ARAŞTIRMA

Geliş Tarihi: 31 Mayıs 2024
Kabul Tarihi: 16 Temmuz 2024

SEÇİM GÜVENLİĞİ BAĞLAMINDA YAPAY ZEKÂ TEKNOLOJİLERİ: GÜNCEL TARTIŞMALAR VE ÖNERİLER[1]

Artificial Intelligence Technologies In The Context Of Election Security: Current Discussions And Recommendations

DOI: 10.58307/kaytek.1492981

Furkan SAİTOĞLU[2]

Özet

Teknoloji alanında yaşanan gelişmeler, siyaset ve kamu yönetiminde de önemli değişiklikleri beraberinde getirmiştir. Özellikle dijitalleşmenin siyaset ve yönetim alanına yansıması avantajları ve dezavantajları da içerdiğinden ayrı bir öneme sahiptir. Gelişen teknolojinin siyasetin temel konusu olan seçim ve seçim güvenliğine etkisi tartışılmakta ve gelecekte de tartışılmaya devam etmesi beklenmektedir. Yapay zekâ teknolojisinin seçimlerin her aşamasında etkinliğini artırması faydalarının yanında birtakım riskleri de taşımaktadır. Çünkü seçim sürecinin adil, şeffaf ve hesap verilebilir şekilde sağlanması, siyasetin önemli bir konusudur. Seçim güvenliği, sadece sandıkların korunmasından ibaret olmayıp, seçimin başlangıcından bitişine kadar geçen süreci ifade etmektedir. Teknoloji ve siyaset tartışmasında yapay zekâ teknolojisinin hızlı ilerlemesi çok kısa zamanda siyasette bazı tehditleri de beraberinde getirmesi olasıdır. Seçim ve seçim güvenliği noktasında yapay zekânın etik şekilde kullanılmasını sağlamak için siyaset ve toplum ne yapmalı? Hangi önlemler alınmalı? Soruları önem arz etmektedir. Çünkü seçimlerin olmazsa olmaz ilkeleri olan etik, güven ve şeffaflık gereksinimi belirleyici rol oynamaktadır. Böylelikle siyaset ve toplum aktörleri yapay zekâ teknolojilerinin kötüye kullanılmaya hangi noktalarda açık olduğunu bilmesi zorunluluğu ortaya çıkmaktadır. Çalışmanın amacı yapay zekâ teknolojisinin seçim ve seçim güvenliği sürecinde yansımalarının nasıl olduğu, neye yol açtığı veya açabileceği, avantajları ve dezavantajlarının neler olduğunu, seçim güvenliğinde etik ve şeffaf anlayış çerçevesinde yapay zekânın etkilerini güncel tartışmalar üzerinden incelemektir. Ayrıca ek olarak Türkiye'de yapay zekâ teknolojisinin olası seçimlere yansıması ve ortaya çıkması muhtemel etik ve şeffaflık gereksinimi sorunlarına karşı nasıl reaksiyon vereceği üzerine çözüm önerileri sunmaktır. Bu çalışmada literatür taraması tercih edilmiştir. Sonuç olarak bu çalışma; yapay zekâ teknolojisinin seçim ve seçim güvenliğine yansımasını ele alarak, literatürde yeni ve eksik kalan alana katkı sunması beklenmektedir.

Anahtar Kelimeler: *Seçim, Seçim Güvenliği, Teknoloji, Yapay Zekâ.*

Abstract

The developments in the field of technology have brought about significant changes in politics and public administration. Especially the reflection of digitalisation on politics and administration is of particular importance as it includes advantages and disadvantages. The impact of developing technology on elections and election security, which is the main subject of politics, is being discussed and is expected to continue to be discussed in the future. Increasing the effectiveness of artificial intelligence technology at every stage of elections carries some risks as well as benefits. Because ensuring a fair, transparent and accountable election process is an important issue in politics. Election security does not only consist of the protection of ballot boxes, but also refers to the process from the beginning to the end of the election. In the discussion of technology and politics, the rapid progress of artificial intelligence technology is likely to bring some threats in politics in a very short time. What should politics and society do to ensure the ethical use of artificial intelligence in terms of election and election security? What measures should be taken? The questions are important. Because the need for ethics, trust and transparency, which are the indispensable principles of elections, play a decisive role. Thus, it is imperative for political and social actors to know at which points artificial intelligence technologies are open to misuse. The aim of the study is to examine how artificial intelligence technology is reflected in the election and election security process, what it causes or may cause, what its advantages and disadvantages are, and the effects of artificial intelligence within the framework of ethical and transparent understanding in election security through current debates. In addition, it is also to offer solutions on how artificial intelligence technology in Turkey will react to the possible reflection of artificial intelligence technology on possible elections and how it will react to the problems of ethics and transparency requirements that are likely to arise. Literature review is preferred in this study. As a result, this study is expected to contribute to the new and missing field in the literature by addressing the reflection of artificial intelligence technology on election and election security.

Keywords: *Elections, Election Security, Technology, Artificial Intelligence*

1 Bu makale 16-18 Mayıs 2024 tarihleri arasında Tunceli'de düzenlenen 24. Uluslararası Kamu Yönetimi Forumu'nda (KAYFOR24) aynı başlıkla sunulan ve özeti KAYFOR24 bildiri özet kitabında yer alan bildirinin tam metin hâlidir.

2 Öğr. Gör., Hatay Mustafa Kemal Üniversitesi, Kırıkhan Meslek Yüksekokulu, Yönetim ve Organizasyon Bölümü, furkan.saitoglu@gmail.com, ORCID: 0000-0001-6915-8189

1. GİRİŞ

Yapay zekâ teknolojisi mühendislik, bilişim ve sağlık alanında olduğu kadar siyaset ve kamu yönetiminde de büyük öneme sahip olup, ilgi görmektedir. Ancak gelişen teknoloji ve yapay zekâ uygulamalarının seçim güvenliğinde önemli rol oynaması noktasında ulusal yazın alanında yeterli seviyede bir çalışma bulunmamaktadır. Uluslararası alanda bazı araştırmacılar da çalışmaların yeterli olmadığını yönünde kaygılarını dile getirmiştir. Yapay zekâ destekli sosyal medya ve diğer uygulamaların seçim sürecine ve seçim güvenliğine etkilerinin anlaşılması için daha fazla araştırma yapılması gerektiğini belirtmiştir. Günümüzde bazı devletler, teknoloji firmaları, siyasi partiler ve adaylar, yapay zekâ teknolojisini kullanmakta, seçim süreci içinde seçmenlerle etkileşime geçerek vatandaşın politik kararlarını, tercihlerini iyi veya kötü yönde değiştirme gibi davranışlar sergilemektedir.

Teknolojinin gelişmesi seçim süreçlerinin (seçim öncesi-seçim günü-seçim sonrası) yapısını değiştirmiştir. Örneğin, dijital seçimler, e-oylama, dijital oy sayımı, yapay zekâ destekli seçim kampanya süreçleri, sosyal medya algoritmaları, sohbet robotları seçim ve seçim güvenliğinin seyrini doğrudan etkileyebilecek potansiyele sahip kavramlar olarak karşımıza çıkar. Dijitalin ve yapay zekâ teknolojisinin seçim sürecine olumsuz etkisi, demokratik değerlerin korunmasını mecbur kılmaktadır. Bireylerin seçme ve seçilme haklarını eşit, adil ve güven içinde kullanması, demokrasinin olmazsa olmazıdır. Seçmen tercihleri ve bu tercihlerin sandığa yansımasının sonucu arasındaki her türlü kötü niyetli girişim, seçimlerin güvenliğini tehlikeye sokacak, seçimlerin meşruluğunu tartışmaya açık hale getirecektir. Seçim güvenliği olgusunun, seçmenler, siyasi aktörler ve devlet arasındaki yönetişimin bilgi teknolojileri konusunda başarılı bir şekilde sistematize edilmesi bu tartışmayı ortadan kaldırabilir.

Bu çalışma sekiz bölümden oluşmaktadır. Araştırmaya giriş yapıldıktan sonra ikinci bölümde yapay zekâ ve seçim güvenliğinin kavramsal çerçevesinden bahsedilmektedir. Üçüncü bölümde yapay zekânın seçim güvenliğine etkisi üzerinde durulmuştur. Dördüncü bölümde yapay zekânın Türk seçim sistemine yansımaları hukuki, siyasi ve kurumsal boyutuyla ele alınmıştır. Beşinci bölümde yapay zekâ, etik ve şeffaflık anlayışı ihtiyacı çerçevesinde incelenmektedir. Altıncı bölüm, yapay zekânın seçim güvenliğine olan tehdidi demokrasinin etkisizleşmesi bağlamında ele alınmıştır. Yedinci bölümde ise yapay zekâ ve seçim güvenliğine yönelik düzenlemeler, tartışmalar ve öneriler genel hatlarıyla ele alınmıştır. Son olarak sekizinci bölümde ise sonuçlar ve öneriler sunulmuştur.

2. KAVRAMSAL ÇERÇEVE

Bu bölüm, teknolojik dönüşüm aracı olarak "yapay zekâ"yı ve demokrasinin olmazsa olmazı olarak bilinen "seçim güvenliği" ilkesini kavramsal bir yaklaşımla incelemekte, ayrıca yapay zekânın günümüze nasıl geldiği sorusundan hareketle yapay zekâyı tarihsel bir yaklaşımla ele almaktadır.

2.1. Teknolojik Dönüşüm Aracı: Yapay Zekâ ve Kısa Tarihi

Yapay zekâ, multidisipliner yaklaşıma sahip bir alan olduğu için genel ve tek bir tanımı bulunmamaktadır. Ancak yapay zekâ ile ilgili yine de bazı tanımlamalar yapılmıştır. Bu tanımlarda yapay zekâ *"zeki bilgisayar programları yapma mühendisliği"*; *"düşünme, anlama, eyleme dökmeyi sağlayacak bilgi işleme çalışması"*; *"insanların yaptıklarını bilgisayarlara yaptırılabilme faaliyeti"* ve *"akıllı davranış üzerine bir çalışma"* olarak açıklanmıştır (Özsalih, 2023: 535).

Başka bir deyişle yapay zekâ, makinelerin (bilgisayar, robot, akıllı aygıtlar vb.) akıllı hareket yeteneklerini ifade eder. Yani, makinelerin insan etkisi olmadan, kendi başına hareket edebileceğini ve öğrenebileceğini açıklamaktadır. En temel şekliyle yapay zekâ, kalıpları belirlemek, ne yapacağına karar vermek ve gelecekteki neticeleri tahmin etmek amacıyla bir algoritmayı (problem çözme kuralı veya hesabı) verilere uygulamaktır (Marr, 2022: 30). Diğer bir tanımda yapay zekâ, insana ait davranışlar gösterebilen makinelerin ve robotların geliştirilmesine imkân veren yeni bir iletişim teknolojisidir. Tahminler, öneriler ve kararlar alma, farklı verileri işlemek için insani düşünme kabiliyetini ve makine zekâsını kullanan teknolojidir (Kavut, 2024: 327).

Yapay zekâ bütünüyle veriye bağlı bir olgudur. Kısaca veri; yapay zekânın yakıtıdır. Dijitalleşmenin artmasıyla her zamankinden daha fazla veriye ulaşılabilmekte, böylece yapay zekânın kısa sürede daha akıllı, hızlı ve etkin hale gelmesini sağlamaktadır. Verilerin çoğalması sayesinde "büyük veri" oluşmakta ve yapay zekânın gıdası rolünü üstlenen yapay zekâ adından sıkça söz ettirmeyi başarmıştır (Marr, 2022: 44-45). Peki, yapay zekâyı bu denli önemli kılan nedir? Sorusuna yanıt olarak: alışkanlıkları, iş yapmayı dönüştürme potansiyelinin olması, sosyo-ekonomik ve uluslararası alandaki işleyişin kurallarını baştan aşağıya değiştirerek yeni fırsatlar ve tehditler ortaya çıkarmasıdır. Ayrıca bilginin öneminin artması ve toplumsal gereksinimlerin dönüşümü yapay zekâyı daha önemli hale getirmiştir (Aydın, 2023: 75-79).

Peki, yapay zekâ bu noktaya nasıl geldi? Yani yapay zekânın tarihsel arka planında neler var? Sorusuna değinmekte yarar vardır. Bir makinenin yaşayan bir canlı kadar akıllı olduğu fikrinden yola çıkan John McCarthy ve Alan Turing makine öğreniminin atası kabul edilir. Yapay zekânın gelişme hızı, derin öğrenme teknolojisi ve sinir ağları gibi yapay zekânın diğer alt birimleri ile kültürü ve insanların fırsatlarını da etkilemiştir (Basnet, 2022: 4). Aslında yapay zekâ yeni bir olgu değildir. Akıllı makineler oluşturma fikri, uzun

zamandır tartışılan bir durumdur. ABD'li bilgisayar bilimcisi John McCarthy 1955'te Darmounth Kolejinde bir yapay zekâ atölyesi açmayı tavsiye ederken "yapay zekâ" kelimesini ilk kez ortaya atmıştır. Tavsiyesinin sonucunda dünyanın ilk yapay zekâ konferansı (1956, Darmounth Konferansı) toplanmıştır. Bu yıldan itibaren akıllı makineler birçok alanda ortaya çıkmıştır. Öte yandan ilk yapay zekâ sinir ağları 1950 yılında, yapay zekâ alanındaki önemli engelleri aşmak için geliştirilmiştir. İnsan zekâsının süreçleriyle (algılama, yorumlama vb.) yarışacak durumda olmaması yapay zekânın gelişim seyrini etkilemiş olup, yapay zekânın tıpkı insanlar gibi olması beklenenden fazla zaman almıştır (Marr, 2022: 43-44). Yapay zekâ araştırmaları 1940'lı yıllarda başlamış olup, 2010'lu yıllardan sonra yapay zekâya ilginin arttığını söylemek mümkündür. Yapay zekânın gelişim seyrini etkileyen üç temel unsur bulunmaktadır. Bunlar; (1) büyük veri kaynakları, (2) makine öğrenimi, (3) bilgisayar işlem gücüdür (Sayler, 2020: 2). Bu üç temel unsurun tamamlanmasıyla yapay zekâ teknolojisi istenilen sıçramayı yapmıştır.

2.2. Demokrasinin Teminatı: Seçim Güvenliği

Seçim güvenliği kavramına değinmeden önce güvenlik olgusunu tanımlamak gerekir. Genellikle tehdit ve risk temelli bir kavram olan güvenlik; olan ve olması muhtemel tehlikeler ile sahip olunan değerlerin belirlenmesi ve korunması üzerine odaklanmıştır. Kısaca güvenlik, değerlerin korunması olarak tanımlanabilir. Bu açıdan bakıldığında seçim güvenliği, "seçime ilişkin değerlerin korunması"dır. Seçim güvenliği; adayların, sandığın, seçmenin ve seçmen tercihinin güvenliğini (yani seçmenin hür şekilde iradesini sandığa yansıtması) barındıran geniş bir yelpazedir. Eskiden seçim güvenliği denilince yalnızca oy ve sandık güvenliğinin sağlanması, adayın fiziki güvenliği, seçimlere hile karıştırılmaması için sandıkların ve oy pusulalarının güvenliği ve seçim gününün güvenliğinde merkezi bir güvenlik yaklaşımının egemen olduğu bir anlayış bulunmaktaydı. Ancak seçime ilişkin değerlerin korunması sadece günübirlik önlemlerin alındığı bir güvenlik türü olmayıp, seçmenin siyasi iradesini özgürce kullanması önemli bir değer olduğundan seçmen tercihinin güvenliği de seçim güvenliği kapsamındadır (Beren, 2013: 197-199).

Demokrasinin olmazsa olmaz unsurlarından biri de seçimlerdir. Halkın iradesinin yansımasının temel şartı, seçimlerin hür ve adil bir ortamda yapılmasıdır. Baskı ortamı ya da eşitsiz ortamda yapılan seçimlerin gerçeği yansıtması beklenemez, meşruluğunu tartışmaya açık hale gelir. Bu açıdan sağlıklı bir seçim süreci seçimlerin güvenli bir ortamda yapılmasından geçmektedir. Seçmenin tercihini etkilemeye yönelik olumsuz bütün durumlar demokrasinin teminatı noktasında seçim güvenliğine tehdit oluşturmaktadır. Diğer yandan seçim süreci; seçim öncesi, seçim günü ve seçim sonrası gibi geniş kapsamlı bir süreçten oluşur. Klasik dar kapsamlı seçim güvenliği (seçim malzemelerinin, adayların ve oyların fiziki güvenliği) anlayışından, küreselleşme ve teknolojik değişimlerle beraber geniş kapsamlı bir seçim güvenliği (adayların, siyasi partilerin,

seçmenlerin tercihlerinin, seçim sonuçlarının, seçim görevlilerinin, medya ve gözlemci vb.) anlayışına geçildiği söylenebilir (Aydın ve Karaşahin, 2023: 18-19). Hızla gelişen teknoloji değişimi beraberinde getirmiş; akıllı makineleri, yapay zekâyı siyaset, seçim süreci ve seçim güvenliğine dâhil etmiştir.

Örneğin, günümüzde yaşanan teknolojik gelişmeler birbirinden farklı teknolojik oylama tekniklerini ortaya çıkararak oylama sürecini daha kolay hale getirmiştir. Uygulamada az olmakla birlikte e-posta veya dijital ortamda oy kullanılması yöntemleri bulunmaktadır. Ancak bu durum güvenlik açıklarını ve risklerini, fiziksel tehdit, dışarıdan müdahale edilmesi gibi birtakım güvenlik tehlikesini de içinde barındırmaktadır (Aydın ve Karaşahin, 2023: 20). Genel olarak seçim güvenliği sadece oylama tekniklerini, sandıkların korunmasını içermeyip çok daha geniş kapsamlı bir süreçtir. Özellikle gelişen yapay zekâ teknolojisi "seçmen tercihlerinin güvenliği", "seçim sonuçlarının güvenliği" gibi modern seçim güvenliği ilkeleri açısından önemlidir.

3. YAPAY ZEKÂNIN SEÇİM GÜVENLİĞİNE ETKİSİ

Yapay zekâ, siyaset ve kamu yönetimi kadar seçim ve seçim güvenliğini de etkilemiştir. Örneğin, büyük veri ve yapay zekânın kullanılması sosyolojik görüntünün belirlenmesi, olası senaryoların oluşturulması ve çeşitli simülasyonların geliştirilmesine zemin hazırlamıştır (Kurnaz, 2023: 1). Ayrıca yapay zekânın doğru kullanılması ülke kalkınması için de oldukça önemlidir. Buradan hareketle, Ted Nelson'un "Bilgisayarın iyi yanı, siz ne derseniz onu yapıyor. Kötü yanı ise, siz ne derseniz onu yapıyor." sözü dijitalleşmenin hangi niyetle kullanıldığını ortaya koyması açısından değerlidir. Öte yandan Kurnaz (2023, 1); dijital siyaset aygıtlarının genelde kötü niyetli unsurlarca daha etkin kullanıldığını, fakat bunların iyi niyetli unsurlarca doğru ve verimli kullanılabileceği sistemlerin oluşturulmasının ve işletilmesinin demokrasinin geleceği bakımından daha önemli olduğunu ifade etmiştir.

Günümüzde akıllı telefonlar ve cihazlar sayesinde, vatandaşların kişisel verileri kaydedilmekte ve seçmen tercihlerinin görüntülenmesi yapılmaktadır. Bu konuda yapay zekâ teknolojisi için önemli olan şey, veri ve daha fazla verinin elde edilmesidir. Yapay zekâ destekli akıllı cihazlar aracılığıyla, seçmenlerin siyasi ve ideolojik tercihlerini analiz etmek için veri, ses ve görüntüye erişim izni verilmektedir. Ancak yapay zekânın, seçmen tercihlerine kişinin rızası olmadan kolayca ulaşabilmesi, seçmen tercihlerinin güvenliğini etkileyebilir.

Yapay zekânın seçmen tercihi güvenliğine etkisine bazı ilginç örnekler verilebilir. Örneğin, uydu görüntüleri yoluyla bir mahallede bulunan araç türlerinden siyasi tercih tahmini yapılarak sedan aracın yoğun olduğu mahallelerde demokratların, kamyonet tarzı araçların yoğun olduğu bölgelerde cumhuriyetçilerin olduğu tespit edilmiştir. Başka bir örnek ise, güneş enerjisi taktıran vatandaşların çevre hassasiyeti fazla olan sol görüşlü

kişilerden oluştuğunu belirlemiştir. Öte yandan seçim kampanyası süreçlerinde Cambridge Analytica ya da HaystagDNA gibi veri analitiği şirketlerince seçmen profillemeleri için büyük miktarlarda bütçe ayrılmıştır. Vatandaşların çevrimiçi siyasi anketlere verdiği cevaplar, beğendiği araç markaları, takip ettiği TV programları veya kahve zevklerinden yola çıkarak seçmen görüntülemesi yapıldığı bilinmektedir. Tüm bu verilerin yardımıyla vatandaşların siyasi yönelimleriyle ilgili önemli emareler ortaya çıkmaktadır. Ayrıca, bu veriler siyasal partiler kadar yabancı devletlerin ve çıkar gruplarının terör organizasyonlarının da ilgisini çektiği bir alan olarak hem seçim güvenliğini hem de ulusal güvenlik açığına yol açmaktadır (Kurnaz, 2023: 11-17).

Yapay zekâ ve veri analizi yöntemleri; seçim kampanyalarının şekillenmesi, seçmen davranışı analizi, seçim sonuçları, seçmen tercihlerinin tahmini ve seçim propagandası araçlarının geliştirilmesinde rol oynamaktadır. Bu rol, siyasi aktörlerin seçmenlere ulaşma, tercihlerini analiz etme ve mesajlarını kişiselleştirme imkânı sağlamaktadır. Ancak yapay zekâ ve uygulamalarıyla ilgili etik kaygıların olması, veri gizliliğinin ihlali gibi konular seçimlerin adil ve şeffaf şekilde gerçekleşmesine olanak vermemektedir (Kırık ve Özkoçak, 2023: 412-428).

Yapay zekâ, seçim öncesi algıyı yönlendirmek için kurgulanmış haber düzeni ve dolaylı sansür gibi yöntemlere başvurabilir. Yapay zekânın gelişmiş algoritmaları, seçmenin kararını değiştirmek veya yanıltıcı, yanlış bilgi vermek amacıyla yönlendirdiği söylenebilir. Örneğin, Cambridge Analytica skandalında Facebook, kararsız olan seçmenleri reklam ve çeşitli kampanyalar yoluyla kendi platformu üzerinden manipüle etmeye imkân tanımıştır. Yapay zekâ, kararsız seçmenleri tespit ederek bu seçmen kitlesini yanlış ve yalan haberlerle etkileyebilir. Bu noktada seçim güvenliği ve yapay zekânın önemi "zekâ yapay ama seçim gerçek" ifadesiyle özetlenebilir. Bu ifade, yapay zekânın kötü amaçlarla kullanılması durumunda ülkenin politik ve sosyolojik kaderini derinden etkileyeceğini göstermektedir.

Yeni Zelanda, Japonya gibi ülkelerde aday olarak seçime katılan yapay zekâ teknolojisi özellikle seçmen kitlelerinin analizinde kullanılmaktadır. Ancak, bu noktada yalan haber ve seçim güvenliği en önemli tartışma konusudur. 2016'daki ABD seçimleri ve 2020'deki İngiltere'nin Brexit oylaması gibi kritik süreçlerde sahte ve bot hesapların oluşturduğu manipülatif durumun yapay zekâ desteğiyle daha fazla olması beklenmiş, bu konuda alınabilecek tedbirler için yine yapay zeka teknolojisinden faydalanılması istenmiştir. Deepfake[1] teknolojisiyle sahte video içerikler manipülatif bilgileri saniyeler içinde sahte hesaplar yoluyla hızla yaymaktadır. Ancak paylaşım trafiğinin ve sahte hesapların belirlenmesi için yapay zekâdan yararlanılması mümkündür. Büyük verinin analiz edilmesinde kullanılan yapay zekâ teknolojisinin sağladığı imkânların aynı zamanda dezenformasyona karşı mücadelede önemli katkılar sunacağı ifade edilmiştir

1 Deepfake, derin öğrenme ve sahte kelimelerinden türetilmiş bir terimdir ve mevcut bir görüntü veya videoda yer alan bir kişinin görüntüsünün değiştirildiği teknolojiyi ifade eder.

(Epnext.com, 2023). Siyaset alanında kritik bir dönüm noktası olarak bilinen seçim ve seçim güvenliğinin dünyanın her yerinde önemli olduğu, seçmen ve siyasi taraflar nezdinde güven sorunu yaşandığı bilinmektedir. Burada şöyle bir paradoks bulunmaktadır: Seçim güvenliğindeki başlıca aktör yapay zekâdır. Yapay zekâ, iyi ve kötü, doğru ve yanlış içerir. Deepfake teknolojisinin kolay erişilebilirliği ve çevrimiçi platformlarda hızla yayılan içeriklerin demokratik katılımı tehdit ettiği düşünülmektedir. Deepfake içeriklerinin kaynağı ve doğruluğu şüpheli olduğu için, içeriklerin demokrasinin işleyişini bozabileceği endişesi vardır. Bu nedenle, hükümetler, vatandaşlar ve bilim insanları bu algıyı anlamak ve buna karşı önlem almak konusunda motive olmaktadır (Karakoç ve Zeybek, 2022: 61-63).

Deepfake teknolojisiyle manipülatif paylaşımlar yapılması, siyasiler arasında haksız rekabete yol açabilir; seçmenlerin güvenliği sahte içeriklerle yönlendirilerek toplumsal infial yaratılabilir. Örneğin, siyasi bir aktörün ses ve görüntüsü deepfake teknolojisi kullanılarak, diğer bir rakip siyasi aktörün politik arenadan silinmesine veya itibarının zedelenmesine neden olabilir. Deepfake teknolojisiyle toplumda söz sahibi veya önemli bir siyasi figürün açıklamaları, toplumsal kutuplaşma ve ayrımcılığı körükleyecek şekilde değiştirilerek olumsuz durumlara yol açabilir.

Yapay zekâ ile yapılan politik deepfake'ler, seçmenlerin gerçeklerden uzaklaşarak ayırt etme yeteneğine darbe vurmaktadır. Gerçekten de dezenformasyon, seçmenlerin demokratik kurumlara olan güvenlerini sarsmaktadır. Seçimlere bağlı dezenformasyon genellikle siyasi muhalifleri sindirme, oylama sürecini manipüle etme, seçmenlerin reklamlarla küçük ölçekli hedeflenmesi, siyasi rakiplerin e-posta vb. sosyal platformlarının hacklenmesi, seçim altyapısına yönelik siber saldırı yapılması, yabancı devletlerce sistem karşıtı aktörlere destek verilmesi ya da seçimin yapıldığı siyasi şartlara yönelik algı ve düşünceleri değiştirmek için kasten yanlış bilgilerin yayılması seçim güvenliğini ve seçmenlerin demokratik kurumlara olan güvenini ciddi anlamda etkilemektedir (Aydın ve Karaşahin, 2023: 27-28).

Yapay zekâ teknolojisi, seçimlere veri güvenliği ve hızını artırma konusunda katkı sağlayabilir. Manipülasyon ve hileli oy kullanımı gibi seçim hilelerini önlemeye yardımcı olabilir. Ayrıca, e-seçimlerin katılımı artırarak seçmenlere istedikleri yerden oy kullanma özgürlüğü verebilir. Şeffaflık ve denetlenebilirlik artırılarak, herkesin görebildiği ve takip edebildiği bir kayıt sistemi oluşturulabilir. Böylece adil koşullarda seçim yapılması sağlanır ve olası sorunların tespit edilmesi kolaylaşır. Özetle, yapay zekâ seçim sürecini daha güvenilir, şeffaf ve katılımcı hale getirebilir (Kırık ve Özkoçak, 2023: 424).

4. YAPAY ZEKÂNIN TÜRK SEÇİM SİSTEMİNE YANSIMALARI

Demokratik toplumlarda seçim güvenliği ve dezenformasyon ilişkisi ana hatlarıyla anayasalarda ortaya konulan hükümlerce, uygulamaya dönük yasalar etrafında biçimlenmiştir. Bu doğrultuda 1982 Anayasası'nın 67, 77, 78, 79, 101, 106, 116 ve 127. maddelerinde Cumhurbaşkanlığı, milletvekili, yerel yönetimler seçimi ve halkoylamasına ilişkin olarak temel çerçeve belirlenmiştir. Seçimlerin uygulanmasına yönelik olarak, 6271 Sayılı Cumhurbaşkanı Seçimi Kanunu, 2839 Sayılı Milletvekili Seçimi Kanunu, 2972 Sayılı Mahalli İdareler İle Mahalle Muhtarlıkları ve İhtiyar Heyetleri Seçimi Hakkında Kanunu, 2820 Sayılı Siyasi Partiler Kanunu ve 298 Sayılı Seçimlerin Temel Hükümleri ve Seçmen Kütükleri Hakkında Kanunlar bağlamında şekillenmiştir. Ayrıca, 5651 sayılı "İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun" ise içerik, yer ve erişim sağlayıcılar yoluyla işlenen suçlarla mücadele etme ve 5237 sayılı Türk Ceza Kanunu'nun hukuksal tedbirler aldığını söylemek mümkündür. Bu düzenlemelerle genel olarak dezenformasyon özel olarak ise seçim güvenliği ve dezenformasyon ilişkisine uygulanabilecek farklı yasalardır (Aydın ve Karaşahin, 2023: 29-34). Ülkemizde, seçim sürecindeki dezenformasyona ve manipülasyona karşı 2022 tarihli 7418 sayılı "Basın Kanunu ile Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun", 2007 tarihli ve 5651 Sayılı "İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanunda Değişiklik Yapılmasına Dair Kanun" ile 2020 tarihli ve 7253 sayılı "İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanunda Değişiklik Yapılmasına Dair Kanunlar yoluyla karşı koymaktadır. Yasalara özetle bakıldığında, sosyal ağ sağlayıcılarına düzenleme getirilmiş; halkı yanıltıcı bilgiyi açıkça yaymak suç kabul edilmiştir. Sonradan yapılan kanunların şekli ve maddi yapısının açıklanması zor olgular içermesi tartışmaları beraberinde getirmiş; basına sansür yasası, ayrıcalıklı hukuk, yargıya siyasi baskı, davalarda sosyal medya mahkemesi gibi ifadelerle anılmasına yol açmıştır. 7418 sayılı yasa mevcut haliyle yalan ile ilgilendiği için gerçeğin silahlaştırılması yönünün eksik kaldığı ifade edilmiştir. Türkiye'nin hassas dinamiklerinin olması (etnik, din, kültürel, jeopolitik vb.) gerçek sorunlar üzerinden sosyal kopuşa yol açma tehlikesini barındırmaktadır (Aposto.com, 2024).

Yapay zekâ teknolojisinin ülkemizde kurumsal bir yönü de bulunmaktadır. Özellikle yapay zekâ altyapısını geliştirme, dijitalleşme alanında etkinlik sağlama gibi olumlu gelişmelere yönelik durumların yanında; risklere, tehlikelere karşı dezavantajlı konulara karşı da stratejiler ve politikalar üretme niyetini de bulunmaktadır. Örneğin, yapay zekâ teknolojisi konusunda Cumhurbaşkanlığı hükümet sistemiyle kurulan "Dijital Dönüşüm Ofisi"ne bazı görevler verilmiştir. Bunlar; "bilgi güvenliğini ve siber güvenliği artırıcı projeler geliştirmek", kamuda büyük veri ve gelişmiş analiz çözümlerinin etkin kullanımına yönelik stratejiler geliştirmek, uygulamalara öncülük etmek ve koordinasyonu sağla-

mak, "kamuda öncelikli proje alanlarında yapay zekâ uygulamalarına öncülük etmek ve koordinasyonu sağlamak"tır. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi'nin hizmet birimleri arasında yer alan "Siber Güvenlik Dairesi Başkanlığı", ulusal siber güvenlik ve bilgi güvenliğini destekleyici projelerin yanı sıra siber güvenlikle ilgili politika ve strateji geliştirme görevlerini üstlenmiştir. "Büyük Veri ve Yapay Zekâ Uygulamaları Dairesi Başkanlığı" ise, kamuda büyük veri ve yapay zekâ uygulamalarını geliştirmek, projelere öncülük etmek, büyük veri analitiği, güvenliği ve mahremiyeti konularında çalışmalar yapmak gibi görevleri içermektedir (cbddo.gov.tr). Diğer bir kurum olan YSK'nın seçimlerin genel yönetimi ve denetiminden sorumlu önemli birimleri bulunmaktadır. Bilişim Teknolojileri Daire Başkanlığı ve bu başkanlığa bağlı Ağ Yönetimi ve Güvenliği Müdürlüğü, Donanım ve Teknik Destek Müdürlüğü, Sistem Yönetimi Müdürlüğü gibi birimler bulunmaktadır. Ayrıca Bilgi Güvenliği Kalite ve Denetim Daire Başkanlığına bağlı olarak İç Denetim Risk ve Kalite Kontrol Müdürlüğü ile Siber Güvenlik ve Siber Olaylara Müdahale Müdürlüğü de yer almaktadır. Yazılım Geliştirme ve Dijital Dönüşüm Daire Başkanlığı ve alt birimlerinden E-Devlet ve Dijital Dönüşüm Müdürlüğü, Yazılım Geliştirme Müdürlüğü bulunmaktadır (ysk.gov.tr). Diğer bir kurum ise, Cumhurbaşkanlığı İletişim Başkanlığı'dır. İletişim Başkanlığının hizmet birimleri arasında yer alan "Stratejik İletişim ve Kriz Yönetimi Dairesi Başkanlığı"nın görevlerinden biri de "Türkiye Cumhuriyeti'ne karşı yürütülen psikolojik harekât, propaganda ve algı operasyonu faaliyetlerini belirleyerek her tür manipülasyon ve dezenformasyona karşı faaliyette bulunmak"tır. Bunun yanında İletişim Başkanına doğrudan bağlı olan "Dezenformasyonla Mücadele Merkezi"; sahte ve yalan haber içeriklerine karşı kamuoyunu aydınlatmayı misyon edinmiş; ayrıca dezenformasyon bültenleri yayımlayarak bülteni iddia-hakikat ekseninde incelemektedir (iletisim.gov.tr).

Seçim güvenliği açısından ülkemizde mükerrer oy kullanımını engellemek için eskiden mavi mürekkep kullanılıyordu. Günümüzde ise bu uygulamanın tekrar kullanılıp kullanılmaması tartışmalıdır, çünkü teknolojik gelişmelerin hızla ilerlediği bir ortamda doğruluğu açıklamaya ihtiyaç duyar. Akıllı makineler ve yapay zekâ teknolojisi sayesinde seçim süreci öncesi, seçim günü ve sonrası gibi süreçlerin etkin bir şekilde kullanılması, bu tür eski moda uygulamaların kaldırılmasını sağlayacaktır.

Ülkemizde seçim günü ve seçim sonrasında dijital oy veya yapay zekâ teknolojisi doğrudan kullanılmamaktadır. Ancak seçim öncesi propaganda amacıyla sahte haberler ve içerikler, kurgulanmış görseller ve sesler genel ve yerel seçimlerde kullanıldığı bilinmektedir. Bu durum, siyasetçiler ve seçmenler için güvenlik açısından tehlike oluşturur. Örneğin, 2023 yılında Cumhurbaşkanlığı ve TBMM seçimlerinde araştırma yöntemleri belirsiz anketler, dijital siyasi mikro hedefli kampanyalar, sahte haberler ve yanıltıcı içeriklerin sosyal medya ve servis sağlayıcı reklamları aracılığıyla büyük ölçekte uygulandığı söylenebilir. Yapay zekânın bazı ücretsiz uygulamalar içermesi, erişimini kolaylaştırmıştır. Bu da kurgusal kampanyalar ve videolarla siyasi adaylara karşı seçmenlerin

düşüncelerini yönlendirme amacını taşımaktadır. Yerel seçimlerde de, dezenformasyonun deepfake videolar ve sahte haberlerle gerçekleştirildiği söylenebilir. Bu noktada, bahsedilen koruyucu yasaların sahte ve yanıltıcı içerikler üreten ve yayınlayan herkese uygulanması gerekmektedir. Yetkili devlet organları, demokrasiyi ve toplumun huzurunu korumak için bütün siyasi partilere ve adaylara yönelik dezenformasyon eylemlerine karşı çıkmalıdır (Aposto.com, 2024). Ayrıca, DİSK, KESK, TTB ve çeşitli sivil toplum kuruluşları tarafından oluşturulan Seçim Güvenliği Platformu, seçim öncesi dönemde sansür, yasak ve yapay zekâ teknolojisinin kasıtlı olarak seçmenleri yönlendirmesine karşı bir oluşum başlatmıştır (Gazetenisan, 2022). Ayrıca, Türkiye'de sahte haberlerin doğruluğunu araştırmak için bazı web siteleri bulunmaktadır. Bunlardan bazıları şöyledir: teyit.org, doğrula.org, gununyalanlari.com'dur. Bu tür siteler, sosyal medyada paylaşılan şüpheli haberlerle ilgili araştırma yapar ve haberlerin sahte olup olmadığını vatandaşlara duyurur (Özsalih, 2023: 541).

14 Mayıs 2023 tarihinde yapılan Türkiye genel seçimleri, internet ve sosyal medyanın etkisi altında kalmıştır. Yapay zekâ destekli sosyal medya algoritmalarına yönelik eleştiriler gelmiştir. Bu algoritmalar, vatandaşlara kişiselleştirilmiş içerikler sunmuştur. Yapay zekâ destekli algoritmaların Türk seçmeni etkilediği ve Türkiye'de bazı hesap ve içeriklere sansür uyguladığı belirtilmiştir. Özellikle Twitter'ın iktidar yanlısı hesap ve etiketleri gizlemek için tedbir aldığı ifade edilmiştir. Ayrıca slogan etiketlerin spam olarak değerlendirilerek gündemde geriye düşmesine engel olduğu ve muhalif içeriklerin daha ön plana çıktığı belirtilmiştir. Terör yanlısı hesapların da kasıtlı şekilde Twitter'ın "Sana Özel" ve "Takip Edilenler" algoritmalarında kullanıldığı ifade edilmiştir. Ancak bazı yayıncı kuruluşlar, herhangi bir müdahale olmadığını belirtmiştir. Sosyal medya kullanıcılarından bazıları, kullanılan bu algoritmaların sunduğu içeriklerin yönlendirici olduğunu belirtmiştir. Genel seçim sürecinde Millet İttifakı adayı Kemal Kılıçdaroğlu'nun sosyal medya üzerinden yaptığı açıklamada, internetin karanlık dünyasıyla ilişkilendirildiğini iddia ederek İletişim Başkanı ve ekibini suçlamıştır. İletişim Başkanı ise bu iddiaları reddetti ve iftira olarak değerlendirmiştir. Bu seçim sürecinde deepfake ve yapay zekâ teknolojisinin etkisi görülmüştür. Millet İttifakı adayı Kemal Kılıçdaroğlu, Rusya'nın seçimlere derin sahte içeriklerle müdahale ettiğini sosyal medya üzerinden mesajla duyurmuştur. Cumhurbaşkanı Erdoğan ise İstanbul'daki bir mitingde bu iddiaları yalanlamış, eleştirmiştir. Bunun yanı sıra her iki Cumhurbaşkanı adayının deepfake yöntemiyle hazırlanan sahte videolarının gündeme gelmesi, sosyal medyada büyük etki göstermesi yapay zekâ destekli deepfake videoların gücünü ve potansiyel risklerini gözler önüne sermiştir. Ülkemizde son genel seçimde yapay zekâ farklı alanlara da yansımıştır. Oy Birliği Platformu; ilk defa çalışmalarını yapay zekâ ile uyumlaştırmıştır. Hatalı oy kullanımını önlemek amacıyla yapay zekâ asistanıyla seçmenlere ve müşahitlere eğitim verme, yine bu teknolojiyi kullanarak hazırlanan eğitim videolarıyla seçmenlerin sandığa daha bilinçli gitmesini sağlayarak geçersiz oyları azaltmayı amaçlanmıştır. Ek

olarak, sosyal medya platformlarında yayınlanan videolarda, yapay zekâ asistanı seçmenlere ve sandık güvenliğini sağlayacak gözlemcilere dikkat etmeleri gereken önemli konuları aktarmıştır. OpenAI tarafından geliştirilen yapay zekâ sohbet robotu ChatGPT kullanılarak 14 Mayıs 2023 genel seçim sonuçlarının ne olacağı sorulmuş; ancak yapay zekâ bu soruya doğru ve sağlıklı yanıtlar veremeyeceğini, güncel bilgilere sahip olmadığını, seçim sonuçlarını etkileyen birçok faktör olduğunu ve en iyisi seçim sonuçlarını beklemek olduğunu belirtmiştir (Kırık ve Özkoçak, 2023: 412-428).

5. ETİK VE ŞEFFAF ANLAYIŞ İHTİYACI ÇERÇEVESİNDE YAPAY ZEKÂ

Spotify'da dinlediğiniz müzikler, Facebook'ta beğendiğiniz topluluklar ve sanatçılar aracılığıyla kişiliğinizi tanıyan şirketler vardır. Bu şirketler, Facebook beğenilerinizden cinsel yönelim, dini görüş, madde kullanma eğilimi gibi verileri doğru bir şekilde tahmin edebilir. Verilere kolaylıkla erişilebildiği için, önemli ve hassas bilgilere basit bir şekilde erişme imkânı bulmaktadır. Ancak bir şeyin mümkün olması, onun doğru olduğu anlamına gelmez. Her şeyin serbest olduğu ve yapay zekâ kullanımıyla ilgili herhangi bir yasal düzenlemenin olmadığı vahşi Batı'nın sonuna gelinmiştir (Marr, 2022: 181). Machiavelli ile bütünleşen "amaca giden her yol mubahtır" yaklaşımı yapay zekânın kullanımı konusunda kendisini göstermektedir. Yapay zekâ, toplumsal alana etki edebilen bir teknolojidir. Ancak, sahip olduğu olumlu özelliklerin yanı sıra potansiyel tehlikeleri de içermektedir. Etik meselesi, yapay zekânın olumsuz yönlerinin tartışılmasını ve gelecekte ortaya çıkabilecek durumların belirlenmesini sağlar. Yapay zekâ, insan ve toplumsal hayatla bağlantılı olduğundan, etik açıdan incelenmelidir (Topakkaya ve Eyibaş, 2019: 86).

Yapay zekâ, kanuni ve hukuki neticeleri bünyesinde barındırır. Yapay zekâ teknolojisi, insan haklarını ihlal etmekten ve önyargı oluşturmaktan ziyade insani değerleri ön plana alacak biçimde yapılandırılması anlayışı, genel olarak etikte "sınırlı optimizasyon" ya da "güvenilir yapay zekâ" şeklinde isimlendirilmekte ve yapay zekâ sektöründe bu durum artık daha fazla benimsenmektedir. Ayrıca yapay zekâyı OECD ve Montreal Bildirgesi gibi uluslararası ilkeler etrafında şekillendirme çabaları bulunmaktadır. Örneğin Montreal bildirgesinde eğitim ve etik başlığı altında; yapay zekânın tasarımı, geliştirilmesi ve katılımcıların eğitimi ile etik kapsamda yeniden geliştirilmesi önerisi benimsenmiştir. Diğer bir alt başlık olan demokrasinin korunması ilkesi ise; demokrasinin politik menfaatler uğruna manipülatif bilgi ve dezenformasyona karşı korumak için, kişilerin kötü niyetli sosyal platformlar ve online mecralar yoluyla kandırılması ve siyasi manipülasyonu engellemek amacıyla çevreleme stratejisinin yanında siyasi profil oluşturmayla mücadele stratejisinin gerekliliği belirtilmiştir. OECD'nin yapay zekâ için benimsediği ilkeler; hukukun üstünlüğüne, insan haklarına, demokratik değerlere ve farklılığa saygı çerçevesinde yapılandırılması, adil bir toplum oluşturmak için uygun güvenlik tedbirleri içermesi gerektiği ve hatta insan müdahalesine imkân tanıması gerektiğidir. Yapay

zekânın güvenilir olarak algılanması için yerine getirilmesi gereken beş etik yapay zekâ ilkesinden bahsetmek mümkündür. Bunlar; iyilik, zarar vermeme, özerklik, adalet ve açıklanabilirlik ilkeleridir (Efe, 2021:1-24).

Yapay zekânın etik kullanımı, yapay zekâ ile veriyi kişilere, müşterilere ve personele gerçek değer katmak amacıyla kullanmaktır. İnsanları kötü niyetle köşeye sıkıştırmaktan ziyade önemli bir değer ve katkı sağlamak aidiyet oluşturur. Bunu yaparken yapay zekâ şirketi kişiler karşısında yapay zekâ ve veriyi nasıl kullandığı hususunda şeffaf olması gerekir ve bu alan üst düzey pek çok şirketin başarısız olduğu bir alandır. Etik ve şeffaf anlayış yapay zekâya gerçek bir değer katar, müşteri ve diğer paydaşlarla arasında güven yaratır. Kişinin oluru alınmadan elde edilen yüz tanıma teknolojisinin kişisel gizliliği ihlal ettiği gerekçesiyle sosyal medya platformu Facebook'un yüksek tazminat ödeme tehlikesiyle karşı karşıyadır. Kişiler mahremiyetle alakalı konularda daha bilinçli oldukça rıza alınma seçenekleriyle karşılaştığı uygulamaların artacağı düşünülmektedir. Şirketlerin kişisel verileri toplamaya ve bu veriye yapay zekâ uygulama hakkı olduğunu düşünmemesi gerekir. Yapay zekâ teknolojisini anlayamama sorunu hesap verebilirlik ve güvenlik ile ilgili önemli sorulara yol açar. Bir durumun nasıl işlediği kavranamazsa, nerede sorun yaşanacağını tespit etmek veya tahmin etmek zordur. Karar alma süreçlerini açıklayamazsak yapay zekâlara nasıl güvenilir? Yapay zekâlara ne zaman güvenip ne zaman güvenilmemesinin ayrımını hislerimizle mi geliştireceğiz? soruları cevapsız kalmaktadır. Yapay zekâ teknolojisini etik kullanmanın bir öğesi de en çok değeri sağladığı nokta, yani hizmete ve kişilere en fazla katkıyı verdiği yerdir. Güven inşa etmenin en önemli unsuru değerdir. Yapay zekâ ne kadar değer üretirse insanlarla arasında o denli güven, memnuniyet sağlar (Marr, 2022: 181-197). Bu doğrultuda yapay zekânın seçim güvenliği noktasında sunacağı katkıların seçmenler ve siyasi partiler arasında ya da siyasi partilerin kendi aralarında güven inşa etmesinde önemli rolü olması beklenebilir. Etik, şeffaf ve güven anlayışının demokrasinin korunması ve seçim güvenliğinin sağlanmasında son derece kritik olduğu, yapay zekânın kullanımı etik ve şeffaf anlayış çerçevesinde yapılandırılması gerekir.

Yapay zekâ doğrudan insan ve toplumsal hayatla bağlantılı olduğundan etik açıdan incelenmelidir. Birçok akıllı makinenin özel bilgilere erişiyor olması ve özel bilgileri yazılım şirketlerine aktarması kişisel güvenliğe ciddi bir tehdittir. Bilişim teknolojisinin güç kazanmasıyla beraber kişilere yönelik özel bilgilerin kişinin bilgisi ve rızası olmadan toplanması, depolanması, yayılması, üzerinde değişiklik yapılması ve kötü niyetli kullanılmasına zemin hazırlamıştır. Yapay zekâ ve etik ilişkisi değerlendirildiğinde temel sorun yapay zekânın sosyal ve bilişsel yönü olan alanlarda kullanılmasıdır. Çünkü yapay zekâ bilinç sahibi olmamakla birlikte, var olan yapay zekâ karar verme ve seçim yapma noktasında sıkıntılar yaşamaktadır. Yapay zekânın sosyal uyum içinde olması için etik bilgisinin olması gerekir. Bu sebeple kişilere zarar verecek davranışları, iyiyi ve kötüyü birbirinden ayırt etme yeteneğine sahip olmalıdır (Topakkaya ve Eyibaş, 2019: 81-99).

Etik bir yapay zekâ mümkün müdür? Yapay zekâ seçme yeteneğine sahip mi? Etik bir yapay zekâda sorumluluk yapay zekâ da mı yoksa üreticisinde mi? Şeklinde etik gerçeklik tartışmaları yapılmaktadır. Yapay zekânın etik gerçekliğine yönelik "makinelerin yaptığı hatalarda etik açıdan sorumluluk kimde" sorusu neticesinde sorumluluk yapay zekâya yüklenirse insanların etik sorumluluğu ortadan kalkacaktır. Yapay zekânın bu şekilde inşa edilmesi etik açıdan başka bir sorundur. Yapay zekânın etik unsur olarak incelenmesi ve etik ilkelere göre yapılanmalıdır (Öztürk Dilek, 2019: 57).

6. YAPAY ZEKÂNIN SEÇİM GÜVENLİĞİNE TEHDİDİ: DEMOKRASİNİN ETKİSİZLEŞMESİ

OpenAI CEO'su Sam Altman, Mayıs 2023'te ABD Senatosu Adalet Komisyonu'na bağlı Gizlilik, Teknoloji ve Hukuk Alt Komitesi'ne yapay zekâ destekli seçim müdahalelerine yönelik kaygılarını dile getirmiştir. Sam Altman, seçim güvenliğini sağlamanın yolunun teknolojinin yasalarla düzenlenmesi olduğunu belirtmiştir. Ayrıca, 2024 Kasım ayında yapılacak olan ABD'deki başkanlık seçimlerinde Ulusal Eyalet Genel Sekreterleri Birliği ile işbirliği yapacaklarını ve ChatGPT'nin seçimle ilgili soruları kurumun bilgilendirme sitesine yönlendireceğini aktarmıştır. Seçime gidecek ülkelerin seçim güvenliğini sağlamak için birtakım tedbirler almıştır. Ancak, yasal tedbirlerin bireysel özgürlükleri engellediği, kâr odaklı sosyal medya platformları ise topluluk kurallarına ve yasalardaki boşluklara takıldığı söylenebilir. Tedbirler alınmayınca da seçim güvenliğinin sağlanamaması ve demokrasinin korunamaması gibi güvenlik risklerine meydan vermektedir. Örneğin; yapay zekâ AB üyesi Slovakya ve Polonya seçimlerine müdahale amacıyla kullanılmıştır. Facebook'ta yapay zekâyla manipüle edilmiş ses kaydına göre; liberal İlerici Slovakya Partisi'nin liderinin basın mensubuna Roman azınlığın oylarını satın alarak seçime hile karıştıracaklarını iddia etmiştir. Bu ses kaydının sahte olduğu, kurumlar ve kişiler tarafından ifade edilmiş olsa da seçim kanununa göre seçim yasaklarının başladığı son kırk sekiz saatlik zamana denk geldiği için kitlelere yeterince duyurulamamıştır. Facebook'un çatı şirketi Meta kaydı kaldırmamış, sadece etkileşimleri sınırlamıştır. Slovakya Dışişleri Bakanlığı, sonuçların açıklanmasından sonra, Rusya'yı dezenformasyon eylemleriyle seçimlere müdahale etmekle suçlamıştır. Slovakya'da bilhassa sosyal medyadaki dezenformasyona karşı mücadele eden teyit kuruluşları, yapay zekânın seçimlere müdahalesinin kendilerini aştığı, yapay zekâ ve hızına karşı gelebilecek aygıtlara sahip olmadıklarını aktarmıştır. Diğer bir ülke örneği Polonya'dır. Polonya seçimlerinde de yapay zeka ile dezenformasyon ve Rusya'nın müdahale ettiği iddiaları vardır. Fakat Polonya'daki olayın faili seçimi kaybeden Rusya yanlısı popülist iktidar değil, merkez sağdaki AB yanlısı ana muhalefet partisidir. Ülkenin Başbakan'nın sesi yapay zekâ desteğiyle taklit edilmiş, AB yanlısı ana muhalefet partisince seçim kampanyası sürecinde kullanılmıştır (Aposto.com, 2024).

İnternetin serbest ve özgür olması, demokrasinin yayılma hedefinin önemli bir unsur olduğu fikrinden dijital aygıtların otokratların kontrolünde bilgiyi ve muhalefeti sindirmeye çalışan güçlü bir araca dönüşmesi tartışılmaktadır. Sosyal medya platformları sadece despotik iktidarların değil, ayrıca hem sağ hem sol aşırı yanlılarının yanlış, sahte bilgileri yaydığı bir alan olduğu sorusu da gündeme gelmiştir. Dijital aygıtların veri toplama ve işleme için kullanılmasıyla beraber, bu teknolojiler devletlerin ve şirketlerin tekelinde güçlü bir gözetim ve manipülasyon aracına evrilmiştir. İnsanların gücü azaldıkça, hem despotik hem de demokratik ülkelerde tepeden aşağıya doğru denetim artmış; katılımı ve öfkeyi yükseltmek için kazanç elde etmeye yönelik iş türleri çoğalmıştır. Örneğin, Çin'de yapay zekâ teknolojisi siyasi sansür ve baskı aracı olarak kullanılmaya başlanmıştır. Gelişen yapay zekâ teknolojileri, daha fazla kontrole yol açmış, politik bir güç aracına dönüşerek sansür uygulama, insanları yönlendirme, yabancı web sitelerini engelleme, erişime kapama, politik hassasiyeti yüksek konuları silmeye kadar yüksek seviyede denetim sistemine yol açmıştır. Çin yapay zekâ sayesinde siyasi ifadeleri ve bilgileri saklama ve muhalif sesleri sindirme yeteneklerini önemli ölçüde arttırmıştır. Veri toplama amaçlı dijital aygıtların bir defa kullanılması, muhalefeti bastırma ve yurttaşları daha iyi takip etmek bazı devletlerce benimseneceği açıktır. Bu aygıtlar, demokratik olmayan devletleri güçlü hale getirecek ve muhalefeti daha etkin biçimde sindirmelerine olanak tanıyacaktır. Demokratik devletlerinde zamanla daha baskıcı duruma gelmesine dahi yol açabilir. Demokrasi karanlıkta ölür ancak yapay zekânın ışığında da can çekişir. Diğer yandan yapay zekâ teknolojilerinin otomasyon ya da personelleri izlemesi, takip etmesi ve devletin sansürü arttırması amacıyla geliştirilmesi gerekmemekte, dijital demokrasilerin özünde demokrasiye aykırı bir kısım yoktur. Bu olumsuz duruma yola açan teknoloji şirketleri veya hükümetlerin eğilimleridir. Sosyal medya platformları üzerinde zaman zaman artan toplumsal ve çalışan baskısının artması, kötü niyetli içeriklerin yayılmasının önüne geçmek üzere algoritmalarında değişime gitmesini zorunlu kılmıştır. Bu sosyal medya platformlarındaki düzenlemeler ışığındaki iyileştirmelerin etkisi yeterli olmamış; hala fazlaca yanıltıcı bilgi ve manipülatif içerikler bulunmaktadır. Demokrasiye en fazla gereksinim duyulan zamanda yapay zekânın demokrasinin altını oyması durumu üzücüdür. Dijital teknolojilerin yönü değiştirilmediği sürece, eşitsizliği arttırmaya ve işgücünün önemli bir kısmının dışarıda kalmasına yol açacaktır. Demokrasi olmadığında karşıt gücün oluşması zorlaşır. Elitist bir kesim, baskı ve propaganda aygıtlarını etkin biçimde kullanabildiği ve siyaseti bütünüyle denetimde tuttuğu sürece, teşkilatmış, anlamlı bir muhalefet kurmakta zordur. Bu sebepten Çin'de etkin bir muhalefetin olması yakın süreçte imkânsızdır. Yapay zekâ tabanlı denetim mekanizmasının ve etkin sansür uygulaması altında bu durum daha zordur. ABD ve Batı'nın genelinde de karşı muhalefetin oluşması hayali azalmakta, yapay zekâ teknolojisinin baskıcı yönü, demokrasiyi de bunalttığı söylenebilir (Acemoğlu ve Johnson, 2023: 317-356).

Yapay zekânın kullanım amacı; seçim güvenliğini, demokrasinin gelişimini ve korunmasını önemli ölçüde etkilemiştir. Demokrasinin ve seçim güvenliğinin sağlanması konuları ülkeden ülkeye farklılıklar göstermekte, otoriterliği veya demokratik değerleri ilke edinip edinmemesine bakılmaksızın doğru veya yanlış niyetlerle kullanılabileceği görülmüştür.

7. YAPAY ZEKÂ VE SEÇİM GÜVENLİĞİNE YÖNELİK DÜZENLEMELER, TARTIŞMALAR VE ÖNERİLER

Avrupa Komisyonu, yapay zekâya yönelik olarak 2021 yılında bütün AB üyeleri için kanuni bir düzenleme tavsiye etmiştir. Bu kanuni düzenleme temelde; içeriklerin yapay zekâ ile oluşturulduğunun açıklanması, yapay zekânın kanuna aykırı biçimde üretilmesini önleyecek şekilde yapılandırılması ve telif hakkı olan içeriklerin özetlerini yayımlama sorumluluğunun kanuna dayanması şeklinde üç ilkededir. Ayrıca Komisyon, Konsey ve Parlamento arasında yapay zekâya dönük kanuni düzenlemelerin gereksinim oldukça yapılması ifade edilmiş. Aralık 2023'te dünyanın ilk yapay zekâ kanununun benimsenmesiyle birlikte demokrasiye ve hukukun üstünlüğüne ciddi zararlar verme kapasitesi sebebiyle, seçim sonuçlarını ve seçmen davranışını etkilemek için kullanılan yapay zekâ teknolojilerini yüksek risk statüsüne alarak düzenleme yapılmıştır. İnsanlara yapay zekâ teknolojisiyle ilgili olarak şikâyet etme, bilgi edinme hakkı verilmiştir. Spesifik şeffaflık riski bağlamında insanların yapay zekâ destekli sohbet robotlarıyla etkileşim kurarken farkında olmalarının zorunluluğu belirtilmiştir (Aposto.com, 2024). AB Yapay Zekâ Yasası, yapay zekâ teknolojilerinin kişi haklarına ve demokrasiye dönük muhtemel riskler barındırdığından dolayı, yasa koyucular insanların hassas bilgilerini ve özelliklerini manipüle eden davranışları yasaklama yoluna gitmiştir. Kurallara uyulmaması, ihlale ve şirketin büyüklüğüne göre para cezaları verilmesi kararlaştırılmıştır (Legal.com, 2023). Görüldüğü üzere AB, seçimlerin güvenliği ve demokrasinin korunması amacıyla yapay zekâ teknolojilerine karşı bir reaksiyon göstermiş; seçim ve seçim güvenliğini yüksek riskli konumda değerlendirmiş; yasal yükümlülükler ve yaptırımları belirlemiştir. AB bütün bu süreçleri kurumsal organları aracılığıyla yapmış; yönetişimi esas alarak yapay zekâ teknolojilerinin olumsuz özelliklerine karşı reaksiyon göstermiştir.

Demokratik süreçlerde seçim dezenformasyonunun detaylı biçimde anlaşılması gerekir. Seçim dezenformasyonu, kamuoyunu manipüle etmek ve seçimlerin güvenliğine zarar vermek amacıyla yanlış/sahte bilgilerin bilinçli olarak yayılmasını içerir ve demokrasinin temel değerlerine ters düşmektedir. Geçmişe bakıldığında seçimlere müdahaleler karmaşık hal almıştır. Neticede demokratik sürecin riske girmesi derhal tedbir almayı zorunlu kılmaktadır. Bu tarihsel süreç dezenformasyonun kötü niyetli yayılmasının neden olduğu sıkıntılara karşı etkin mücadele etme stratejisi bakımından önemlidir. Dezenformasyonla mücadelenin özünde yapay zekâ gözlemcileri diye tabir edilen yapay zeka destekli otomatik sistemler bulunmakta olup, belli eylemleri ve alanları etik ko-

nuda takip etmek, analiz etmek ve düzenlemek, bunun yanında seçimlerin güvenliğini ve bütünlüğünü sağlamak için dezenformasyon olaylarıyla mücadele etme rolünü üstlenmiştir. Bu bağlamda yapay zekânın modern seçimlerde adalet ve şeffaflık açısından önemli rol oynadığını söylemek mümkündür. Büyük veri analizi ve veri tanımlamaları seçim sürecini manipülatif olaylara karşı korur (Unite.ai, 2023).

2023 Kasım ayında yayımlanan bir raporda, İngiltere'deki seçim gözetim organlarına yönelik kaygılar dile getirilmiş; deepfake içeriklere karşı yetkilerinin kısıtlı olduğu, politik aktörlerin olası yapay zekâ destekli sahte video içeriklerine karşı güvenlik boşluğunda olduğunu söylenebilir. Bu deepfake videoların siyasi aktörleri hedef alması seçimlerde muhtemel manipülasyonlara yönelik farkındalığı arttırmıştır. Ayrıca bu içeriklerin kanunen gri alanda kalması olayın boyutunu daha da ciddileştirmektedir. İngiltere Seçim Komisyonu›nun deepfake›lere karşı yetkisinin olmaması, daha fazla olağanüstü yetki talep etmesine yol açmıştır. Yapay zekâ gözlemcilerinin demokratik değerleri koruma, tehditlerle mücadele etme de işbirliği ve gayreti önemlidir. Yapay zekâ gözlemcileri; makine öğrenimi ve derin öğrenme, seçimlere dönük sahte bilgilere karşı algoritmalar kullanmaktadır. Bu aygıtlar sayesinde kötü niyetli unsurların farklılaşan stratejilerini tespit ederek önüne geçmektedir. Bu algoritmaların uyarlanabilir yapısı seçimlerin güvenliğine yönelik tehlikeleri tanıma ve ortadan kaldırma gibi nitelikleri barındırırken; doğal dil işleme (NLP) yoluyla aldatıcı ve yanlış verileri etkili biçimde yorumlayarak belirleme ve mücadele etme kabiliyetini artırmaktadır. Yapay zekâ gözlemcileri aktif, çok yönlü, gelişmiş makine algoritmaları, sürekli izleme yöntemiyle sosyal medya manipülasyonuna karşı durma ve demokrasinin korunmasında önemli katkılar sağlamıştır. Yapay zekâ destekli teknolojiyle birlikte toplumsal farkındalığı artırmak ve deepfake içeriklere karşı etkin kanuni düzenlemelerle bütünleştirmek oldukça önemlidir. Yapay zekâ teknolojilerinin şeffaflığa, hesap verebilirliğe ve adalete odaklanarak etik biçimde yayılmasını sağlanabilir. Ayrıca, kitleler arasında siyasal okuryazarlığın teşvik edilmesi, sürekli değişen bilgi çağında bireylerin bilgiyi eleştirel bir şekilde değerlendirmeleri ve bilinçli kararlar vermeleri için yetkilendirilmesi gerekir (Unite.ai, 2023). Diğer yandan yapay zekâ teknolojisinin seçim ve seçim güvenliğine katkısının sadece seçim öncesi dezenformasyon veya manipülatif olayların önüne geçmekten ibaret olmayıp yapay zekânın seçimlerde dürüst ve adil bir şekilde kullanılması halinde nasıl bir fayda sağlar? Sorusundan hareketle; dijital oylama, bütün seçmenlerin mekân fark etmeksizin oy kullanabilme serbestisi ve ikinci tur oylamaların hızlı biçimde gerçekleşmesine imkân tanır. Bunun yanı sıra yapay zekâ, seçimlerin şeffaflığını ve hesap verebilirliğini arttırır. Örneğin, yapay zekâ bütün oyların kaydını tutabilir ve oy zarflarının kaybolması ya da zarar verilmesinin önüne geçebilir. Oy güvenliğini üst düzeye çıkararak güvenceye alabilir (Dünya Gazetesi, 2023).

Öte yandan yapay zekânın seçmen kitlesini incelediği ve seçim kampanyalarında kullanıldığı görülmektedir. Örneğin, 2022'de Güney Kore'deki cumhurbaşkanlığı seçimlerin-

de muhalefet adayı olan Yoon Suk-Yeol'un yapay zekâ destekli dijital avatar sayesinde 7 milyondan fazla genç seçmenle iletişim kurmuş; cevapları basına yansıyan Yoon Suk-yeol seçimi kazanmıştır. ABD'de ise Demokrat Parti'nin seçmenlerin sosyal platformlardaki siyasi yönelimleri inceleyerek seçim kampanya giderleri için yapay zekâ desteğiyle kişilere özel mektuplar yazdığı ortaya çıkmıştır. Diğer yandan yapay zekâ yalnızca seçim kampanyalarında değil seçim ve sandık güvenliği noktasında kazanımlar sunabilir. Bilhassa yapay zekâ destekli uygulamalar oy verme işlemlerinde bireysel asistan/yardımcı olarak görevlendirilebilir, sandık sonuçlarının izlenmesinde etkinlik sağlayabilir, eski seçim sonuçlarıyla karşılaştırmalı değerlendirme imkânı sunabilir, olağanüstü olayların izlenmesine katkı sağlayabilir. Başka bir örnek, Yeni Zelanda'da 2018 yılında gerçekleşen seçimlerdir. Dünyanın ilk yapay zekâlı politikacısı olan "SAM" siyaset tarihine geçmiştir. SAM, zaman ve mekân sınırı olmaksızın, günümüzde hala web sitesi üzerinden seçmenlerin isteklerini, problemlerini dinleyip, çareler sunabilmektedir. Diğer bir örnek, 2018 Rusya seçimlerinde seçime katılan Yandex yapay zekâsı Alice'dir. Alice seçimlerde Rus seçmenlerden neredeyse 25 bin oy almış; muhalif ifadeler kullananlara ise yaptırım uygulanmasını aktaran Alice, seçmenlerden tepki almıştır. Japonya'da ise yapay zekâ yerel seçimlerde kullanılmıştır. Japonya'nın başkenti olan Tokyo'nun Tama ilçesinde belediye başkanlığı seçimine katılan "Mitchihido Matsuda" adından yapay zekâ 4 bin oy alarak 3'üncü olmuştur. Matsuda'nın seçim vaadi ise 100 kişiden 99'unun kendi yönetiminden hoşnut kalacağı ifadesi olmuştur (Epnext.com, 2023).

Bütün bu gelişmeler ışığında yapay zekâ teknolojisine yönelik önlemler, çözüm önerileri ve modeller Sheetal Mavi (2016: 27-29)'nın "Bulut Bilişim: Güvenlik Sorunları ve Zorluklar" adlı çalışmasında güvenlik yönetim modeli dile getirilmiştir. Örneğin, güvenlik yönetiminde vatandaşlar için yasal düzenlemelerin geliştirilmesinin önemli olduğu, güvenlik mekanizması ve gündeminin yasal stratejiyle uyumlu olması gerektiği söylenmiştir. Güvenlik ekibinin çalıştığı kuruluşlarda, beklentiler üzerinde anlaşılamaması, sorumlulukların ve rollerin açık şekilde tanımlanmaması güvenlik ekibi arasında kendilerinden istenilen deneyim ve becerileri geliştirme noktasında koordinasyon eksikliğine ve karmaşıklığa yol açabilir. Mavi (2016)'nın çalışmasında diğer bir öneri, güvenlik yönetişimi olup; temel amacı güvenlik girişimlerine rehberlik etmek, bilişim teknolojileriyle uyumlu bir güvenlik yönlendirme komitesi geliştirilmesidir. Bu komite, güvenlik yönetim ekibinin ve bilgi güvenliği işlevlerini yerine getirmeye dâhil olan diğer grupların rollerini ve sorumluluklarını net şekilde tanımlanmalıdır. Diğer bir güvenlik yönetim modeli olarak ise güvenlik farkındalığı karşımıza çıkmaktadır. Bireyler güvenlik için en zayıf halka olmasından dolayı bilgi, kültür ve farkındalığın bireylerle ilgili risklerini yönetmede etkili bir araç olduğu belirtilmiştir. Ayrıca gereksinim duyulabilecek kişilere güvenlik farkındalık eğitiminin sağlanmaması da yapay zekâ şirketlerine zarar verebilir.

8. SONUÇ VE ÖNERİLER

Sosyal medya platformları, yapay zekâ destekli sohbet robotları vb. akıllı uygulamaların kötü niyetle kullanıldığı zaman ülke siyasetini ve kamuoyu dinamiklerini kaotik ortama sürüklediği görülmüştür. Yapay zekâ teknolojisinin kötüye ve yanlışa yol açan uygulamalarının kontrol edilmesi gerekmektedir. Bu kontrol sansür veya baskı olarak algılanmamalıdır. Demokrasinin teminatı olan "seçim güvenliği"nin sağlanması kamu düzeni ve güvenliğinin bir parçasıdır; iktidarıyla, muhalefetiyle ve vatandaşıyla topyekûn bir gayret sarf edilmesini zorunlu kılmaktadır.

Yapay zekâ teknolojisinin güvenlik risklerini barındırdığı, seçim güvenliğine de risk teşkil ettiği ancak seçim sürecine katkılarının da olabileceği görülmüştür. Yine de yüksek risk olarak tanımlanan seçim ve demokrasinin güvenliği konusu öneriler, çözüm yolları ile devlet ve hükümetlerce tedbir alınmaya çalışılmaktadır. Bazı ülkelerin bu gelişmeler karşısında somut, yasal ve kurumsal bir hazırlıkları olmadığı, işlevsel ve yapısal anlamda yapay zekânın risklerini ve olumsuzluklarını azaltmaya gayret etmemesi ilginçtir. Yapay zekâ teknolojisi ve dijitalleşen siyaset ile birlikte, sosyal medya içerikleri, haberler vb. mecralar güvenlik tehlikelerini beraberinde getirmekte olup, işlevsel ve yapısal anlamda tedbirler almayı mecbur kılmaktadır. Türkiye'nin yapay zekâ bağlamında seçim ve seçim güvenliği ekseninde bir hazırlığının olmadığı söylenebilir. Seçim güvenliği bağlamında yapay zekâ teknolojisine yönelik işlevsel ve yapısal anlamda tedbirlerin alınması gerekir. Acilen Yapay Zekâ Yasası, seçim mevzuat düzenlemeleri yapılmalıdır. YSK bünyesinde seçim sürecince yapay zekâ algoritmaları, deepfake vb. içeriklere karşı tedbirler alınmalı, hizmet birimleri oluşturularak teknik ve uzman personellerden faydalanılmalıdır. Ülkemizde "Ulusal Yapay Zekâ Stratejisi" belgesinin yürürlüğe girdiği, yapay zekânın iyi ve kötü yanlarına karşı kurumsal ve toplumsal farkındalığın ancak uygulanabilirlik noktasında bazı eksikliklerin ve olumsuz durumlara nasıl bir reaksiyon vereceği belirsizdir. Öte yandan yapay zekâ-seçim güvenliği alanında güvenlik yönetişimi sağlanmalıdır. Yalanın 'gerçek'leştirilmesi veya gerçeğin 'yalan'laştırılması seçime olan ilgiyi, güveni, inancı, umudu kaybettirecektir. Bunun önüne geçilmesi siyasetin ve toplumun geleceğe borcudur.

Etik Beyanı: Yazar bu çalışmanın tüm hazırlanma süreçlerinde etik kurallara uyulduğunu beyan eder. Aksi bir durumun tespiti halinde Kamu Yönetimi ve Teknoloji Dergisinin hiçbir sorumluluğu olmayıp, tüm sorumluluk çalışmanın yazarına aittir.

Ethics Statement: The author declares that the ethical rules are followed in all preparation processes of thisstudy. In the event of a contrary situation, the Journal of Public Administration and Technology has noresponsibility and all responsibility belongs to the author of the study.

Yazar Katkıları: Öğr. Gör. Furkan SAİTOĞLU çalışmanın tamamında tek başına katkı sunmuştur.

Author Contributions: Öğr. Gör. Furkan SAİTOĞLU has contributed to all parts and stages of the study

Çıkar Beyanı: Yazar ve herhangi bir kurum/kuruluş arasında çıkar çatışması yoktur.

Conflict of Interest: There is no conflict of interest among the author and any institution.

Teşekkür: Yayın sürecinde katkısı olan hakemlere teşekkür ederim.

Acknowledgement: I would like to thank the referees who contributed to the publication process.

REFERENCES

Acemoğlu, D. & Johnson, S. (2020) İktidar ve Teknoloji 'Bin Yıllık Mücadele'. Doğan Kitap.

Aydın, A. (2023) Yapay Zekâ Dönüşümü ve Dünyada Yapay Zekâ Stratejileri, Ed.: Safa Uslu, Prof. Dr. Cenay BABAOĞLU ve Yavuz E. Beyribey. İstanbul: SETA Kitapları 100.

Aydın, N. & Karaşahin T. (2023), "Seçim Güvenliği Bağlamında Dezenformasyon". Fides Hukuk Dergisi, Y. 6, S. 6. s. 17-39.

Basnet, A.B. (2022) "Artıfıcıal Intellıgence In Cyber Securıty". Centrıa Unıversıty Of Applıed Scıences. Bachelor of Engineering. Thesıs. s. 1-29.

Beren, F. (2013) "Seçmen Tercihine Etki Eden Faktörler ve Seçim Güvenliği: Şanlıurfa İli Örneği". Akademik İncelemeler Dergisi (Journal of Academic Inquiries) Cilt/Volume: 8, Sayı/Number:1. s. 191-214.

Efe, A. (2021) "Yapay zekâ risklerinin etik yönünden değerlendirilmesi". Bilgi ve İletişim Teknolojileri Dergisi, 3(1), s. 1-24.

Karakoç, E. & Zeybek, B. (2022) "Görmek İnanmaya Yeter Mi? Görsel Dezenformasyonun Ayırt Edici Biçimi Olarak Siyasi Deepfake İçerikler". Marmara Üniversitesi Öneri Dergisi • Cilt 17, Sayı 57, Ocak 2022, ISSN 2147-5377. s. 50-72.

Kavut, S. (2024) "Toplumların Dijital Dönüşüm Aracı Olarak Yapay Zekâ Çalışmaları: Türkiye'nin ve Türk Devletleri Teşkilatının Yapay Zekâ Kullanımı Üzerine Bir Analiz". Erciyes İletişim Dergisi, 11(1), s. 325-344.

Kırık, A. M. & Özkoçak, V. (2023) "Medya Ve İletişim Bağlamında Yapay Zekâ Tarihi ve Teknolojisi: ChatGPT ve Deepfake İle Gelen Dijital Dönüşüm". Karadeniz Uluslararası Bilimsel Dergi, (58), s. 73-99.

Kurnaz, A. (2023) "Dijital Siyasetin Yükselişi ve Yapay Zekâ". Siyaset, Kamu Yönetimi ve Uluslararası İlişkiler Bağlamında Yapay Zekâ Tartışmaları, Ekin Yayınevi. s. 1-26.

Marr, B. (2022) Yapay Zekâ Devrimi Dijital Dönüşüm İşinizi Nasıl Etkileyecek, Çev.: Ümit Şensoy. İstanbul: Akbank Yayınları.

Mavi, S. (2016) "Cloud Computing: Security Issues and Challenges". IITM Journal of Management and IT. Volume 7 Issue 1 January-June, 2016. s. 25-31.

Özsalih, A. (2023) "Yapay Zekâ Yoluyla Oluşturulan Sahte Haberlerin Medya

Gündemini Belirlemesi". The Turkish Online Journal of Design Art and Communication, 13 (3), s. 533-550.

Öztürk Dilek, G. (2019) "Yapay Zekânın Etik Gerçekliği". AUSBD, 2 (4), s. 47-59.

Sayler, M.K. (2020) "Artificial Intelligence and National Security". Congressional Research Service R45178. https://crsreports.congress.gov. s. 1-39.

Topakkaya, A. & Eyibaş, Y. (2019) "Yapay Zekâ Ve Etik İlişkisi". Felsefe Dünyası Dergisi, Sayı: 70. s. 81-99.

ELEKTRONİK KAYNAKLAR

Aposto.com (2024), "Seçim güvenliğine tehdit: Gerçeğin silahlaştırılması".

https://aposto.com/s/secim-guvenligine-en-buyuk-tehdit-gercegin-silahlastirilmasi, Erişim Tarihi: 12.04.2024.

Dünya Gazetesi (2023), "Artık seçimleri yapay zekâ yapsın!".

https://www.dunya.com/kose-yazisi/artik-secimleri-yapay-zekâ-yapsin/693849 Erişim Tarihi: 15.04.2024.

EPN Haber Merkezi (2023), "Yapay Zekâ Seçimlere de Damga Vuracak".

https://epnext.com/yapay-zekâ-secimlere-de-damga-vuracak/,ErişimTarihi: 10.04.2024.

Gazetenisan.net (2022), "Seçimler yaklaşırken güvenlik ve yapay zekâ". https://www.gazetenisan.net/2022/09 Erişim Tarihi: 10.04.2024.

Legal.com (2023), "Avrupa Birliği Yapay Zekâ Yasası: Güvenilir Yapay Zekâ İçin Kapsamlı Kurallar Üzerinde Varılan Anlaşma". https://legal.com.tr/blog/ekonomi/avrupa-birligi-yapay-zekâ-yasasi-guvenilir-yapay-zekâ-icin-kapsamli-kurallar-uzerinde-varilan-anlasma/, Erişim Tarihi: 15.04.2024.

T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi, https://cbddo.gov.tr/hizmet-birimlerimiz/ Erişim Tarihi: 05.05.2024.

T.C. Cumhurbaşkanlığı İletişim Başkanlığı, https://iletisim.gov.tr/teskilat-semasi, Erişim Tarihi: 05.05.2024.

Unite. ai (2023), "Sorumlu Yapay Zekâ: Seçim Dezenformasyonuyla Mücadelede Yapay Zekâ Gözlemcilerinin Önemli Rolü". https://www.unite.ai/tr/responsible-ai-the-crucial-role-of-ai-watchdogs-in-countering-election-disinformation/, Erişim Tarihi: 15.04.2024.

Yüksek Seçim Kurulu, https://www.ysk.gov.tr/web_ysk_teskilati, Erişim Tarihi: 05.05.2024.