniklerinin her ikisinin de kullanıcıların gizliliğini etkilemesidir. Zayıf hedefleme biçimleri bile, reklam verenlerin kullanıcı ve çevrimiçi ortamda neye baktıkları hakkında kitle iletişim araçları reklamcılığına göre daha fazla veri toplamasına ve kullanmasına dayanır. Kasıtlı olarak rahatsız edici reklamcılık ayrıca çevrimiçi deneyimlerini izinsiz olarak kesintiye uğratarak kullanıcıların gizliliğine müdahale eder. Acquisti ve Spiekermann (2011), çevrimiçi ortamda rahatsız edici pop-up reklamların, reklamı yapılan mallar için ödeme yapma istekliliğini olumsuz yönde etkilediğini göstererek bu bulguyu güçlendirmektedir. Bu, gizlilik tartışmalarının çoğu veriyle zenginleştirilmiş reklamlara odaklanmış olsa da reklamların davranışsal hedeflemenin ötesinde kullanıcıların gizliliğine müdahale edebileceği birçok başka olumsuz yol olduğunu tekrar vurgulamaktadır. Bu nedenle, kullanıcı gizliliğine yönelik daha kapsamlı bir yaklaşım, rahatsız edici olmanın kullanıcı deneyimini nasıl engellediğini ve bunun rahatsız edici olmayan ancak kişisel olarak hedeflenen reklamlarla nasıl değiştirilebileceğine odaklanmaktır (Tucker, 2015, s.546; Acquisti ve Spiekermann, 2011, s.417).

2010'da Amerikan Reklam Endüstrisi, tüketicilerin gizlilik endişelerini giderebilmek için AdChoices programını uygulamış ve tüketicilere reklamların üzerine yerleştirilmiş AdChoices simgelerine tıklayarak ulaşılabilen özel bir web sitesi aracılığıyla çevrimiçi davranışsal reklamcılığı devre dışı bırakabilme seçeneği sunmuşlardır. Böylece program, tüketicilere kişisel bilgilerinin reklam amaçlı kullanımı hakkında "bildirim ve seçenek" sunmaktadır. Johnson vd. (2020) AdChoices uygulamasının etkinliğini araştırmışlar ve tüketicilerin anketlerde güçlü gizlilik endişelerini dile getirmelerine rağmen, Amerika'daki reklam gösterimlerinin yalnızca %0.23'ünün çevrimiçi davranışsal reklamcılığı devre dışı bırakan kullanıcılardan oluştuğunu tespit etmişlerdir. Buna ek olarak, devre dışı bırakma seçeneğini seçen kullanıcıların, davranışsal hedeflemeye izin veren kullanıcılara göre %52 daha az gelir getirdiğini tespit etmişlerdir. Bu bulgular, endüstrinin daha sonra AdChoices programını uyguladığı Avrupa Birliği ve Kanada'dan elde edilen kanıtlarla büyük ölçüde tutarlıdır. Sonuç olarak davranışsal reklamcılığı devre dışı bırakan kullanıcılara, hedefli reklamlar sunulamamış olması, tüketicisi başına reklam harcamasında yaklaşık 8,58 ABD doları tutarında bir kayıpla sonuçlanmıştır.

Gizlilik endişeleri, firmaları doğrudan gelir kaybıyla hemen etkiler çünkü tüketiciler, mahremiyetlerini tehdit ediyor gibi görünen firmalara yanıt vermemeyi veya onlardan satın almamayı seçerler. Örneğin, tüketiciler, firmanın kullanım alışkanlıkları hakkındaki bilgileri reklam firmalarına satacağından korkuyorlarsa, belirli bir akıllı ev asistanı satın alma planlarından vazgeçebilirler (Bleier vd., 2020, s.2).

Campbell vd. (2015), tüketicilerin verilerinin gizliliğini korumaya yönelik düzenleyici girişimlerin, veri yoğun endüstrilerin rekabetçi yapısını nasıl etkilediğini modellemişlerdir. Çalışmada, işletmelerin

tüketicilere bildirimde bulunmak, verilerini toplamak ve depolamak için onlardan onay almalarını zorunlu kılmanın, daha küçük ve yeni firmalar açısından nispeten büyük işletmelere göre daha dezavantajlı olduğunu tespit etmişlerdir. Bunun nedeni, küçük ve yeni firmaların tüketicilerin onayı karşılığında ikna edici bir ürün ölçeğine ve operasyon geçmişine sahip olmamalarıdır.

SONUÇ:

Dijital çağda tüketicilerin bilgiye daha kolay erişmeleri, daha bağlantılı ve yetkili konuma gelmeleri, pazarlama iletişiminin kontrolünü de büyük ölçüde ellerinde bulundurmalarıyla sonuçlanmıştır. Geleneksel reklamcılıkta içerik üretme ve reklamın tüketiciye sunulma biçimi, daha çok reklam verenlerin sezgi ve tecrübesine dayanmaktaydı. Dijital reklamcılıkta ise veriye dayalı reklamlar üretilmekle birlikte, reklamın tüketiciye ulaştırılma kanallarının seçiminde de tüketicilerin dijital izleri kullanılmaktadır.

Dinamik Reklam Optimizasyonu (DRO) ile reklam metni, ürün resmi, afiş boyutu gibi reklam öğelerini gerçek zamanlı olarak tüketicilerin ilgi alanlarına uyarlayarak, reklamın etkinliği en üst düzeye çıkarılmış (Lee ve Cho, 2020) ve kişiye özgü en iyi reklam içeriğinin bütünsel olarak yakalanması mümkün olmuştur. Makine öğrenmesi, dijital reklamcılıkta hedefli reklamların üretilmesinde yaygın olarak kullanılmaktadır. Bir makine öğrenmesi algoritması, tüketicilerin geçmiş okumaları, alışverişleri gibi tüm dijital izleri değerlendirerek, kişiye özgü bir reklam teklifinde bulunabilir. Dolayısıyla bir makine öğrenmesi algoritması, tercih ve davranış verilerini kullanarak, her tüketicinin ayrı bir segment oluşturduğu, büyük ölçekli, otomatik olarak kişiselleştirme ve hedefleme gerçekleştirebilen bir model sunar. Çalışmada dijital reklamcılıkta makine öğrenmesi algoritmalarının nasıl kullanıldığını gösteren literatürdeki önemli çalışmalara yer verilmiştir. Diğer taraftan, makine öğrenmesi algoritmaları ile kişiselleştirilmiş reklamcılığın işletmelere sağladığı karlılığın, geleneksel reklamcılığa göre anlamlı düzeyde yüksek olduğu gösterilmiştir.

İşletmelere sağladığı tüm faydalara rağmen, makine öğrenmesi teknikleri kullanılan hedef reklamcılık, tüketici mahremiyeti ve veri gizliliği tartışmalarının odağında yer almaktadır. Bu nedenle çalışmada makine öğrenmesinin hedef reklamcılıkta kullanımının faydalarının yanında, gizlilik endişeleri de ele alınarak konuya bütünsel bir yaklaşım getirilmesi hedeflenmiştir. Böylece işletmelerin ve reklam verenlerin hedef reklamcılık tekniklerini kullanırken, veri gizliliği endişelerini arttırarak tüketici kaybetmemeleri için alabilecekleri önlemler tartışılmıştır.

Gizlilik kaygıları, tüketicilerin banner reklamlara tıklama olasılığını azaltarak, dijital reklamlarla beslenen firmaların kârlarına zarar verebilir. Ek olarak, kişiselleştirilmiş çevrimiçi reklamlardan bıkan tüketiciler, hedeflenen reklamları almaktan vazgeçebilir veya hedeflenen reklam destekli platformlar için kayıplara neden olabilecek reklam engelleme teknolojisini kullanabilir. Son araştırmalar, reklam engellemenin gelecekteki web sitesi trafiği üzerindeki olumsuz etkilerini göstermektedir (Shiller vd., 2018). Ayrıca, bu doğrudan etkiler borsa değerini etkileyebilir (Bleier vd., 2020, s.3).

Hem makine öğrenmesi algoritmalarının sunduğu kişiselleştirilmiş reklamcılığın sürdürülmesi, hem de veri gizliliği endişeleri nedeniyle müşteri kayıplarının önlenmesi için atılması gereken önemli adımlar mevcuttur. Amerikan Reklam Endüstrisi'nin AdChoices uygulamasında olduğu gibi tüketicilere çevrimiçi davranışsal reklamcılığı devre dışı bırakma olanağı tanınarak, bildirim ve seçenek hakkı tanınabilir. Yapılan çalışmalar çevrimiçi davranışsal reklamcılığı devre dışı bırakan tüketici sayısının çok az olduğunu, buna rağmen böyle bir tercih hakkı sunulmasının tüketiciler üzerinde olumlu bir izlenim bıraktığını ortaya çıkarmıştır (Johnson vd., 2020). Diğer taraftan Almuhimedi vd. (2015) bir saha çalışmasında, mobil cihazlarda basit bir dürtme yaklaşımı ile katılımcıların mobil uygulama gizlilik ayarlarını değiştirmelerine ve veri paylaşım davranışlarını gizlilik tercihleriyle uyumlu hale getirmelerine yol açabileceğini göstermiştir. Bu amaçla, mahremiyet için tasarım, halihazırda oluşturulmuş kişisel verileri koruyan ana akım mekanizmaların ötesine geçmeli ve bunun yerine hem bireyleri hem de kuruluşları çeşitli bağlamlarda önleyici davranışlara yönlendirmek için yaratıcı yollar geliştirmelidir (Wu vd., 2019, s.4). Kullanıcılara devredilen bir gizlilik yönetimi sorumluluğu, ortamların

karmaşık yapısı ve gizlilik saldırıları nedeniyle verimsizleşmektedir. Bu nedenle, kullanıcıların gizliliklerini korumalarına yardımcı olmak için otomatikleştirilmiş gizlilik yönetim sistemleri geliştirmeye acil bir ihtiyaç vardır. Bu çalışmada, veri gizliliği ihlallerinin çözümünde de makine öğrenmesi algoritmalarının kullanımı önerilmektedir. Nitekim yapılan araştırmalarda gizlilik politikasının değerlendirilmesi ve kullanıcı tercih yönetimi konularında makine öğrenmesi uygulamalarının etkili sonuçlar verdiği kanıtlanmıştır (Liu vd., 2021). Makine öğrenmesi algoritmalarının tercih edilmesinin temel sebebi gizlilik politikaları bilgilerinin uzun ve karmaşık metinler halinde yazılması ve çoğu tüketicinin bu bilgileri okumadan onaylamasıdır. Literatürde gizlilik politikası metinlerinin anlaşılır ve çok kısa metinlere dönüştürmek için makine öğrenmesi algoritmalarından yararlanılmıştır (Tesfay vd., 2018). Kullanıcı gizliliğinin korunmasındaki bir diğer zorluk, her kullanıcının farklı bir gizlilik hassasiyeti ve tercihine sahip olmasından kaynaklanmaktadır. Uygulamaları yüklerken, kullanıcılardan genellikle kaynaklara erişim izinleri istenir. Kullanıcı gizlilik tercihlerini tahmin etmek ve karar vermeye yardımcı olmak için makine öğrenmesi teknikleri uygulanmaktadır. Araştırmalar, makine öğrenmesi yardımıyla benzer düşünen kullanıcı kümelerine dayalı öneriler sağlamanın ve insanların gizlilik tercihlerine ilişkin tahmine dayalı modellerin kullanılmasının, kullanıcıların memnuniyetini arttırdığını göstermektedir (Liu vd., 2021). Dolayısıyla dijital reklamcılıkta makine öğrenmesi algoritmaları ve otomatik sitemlerin kullanımıyla meydana gelen veri gizliliği ihlallerinin giderilmesi için, yine makine öğrenmesi algoritmalarının kullanılabileceği görülmektedir. Gelecekte makine öğrenmesi algoritmalarının kullanılmasıyla kişiselleştirilmiş reklamcılığın daha da ilerleyerek her bireyin bir segment olarak kabul edildiği mikro pazarlama süreçlerine geçileceği öngörülmektedir. Bunula birlikte tüketici verilerinin dijital reklamcılıkta kullanılması ancak makine öğrenmesi ile kişiye özgü veri gizlilik ayarlarının yapılarak mahremiyetin, tüketicinin gizlilik sınırları çerçevesinde yapılandırılması önem taşımaktadır. Böylece şirketlerin hem karlılığı koruması hem de veri gizliliği nedeniyle tüketici kayıplarının önüne geçmesi mümkün olacaktır.

Çalışmada dijital reklamcılıkta makine öğrenmesinin ne şekilde kullanıldığı, bununla birlikte meydana getirdiği veri gizliliği ihlalleri ele alınmıştır. Çalışmanın dijital reklamcılıkla ve veri gizliliği ile sınırlı tutulması temel kısıtlarıdır. Gelecek çalışmalarda dijital pazarlamanın tüm alanlarında, makine öğrenmesi algoritmalarının veri gizliliği ihlallerini önlemede kullanılabileceği düşünülmektedir. Diğer taraftan makine öğrenmesi algoritmalarının tüketicilerin gizlilik ihlallerinin yanında güvenlik endişelerine yönelik çözümlerde de kullanılması önerilmektedir.

Etik Standart ile Uyumluluk

Çıkar Çatışması: *Yazarlar herhangi bir çıkar çatışmasının olmadığını beyan eder.*

Etik Kurul İzni: *Bu çalışma için etik kurul iznine gerek yoktur.*

Finansal Destek: *Yoktur.*

Teşekkür: *Yoktur.*

KAYNAKÇA:

Acquisti, A. ve Spiekermann, S. (2011). Do Interruptions Pay Off? Effects Of Interruptive Ads On Consumers' Willingness To Pay. *Journal of Interactive Marketing*, *25*(4), 226-240. https://doi.org/10.1016/j.intmar.2011.04.003

Almuhimedi, H., Schaub, F., Sadeh, N., Adjerid, I., Acquisti, A., Gluck, J., ... ve Agarwal, Y. (2015, April). Your Location Has Been Shared 5,398 Times! A Field Study On Mobile App Privacy Nudging. In *Proceedings of the 33rd annual ACM conference on human factors in computing systems* (ss.787-796).

Alzubi, O. A., Alzubi, J. A., Alweshah, M., Qiqieh, I., Al-Shami, S., ve Ramachandran, M. (2020). An Optimal Pruning Algorithm Of Classifier Ensembles: Dynamic Programming Approach. *Neural*

Computing and Applications, *32*(20), 16091-16107. https://doi.org/10.1007/s00521-020-04761-6

Avila Clemenshia, P. ve Vijaya, M. S. (2016). Click Through Rate Prediction For Display Advertisement. *International Journal of Computer Applications (975-8887), 1*(136), 18-24

Bansal, G., Zahedi, F.M. ve Gefen, D. (2010). The Impact Of Personal Dispositions On Information Sensitivity, Privacy Concern And Trust In Disclosing Health Information Online. *Decision Support Systems*, *49*(2), 138-150. https://doi.org/10.1016/j.dss.2010.01.010

Bari, L., & O'Neill, D. P. (2019). Rethinking Patient Data Privacy in The Era Of Digital Health. *Health Affairs*, 12. https://www.healthaffairs.org/do/10.1377/forefront.20191210.216658

Baruh, L., Secinti, E. ve Cemalcilar, Z. (2017). Online Privacy Concerns And Privacy Management: A Meta-Analytical Review. *Journal of Communication*, *67*(1), 26-53. https://doi.org/10.1111/jcom.12276

Bélanger, F. ve Crossler, R. E. (2011). Privacy In The Digital Age: A Review Of Information Privacy Research In Information Systems. *MIS Quarterly*, 1017-1041. https://doi.org/10.2307/41409971

Bélanger, F., Hiller, J. S. ve Smith, W. J. (2002). Trustworthiness In Electronic Commerce: The Role Of Privacy, Security, And Site Attributes. *The Journal Of Strategic Information Systems*, *11*(3-4), 245-270. https://doi.org/10.1016/S0963-8687(02)00018-5

Bergemann, D. ve Bonatti, A. (2011). Targeting In Advertising Markets: Implications For Offline Versus Online Media. *The RAND Journal of Economics*, *42*(3), 417-443. https://doi.org/10.1111/j.1756-2171.2011.00143.x

Bleier, A., Goldfarb, A. ve Tucker, C. (2020). Consumer Privacy And The Future Of Data-Based Innovation And Marketing. *International Journal of Research in Marketing*, *37*(3), 466-480. https://doi.org/10.1016/j.ijresmar.2020.03.006

Breiman L. (2001). Random Forests, Machine Learning, 45 (1), 5-32.

Campbell, J., Goldfarb, A. ve Tucker, C. (2015). Privacy Regulation And Market Structure. *Journal of Economics & Management Strategy*, *24*(1), 47-73. https://doi.org/10.1111/jems.12079

Chapelle, O., Manavoglu, E. ve Rosales, R. (2014). Simple And Scalable Response Prediction For Display Advertising. *ACM Transactions on Intelligent Systems and Technology (TIST)*, *5*(4), 1-34. https://doi.org/10.1145/2532128

Chen, S. ve Li, J. (2009, May). Factors Influencing The Consumers' Willingness To Buy In E-Commerce. In *2009 International Conference on E-Business and Information System Security* (pp. 1-8). IEEE. https://doi.org/10.1109/EBISS.2009.5137979

Choi, J. A., & Lim, K. (2020). Identifying Machine Learning Techniques For Classification Of Target Advertising. *ICT Express*, 6(3), 175-180. https://doi.org/10.1016/j.icte.2020.04.012

Clarke, R. (1999). Internet Privacy Concerns Confirm The Case For Intervention. *Communications of the ACM*, *42*(2), 60-67. https://doi.org/10.1145/293411.293475

Culnan, M. J. ve Armstrong, P. K. (1999). Information Privacy Concerns, Procedural Fairness, And Impersonal Trust: An Empirical Investigation. *Organization Science*, *10*(1), 104-115. https://doi.org/10.1287/orsc.10.1.104

Dinev, T. ve Hart, P. (2006). An Extended Privacy Calculus Model For E-Commerce Transactions. *Information Systems Research*, *17*(1), 61-80.

Drennan, J., Sullivan, G. ve Previte, J. (2006). Privacy, Risk Perception, And Expert Online Behavior: An Exploratory Study Of Household End Users. *Journal of Organizational and End User Computing (JOEUC)*, *18*(1), 1-22. https://doi.org/10.4018/joeuc.2006010101

Eastlick, M. A., Lotz, S. L. ve Warrington, P. (2006). Understanding Online B-To-C Relationships: An Integrated Model Of Privacy Concerns, Trust, And Commitment. *Journal Of Business Research*, *59*(8), 877-886. https://doi.org/10.1016/j.jbusres.2006.02.006

Ekinci, E., Omurca, S. İ., Kırık, E. ve Taşçı, Ş. (2020). Tıp Veri Kümesi İçin Gizli Dirichlet Ayrımı. *Dokuz Eylül Üniversitesi Mühendislik Fakültesi Fen Ve Mühendislik Dergisi*, 22 (64), 67-80. https://doi.org/10.21205/deufmd.2020226408

Goldfarb, A. ve Tucker, C. (2011). Online Display Advertising: Targeting And Obtrusiveness. *Marketing Science*, *30*(3), 389-404. https://doi.org/10.1287/mksc.1100.0583

Gomez, J., Pinnick, T. ve Soltani, A. (2009). *Knowprivacy: The Current State Of Web Privacy, Data Collection, And Information Sharing.* Berkeley, CA: UC Berkeley School of Information. https://www.ischool.berkeley.edu/projects/2009/knowprivacy

Gülpınar Demirci, V. ve Altaş, D. (2020). *Yapay sinir ağları.* D. Altaş ve İ. E. Yıldırım (Ed.), Uygulamalı çok değişkenli İstatistik Teknikler içinde (s.167-188). Eskişehir: Seçkin Yayınevi.

Gülpınar Demirci, V. ve Kaplan, B. (2020). *Veri madenciliği ve pazarlama*. C. Söylemez ve A. Kayabaşı (Ed.) Dijital Pazarlama: Güncel Konular içinde (s.253-282). Bursa: Ekin Yayınevi.

Hsu, C. W. ve Lin, C. J. (2002). A Comparison Of Methods For Multiclass Support Vector Machines. IEEE Transactions On Neural Networks, 13(2), 415-425. https://doi.org/10.1109/72.991427

Hummel, P., Braun, M. ve Dabrock, P. (2021). Own Data? Ethical Reflections On Data Ownership. *Philosophy & Technology*, *34*(3), 545-572. https://doi.org/10.1007/s13347-020-00404-9

Johnson, G. A., Shriver, S. K. ve Du, S. (2020). Consumer Privacy Choice In Online Advertising: Who Opts Out And At What Cost To Industry?. *Marketing Science*, *39*(1), 33-51. https://doi.org/10.1287/mksc.2019.1198

Khan, K., Rehman, S. U., Aziz, K., Fong, S. ve Sarasvady, S. (2014, February). DBSCAN: Past, present and future. In *The fifth international conference on the applications of digital information and web technologies (ICADIWT 2014)* (ss.232-238). IEEE. https://doi.org/10.1109/ICADIWT.2014.6814687

Kuppusamy, K. S. (2018). Machine Learning Based Heterogeneous Web Advertisements Detection Using A Diverse Feature Set. *Future Generation Computer Systems*, *89*, 68-77. https://doi.org/10.1016/j.future.2018.06.028

Lee, H. ve Cho, C. H., (2020) Digital Advertising: Present and Future Prospects. *International Journal of Advertising*, 39(3), 332-341. https://doi.org/10.1080/02650487.2019.1642015

Liao, Y., Vitak, J., Kumar, P., Zimmer, M. ve Kritikos, K. (2019, March). Understanding the role of privacy and trust in intelligent personal assistant adoption. In *International Conference on Information* (ss. 102-113). Springer, Cham.

Liu, B., Ding, M., Shaham, S., Rahayu, W., Farokhi, F. ve Lin, Z. (2021). When Machine Learning Meets Privacy. *ACM Computing Surveys*, *54*(2), 1–36. https://doi.org/10.1145/3436755

Ma, L. ve Sun, B. (2020). Machine Learning And AI In Marketing – Connecting Computing Power To Human Insights. *International Journal of Research in Marketing*, 37(3), 481-504. https://doi.org/10.1016/j.ijresmar.2020.04.005

Malhotra, N. K., Kim, S. S. ve Agarwal, J. (2004). Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model. Information Systems Research, 15(4), 336–355. https://doi.org/10.1287/isre.1040.0032

Marini, F. ve Amigo, J. M. (2020). Unsupervised Exploration Of Hyperspectral And Multispectral Images. *In Data Handling in Science and Technology*, *32*, 93-114. https://doi.org/10.1016/B978-0-444-63977-6.00006-7

Metheny, M. (2017). *Security and privacy in public cloud computing*. Federal Cloud Computing, Federal Cloud Computing: The Definitive Guide for Cloud Service Providers içinde, Second Edition, Elsevier Inc, Syngress, ss. 79–115.

Miller, A. R. ve Tucker, C. (2009). Privacy Protection And Technology Diffusion: The Case Of Electronic Medical Records. *Management Science*, *55*(7), 1077-1093. https://doi.org/10.1287/mnsc.1090.1014

Mitchell, T. (1997). *Machine Learning*. New York: McGraw Hill.

NIST Special Publication (2013). Security And Privacy Controls For Federal Information Systems And Organizations, Revision 5, *800* (53), 8-13. https://doi.org/10.6028/NIST.SP.800-53r5

Onan, A., Korukoğlu, S. ve Bulut, H. (2016). Ensemble Of Keyword Extraction Methods And Classifiers İn Text Classification. *Expert Systems with Applications, 57*, 232–247. https://doi.org/10.1016/j.eswa.2016.03.045

Pan, S. J. ve Yang, Q. (2009). A Survey On Transfer Learning. IEEE Transactions On Knowledge And Data Engineering, 22(10), 1345-1359. https://doi.org/10.1109/TKDE.2009.191

Pavlou, P. A. (2011). State Of The Information Privacy Literature: Where Are We Now And Where Should We Go? MIS Quarterly, 35(4), 977–988. https://doi.org/10.2307/41409969

Perlich, C., Dalessandro, B., Raeder, T., Stitelman, O. ve Provost, F. (2014). Machine Learning For Targeted Display Advertising: Transfer Learning In Action. *Machine Learning*, *95*(1), 103-127. https://doi.org/10.1007/s10994-013-5375-2

Prainsack, B. (2019). Logged Out: Ownership, Exclusion And Public Value In The Digital Data And Information Commons. *Big Data & Society, 6*(1), 1-15. https://doi.org/10.1177/2053951719829773

Ren, K., Zhang, W., Chang, K., Rong, Y., Yu, Y. ve Wang, J. (2017). Bidding Machine: Learning To Bid For Directly Optimizing Profits In Display Advertising. *IEEE Transactions on Knowledge and Data Engineering*, *30*(4), 645-659. https://doi.org/10.1109/TKDE.2017.2775228

Shah, N., Engineer, S., Bhagat, N., Chauhan, H. ve Shah, M. (2020). Research Trends on the Usage of Machine Learning and Artificial Intelligence in Advertising. *Augmented Human Research*, 5(1), 1-19. https://doi.org/10.1007/s41133-020-00038-8

Shanahan, J. G. ve Kurra, G. (2011). Digital Advertising: An Information Scientist's Perspective. In *Advanced Topics in Information Retrieval* (s. 209-237). Springer, Berlin, Heidelberg.

Sharma, A., Kulkarni, S. V., Kalbande, D. ve Dholay, S. (2019). Cost Optimized Hybrid System İn Digital Advertising Using Machine Learning. *Int J Innov Technol Explor Eng*, *8*(8), 934-939.

Shiller, B., Waldfogel, J. ve Ryan, J. (2018). The Effect Of Ad Blocking On Website Traffic And Quality. *The RAND Journal of Economics*, *49*(1), 43-63. https://doi.org/10.1111/1756-2171.12218

Smith, H. J., Dinev, T. ve Xu, H. (2011). Information Privacy Research: An Interdisciplinary Review. *MIS Quarterly*, 35(4), 989-1015. https://doi.org/10.2307/41409970

Sutton, R. S. ve Barto, A. G. (2018). *Reinforcement Learning: An İntroduction*. MIT Press.

Şahin, Ü. ve Yücesoy, V. (2019). Çok Kollu Haydutlar İle Dinamik Ambulans Konumlandırma. In *27th Signal Processing and Communications Applications Conference (SIU), 2019* (ss. 1-4). IEEE.

Tesfay, W. B., Hofmann, P., Nakamura, T., Kiyomoto, S. ve Serna, J. (2018, April). I Read But Don't Agree: Privacy Policy Benchmarking Using Machine Learning And The EU GDPR. In Companion Proceedings of the The Web Conference 2018 (ss. 163-166).

Tucker, C.E. (2015). Privacy and the internet. In Handbook of Media Economics (Eds. Simon P. Anderson, Joel Waldfogel, David Strömberg), Volume 2, Elsevier B.V. pp. 541-562. https://doi.org/10.1016/B978-0-444-63685-0.00011-5

Vapnik, V. (1995). *The Nature Of Statistical Learning Theory*. Newyork: Springer-Verlag.

Vermorel, J. ve Mohri, M. (2005, October). *Multi-armed bandit algorithms and empirical evaluation.* In European conference on machine learning (ss. 437-448). Springer, Berlin, Heidelberg.

Vural, Y. (2018). Veri Mahremiyeti: Saldırılar, Korunma Ve Yeni Bir Çözüm Önerisi. *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi*, *4*(2), 21-34. https://doi.org/10.18640/ubgmd.517767

Watkins, C. J. ve Dayan, P. (1992). Q-Learning. *Machine Learning*, *8*(3), 279-292.

Weber, R. H. (2010). Internet of Things–New Security And Privacy Challenges. *Computer Law & Security Review*, 26(1), 23-30. https://doi.org/10.1016/j.clsr.2009.11.008

Wen, T. J., Chuan, C. H., Yang, J., & Tsai, W. S. (2022). Predicting Advertising Persuasiveness: A Decision Tree Method for Understanding Emotional (In) Congruence of Ad Placement on YouTube. *Journal of Current Issues & Research in Advertising*, 43(2), 200-218. https://doi.org/10.1080/10641734.2021.1963356

Westin, A.F. (1967). *Privacy And Freedom*. New York: Atheneum.

Wieringa, J., Kannan, P. K., Ma, X., Reutterer, T., Risselada, H. ve Skiera, B. (2021). Data Analytics In A Privacy-Concerned World. *Journal of Business Research*, *122*, 915-925. https://doi.org/10.1016/j.jbusres.2019.05.005

Wu, P. F., Vitak, J. ve Zimmer, M. T. (2019). A Contextual Approach To Information Privacy Research. *Journal of the Association for Information Science and Technology*, 1-6. https://doi.org/10.1002/asi.24232

Zins, C. (2007). Conceptual Approaches For Defining Data, Information, And Knowledge. *Journal Of The American Society For Information Science And Technology*, 58(4), 479-493. https://doi.org/10.1002/asi.20508

EXTENDED SUMMARY

Research Problem:

Machine learning is a branch of the computational algorithm developed by imitating people's decision-making systems by learning from a certain dataset. Shah et al. (2020) have proven that companies in different industries such as Starbucks, Dell, Ikea, Dove, and BMW that invest in certain platforms such as Facebook, Twitter, and YouTube that use artificial intelligence and machine learning techniques in advertising have achieved significant growth in gaining leads (p.12). Machine learning is also promising for the future of advertising, as it gives companies more control over advertising. However, this may result in a data privacy breach, as in the Cambridge-Analytica scandal involving Facebook. The serious challenge with these new applications of advertising is users' expectations of ensuring that their privacy rights are protected in target advertising. For this reason, the laws to be enacted in this area, the implementation of these laws, and the correct use of machine learning technologies are very effective (Shah et al., 2020, p.2).

Purpose:

The aim of the article is with the advantages of obtaining deep customer insights and serving targeted advertisements through machine learning algorithms in digital advertising, one of the most important disadvantages is to address data privacy breaches. In addition, it discusses the current techniques for resolving data privacy violations in digital advertising. Machine learning provides companies with more power to control advertisements; but the most important issue of debate is the customization of

advertisements and therefore the possibility that data privacy is compromised. This paper discusses the issue with a holistic approach by focusing on the concerns of data privacy in addition to the benefits of targeted advertisements and machine learning algorithms for businesses.

Literature Review:

Wen et al. (2022) identified the factors that increase the credibility of the advertisement, Sharma et al. (2019) reached the target audience in advertising, Kuppusamy (2018) designed an advertising perception system, Ren et al. (2017) used Machine Learning methods for the bidding algorithm.

Methodology:

This article aimed to contribute to the literature in this field by showing how machine learning algorithms are used in digital advertising and by showing that a solution to the data privacy problem can be found with the help of machine learning algorithms in the presentation of personalized advertisements.

Results and Conclusions:

There are important steps to be taken both to maintain the personalized advertising offered by machine learning algorithms and to prevent the loss of customers due to data privacy concerns. By giving consumers the ability to opt-out of online behavioural advertising, as in the American Advertising Industry's AdChoices application, they may be given notice and choice. Studies have revealed that the number of consumers who opt out of online behavioural advertising is very small, however, offering such a choice leaves a positive impression on consumers. Johnson et al. (2020). On the other hand, Almuhimedi et al. (2015) showed in a field study that a simple nudge approach on mobile devices can lead participants to change their mobile app privacy settings and align their data-sharing behaviour with their privacy preferences. To this end, privacy design must go beyond the mainstream mechanisms that protect personal data already established and instead develop creative ways to guide both individuals and organizations to preventive behaviour in a variety of contexts (Wu et al., 2019, p.4). A privacy management responsibility delegated to users becomes inefficient due to the complexity of environments and privacy attacks. Therefore, there is an urgent need to develop automated privacy management systems to help users protect their privacy. In this study, it is recommended to use machine learning algorithms in the solution to data privacy violations. As a matter of fact, in research, it has been proven that machine learning applications give effective results in the evaluation of privacy policy and user preference management (Liu et al., 2021). The main reason why machine learning algorithms are preferred is that privacy policy information is written in long and complex texts and most consumers approve this information without reading it. In the literature, machine learning algorithms have been used to convert privacy policy texts into understandable and very short texts (Tesfay et al., 2018). Another challenge in protecting user privacy is that each user has a different privacy sensitivity and preference. When installing applications, users are often asked for permission to access resources. Machine learning techniques are applied to predict user privacy preferences and aid decision-making. Research shows that providing recommendations based on clusters of like-minded users with the help of machine learning and using predictive models of people's privacy preferences increases user satisfaction (Liu et al., 2021).

It is seen that machine learning algorithms can be used to eliminate data privacy violations that occur with the use of machine learning algorithms and automatic systems in digital advertising. With the use of machine learning algorithms in the future, it is predicted that personalized advertising will progress further, and micro-marketing processes will be adopted where each individual is considered as a segment. However, it is important to use consumer data in digital advertising to configure privacy within the limits of consumer privacy by making personal data privacy settings with machine learning. Thus, it will be possible for companies to both protect profitability and prevent consumer losses due to data privacy.