



T.C.

BANDIRMA ONYEDİ EYLÜL ÜNİVERSİTESİ

SOSYAL BİLİMLER ENSTİTÜSÜ

AVRUPA BİRLİĞİ SİYASETİ VE ULUSLARARASI İLİŞKİLER

ANABİLİM DALI

Yüksek Lisans Tezi

**YAPAY ZEKA VE AKILLI ALGORİTMA
SİSTEMLERİNİN ULUSLARARASI SİSTEM
DİNAMİKLERİ ÜZERİNDEKİ ETKİSİ: BREXİT
ÖRNEĞİ**

Başak BERKER

2215030025

Tez Danışmanı:

Doç. Dr. Altuğ GÜNAR

T.C.
BANDIRMA ONYEDİ EYLÜL ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
ULUSLARARASI İLİŞKİLER ANABİLİM DALI

Yüksek Lisans Tezi

YAPAY ZEKA VE AKILLI ALGORİTMA
SİSTEMLERİNİN ULUSLARARASI SİSTEM
DİNAMİKLERİ ÜZERİNDEKİ ETKİSİ: BREXİT
ÖRNEĞİ

Başak BERKER

2215030025

Tez Danışmanı:
Doç. Dr. Altuğ GÜNAR

YÜKSEK LİSANS TEZİ ONAYI

Bandırma Onyedİ Eylöl Üniversitesi Sosyal Bilimler Enstitüsü Avrupa Birlięi Siyaseti ve Uluslararası İlişkiler Anabilim Dalı, Uluslararası İlişkiler Programında Yüksek Lisans öğrencisi Başak BERKER tarafından Doç. Dr.Altuę GÜNAR'ın danışmanlığında hazırlanan “Yapay Zeka Ve Akıllı Algoritma Sistemlerinin Uluslararası Sistem Dinamikleri Üzerindeki Etkisi: Brexit Örneęi” başlıklı tez aşağıdaki jüri üyeleri tarafından 30/09/2025 tarihinde yapılan Tez Savunma Sınavında oybirliği ile başarılı bulunmuş ve Yüksek Lisans Tezi olarak kabul edilmiştir.

Jüri Başkanı - Danışman

Doç. Dr. Altuę GÜNAR

Jüri Üyesi

Dr. Öğr. Alptekin MOLLA

Jüri Üyesi

Doç. Dr. Didem SAYGIN

**ETİK BEYAN
TÜRKİYE CUMHURİYETİ**

BANDIRMA ONYEDİ EYLÜL ÜNİVERSİTESİ

SOSYAL BİLİMLER ENSTİTÜSÜ MÜDÜRLÜĞÜNE

Bu belge ile bu tezdeki bütün bilgilerin akademik kurallara ve etik ilkelere uygun olarak toplanıp sunulduğunu beyan ederim. Bu kural ve ilkelerin gereği olarak, çalışmada bana ait olmayan tüm veri, düşünce ve sonuçları andığımı ve kaynağını gösterdiğimi ayrıca beyan ederim.

Tezi Hazırlayan Öğrencinin

Adı ve Soyadı

Başak BERKER

30/09/2025

ÖZET

YAPAY ZEKA VE AKILLI ALGORİTMA SİSTEMLERİNİN ULUSLARARASI SİSTEM DİNAMİKLERİ ÜZERİNDEKİ ETKİSİ: BREXİT ÖRNEĞİ

Başak BERKER

Bu çalışma, yapay zeka ve akıllı algoritmaların uluslararası sistem üzerindeki etkilerini kavramsal, politik, ekonomik ve teknolojik boyutlarıyla incelemeyi amaçlamaktadır. Araştırmanın temel sorusu, yapay zekanın sadece bireysel yaşamı değil, aynı zamanda ulus devlet yapıları, siyasi kültürler ve küresel güç dengeleri üzerinde nasıl bir dönüşüm yarattığıdır. Yapay zeka, bilişim teknolojileriyle birlikte gelişerek sosyal medya, bilgi akışı, veri analizi ve stratejik karar alma gibi alanlarda etkili bir aktör haline gelmiştir. Bu durum, ulus devlet sınırlarının ve kültürel kodların bulanıklaşmasına, yeni bir siyasi ve ekonomik paradigma oluşumuna zemin hazırlamaktadır. Araştırmada nitel yöntem kullanılmış, literatür taraması ve vaka analizi yoluyla hem kuramsal hem de uygulamaya dönük çıkarımlara ulaşılmıştır. Vaka analizi çerçevesinde özellikle Brexit sürecinde yapay zeka destekli algoritmaların seçmen davranışları üzerindeki etkileri ele alınmış; Cambridge Analytica örneği üzerinden büyük veri manipülasyonunun siyasal süreçlerdeki rolü incelenmiştir. Elde edilen bulgular, algoritmaların politik karar alma süreçlerini yönlendirebildiğini ve demokrasilerde bilgi manipülasyonu yoluyla seçmen tercihlerini şekillendirme potansiyeli taşıdığını ortaya koymuştur. Özellikle politik kampanyalarda veri manipülasyonu ve seçmen hedefleme gibi stratejilerin, demokratik süreçler üzerinde belirleyici bir rol oynadığını göstermektedir. Sonuç olarak, yapay zekânın sadece teknik bir araç değil, küresel sistemde yeni bir güç formu olarak yükseldiği; toplumsal yapılar, ekonomi ve siyasal iletişim üzerinde dönüştürücü bir rol üstlendiği değerlendirilmiştir.

Anahtar Kelimeler: Akıllı algoritmalar, Dijital Siyaset, Uluslararası ilişkilerde teknoloji, Veri Manipülasyonu, Yapay Zeka.

ABSTRACT

THE IMPACT OF ARTIFICIAL INTELLIGENCE AND SMART ALGORITHM SYSTEMS ON THE DYNAMICS OF THE INTERNATIONAL SYSTEM: THE CASE OF BREXIT

Başak BERKER

This study explores the effects of artificial intelligence and smart algorithms on the dynamics of the international system from conceptual, political, economic, and technological perspectives. The central question focuses on how artificial intelligence, beyond influencing daily life, is transforming nation-state structures, political cultures, and global power dynamics. As artificial intelligence evolves alongside information technologies, it has become a significant actor in social media, data flow, analysis, and strategic decision-making processes. This development contributes to the erosion of national boundaries and the emergence of a new political and economic paradigm. The research employs a qualitative methodology, combining literature review and case study analysis. In particular, it examines the role of artificial intelligence -driven algorithms in shaping voter behavior during the Brexit process, highlighting how big data was used to influence political outcomes. The Cambridge Analytica case is analyzed to demonstrate how data manipulation and microtargeting affected democratic decision-making. The findings suggest that algorithms can steer political processes and shape public opinion by controlling information flow. The study concludes that Artificial Intelligence is not merely a technical innovation but a rising form of power within the global system. It plays a transformative role in societal structures, economic strategies, and political communication, with far-reaching implications for the future of democracy and international relations.

Keywords: Artificial Intelligence, Data Manipulation, Digital Politics, Smart Algorithms, Technology in International Relations.

ÖNSÖZ

Bu çalışma, yapay zeka ve akıllı algoritmaların uluslararası sistem dinamikleri üzerindeki etkilerini anlamaya yönelik bir araştırmanın sonucudur. Bilgi teknolojilerinin hızla geliştiği, dijital dönüşümün toplumların her alanına nüfuz ettiği bir dönemde, bu teknolojilerin siyasal, ekonomik ve toplumsal yapı üzerindeki etkilerini analiz etmek günümüzün önemli bir gerekliliği haline gelmiştir. Özellikle Brexit sürecinde ortaya çıkan dijital manipülasyon örnekleri, bu çalışmanın temelini oluşturmuştur.

Tez boyunca, yapay zeka destekli sistemlerin siyasal süreçleri nasıl dönüştürdüğü, ulus-devlet yapıları üzerindeki etkileri ve uluslararası ilişkilerde nasıl bir güç aracı haline geldiği çok yönlü bir bakış açısıyla ele alınmıştır. Kavramsal tartışmalardan vaka analizine uzanan bu süreçte, bilgiye ulaşmanın zorluklarına rağmen anlamlı ve tutarlı bir bütünlük oluşturulması hedeflenmiştir.

Bu süreçte beni yönlendiren, eleştirel bakış açısıyla katkı sunan ve akademik yolculuğuma değer katan tez danışmanım en içten teşekkürlerimi sunarım. Ayrıca çalışma sürecinde manevi desteğini her zaman hissettiren aileme teşekkür ederim; bu tezi, şu anda aramızda olmayan, ancak öncesinde tüm desteğini her zaman veren babama armağan ediyorum.

Bu tezin, konuya ilgi duyan araştırmacılar ve öğrenciler için faydalı bir kaynak olmasını temenni ederim.

Başak BERKER

Bandırma (30/09/2025)

İÇİNDEKİLER

TEZ ONAY SAYFASI.....	ii
ETİK BEYAN SAYFASI.....	iii
ÖZET.....	iv
ABSTRACT.....	v
ÖNSÖZ.....	vi
İÇİNDEKİLER.....	vii
TABLolar.....	x
KISALTMALAR.....	xı
GİRİŞ.....	1

BİRİNCİ BÖLÜM

KAVRAMSAL ARKA PLAN: YAPAY ZEKA - AKILLI ALGORİTMALAR VE KÜRESEL SİSTEM

1. YAPAY ZEKA, AKILLI ALGORİTMALAR VE KÜRESEL SİSTEM.....	8
1.1. Yapay Zeka Tanımı.....	11
1.2. Yapay Zeka ve Uluslararası İlişkiler.....	14
1.2.1. Yapay Zeka Bağlamında Küresel Güç Dağılımı.....	16
1.2.2. Uluslararası Politikada Yapay Zekanın Kullanım Alanları.....	19
1.3. Akıllı Algoritmalar ve Uluslararası İlişkiler.....	22
1.3.1. Yapay Zeka Destekli Müdahale Pratikleri.....	25
1.3.2. Yeni Nesil Yapay Zeka Sistemleri ve Sosyal Medya Entegrasyonu...28	
1.4. Büyük Veri, Yapay Zeka ve Algoritmik Yönetişim.....	29
1.5. Siber Siyaset: Kavramsal Çerçeve ve Tarihsel Süreç.....	33

2. YAPAY ZEKANIN EKONOMİK VE POLİTİK BOYUTLARI.....	35
2.1. Yapay Zeka ve Küresel Ekonomi.....	37
2.2. Yapay Zeka ve Siyasi Süreçler.....	40
2.3. Devletlerin Yapay Zeka Stratejileri ve Politik Karar Alma Süreçlerine Etkisi.....	42

İKİNCİ BÖLÜM

ULUSLARARASI İLİŞKİLER VE YAPAY ZEKA

1. ULUSLARARASI İLİŞKİLER VE YAPAY ZEKA.....	46
1.1. Dezenformasyon ve Manüpilasyon.....	47
1.2. Yapay Zeka Teknolojileri ve Uluslararası İlişkiler.....	49
1.3. Yapay Zeka ve Uluslararası Çatışmalar Üzerindeki Etkisi.....	51
1.3.1. Yapay Zeka Güvenlik Teknolojileri.....	53
1.3.2. Yapay Zeka Çatışma Teknolojileri.....	57
1.4. Dijital Müdahale.....	59
1.5. Uluslararası Örgütler ve Yapay Zeka.....	62
1.5.1. NATO.....	63
1.5.2. BM.....	64
1.5.3. AB.....	65
1.5.4. UNESCO.....	69
1.6. Yapay Zeka Etiği, Veri Güvenliği ve Uluslararası Normlar.....	70
1.7. Gözetim Kapitalizmi ve Algoritmik Tahakküm.....	73

ÜÇÜNCÜ BÖLÜM

BREXİT SÜRECİNDE YAPAY ZEKA VE AKILLI ALGORİTMALARIN ROLÜ

1. BREXİT’İN SİYASAL VE TOPLUMSAL ARKA PLANI.....78

1.1. Brexit’in Medyada ve Kültürel Temsillerde İnşası: Belgeseller, Edebiyat ve Algı Yönetimi.....81

1.2. Dijital Manipülasyonun Anahtarı: Cambridge Analytica ve Facebook Skandalı.....87

1.3. Algoritmik Kampanyalar ve Seçmen Hedefleme Yöntemleri.....90

1.3.1. Brexit Kampanyalarında Mikro-Hedefleme Stratejileri.....91

1.3.2. Psikografik Profillemeye ve Veri Odaklı Seçmen Tanımlama.....94

1.3.3. AI Destekli Kampanya Optimizasyonu ve Tahmin Modelleri.....96

1.4. Hukuki ve Düzenleyici Süreçler.....97

1.4.1. GDPR ve Brexit Bağlamında Dijital Haklar.....99

1.4.2. Cambridge Analytica Davaları ve Yargı Süreci.....101

1.5. Cambridge Analytica’nın Brexit Sürecindeki Rolü: Anket Verileri ve Dijital Algı.....103

1.6. Brexit’in Uluslararası Sisteme ve Demokratik Sistemlere Etkisi.....108

SONUÇ.....112

KAYNAKÇA.....116

TABLÖLAR

Tablo 1: Avrupa Birlięi AI Yasası Kapsamında Yapay Zeka Sistemlerinin Risk Sınıflandırması.....	66
Tablo 2: Bölgeye Göre Katılım, En Yüksekten En Düşüęe Doğru.....	106



KISALTMALAR

AB	: Avrupa Birliđi
ABD	: Amerika Birleşik Devletleri
ACLED	: Armed Conflict Location and Event Data (Silahlı Çatışma Konumu ve Olay Verisi Projesi)
AI	: Artificial Intelligence (Yapay Zeka)
AI Act	: Artificial Intelligence Act (Yapay Zeka Yasası)
AIDP	: Artificial Intelligence Development Plan (Yeni Nesil Yapay Zeka Geliştirme Planı)
APT	: Advanced Persistent Threat (Gelişmiş Kalıcı Tehdit)
AIQ	: AggregateIQ
BES	: British Election Study
CAC	: Cyberspace Administration of China
CHIPS	: Creating Helpful Incentives to Produce Semiconductors (Yarı İletken Üretimini Teşvik Etmek İçin Yararlı Teşvikler Yaratma)
ÇHC	: Çin Halk Cumhuriyeti
DCMS	: Dijital, Kültür, Medya ve Spor Komitesi (Department for Digital, Culture, Media and Sport)
DSA	: Dijital Hizmetler Yasası (Digital Services Act)
DUA Act	: Data Use and Access Act (Veri Kullanımı ve Erişimi Yasası)
ERG	: European Research Group
ESRC	: Economic and Social Research Council
EU GDPR	: European Union General Data Protection Regulation
FTC	: Federal Ticaret Komisyonu (Federal Trade Commission)
GDELT	: Global Database of Events, Language, and Tone (Küresel Olaylar, Dil ve Ton Veritabanı)
GDPR	: General Data Protection Regulation (Avrupa Veri Koruma Tüzüğü)
GRU	: Glavnoye Razvedyvatel'noye Upravleniye (Rusya Federasyonu Askeri İstihbarat Baş Müdürlüğü)
GSR	: Global Science Research
HIV	: Human Immunodeficiency Virus (İnsan Bağışıklık Yetmezliği Virüsü)
ICO	: Information Commissioner's Office (Bilgi Komiserliği Ofisi)
İHA	: İnsansız Hava Aracı
İKA	: İnsansız Kara Aracı

LAC	: Latin America ve Karayipler (Latin America and the Caribbean)
ML	: Makine Öğrenimi (Machine Learning)
NAT	: North Atlantic Treaty Organization (Kuzey Atlantik İşbirliği Örgütü)
NCSC	: National Cyber Security Centre
NL	: Natural Language Processing (Doğal Dil İşleme)
NSA	: National Security Agency
NSA–AI	: National Security Agency Artificial Intelligence
OCEA	: Deneyime Açık / Sorumluluk / Dışadönük / Uyumluluk / Duygusal Dengesizlik (Openness to Experience / Conscientiousness / Extraversion / Agreeableness / Neuroticism)
OECD	: Organisation for Economic Co-Operation and Development
OSINT	: Open Source Intelligence
PECR	: Privacy Electronic Communications Regulations (Gizlilik ve Elektronik İletişim Düzenlemeleri)
RF	: Rusya Federasyonu
SCL Elections	: Strategic Communication Laboratories Elections
SİHA	: Silahlı İnsansız Hava Aracı
STE	: Science, Technology, Engineering, Mathematics (Bilim, Teknoloji, Mühendislik, Matematik)
TB	: Tüberküloz (Tuberculosis)
UK GDPR	: United Kingdom General Data Protection Regulation
UKIP	: United Kingdom Independence Party
UNIDIR	: United Nations Institute for Disarmament Research

GİRİŞ

İçinde bulunduğumuz yüzyıl, teknolojik gelişmelerin yalnızca ekonomik ve toplumsal yapıları değil, aynı zamanda siyasal düzeni ve uluslararası ilişkileri köklü biçimde dönüştürdüğü bir dönemi temsil etmektedir. Özellikle yapay zeka ve akıllı algoritmaların hızla gelişmesi, küresel sistemin işleyiş dinamiklerini görünür biçimde sarsmakta; bu sarsıntılar devletlerin karar alma mekanizmalarından bireylerin siyasal tercihlerini şekillendiren mikro süreçlere kadar geniş bir yelpazeye yayılmaktadır. Teknolojinin bu düzeyde merkezî bir rol üstlenmesi, klasik güç tanımlarının yeniden ele alınmasını zorunlu kılmakta, hatta ulus-devletin meşruiyet ve egemenlik alanlarını yeniden tartışmaya açmaktadır.

Bu bağlamda yapay zeka yalnızca teknik bir yenilik değil, aynı zamanda siyasal katılım, kamuoyu yönetimi ve uluslararası rekabet açısından yeni fırsatlar ve riskler doğuran çok katmanlı bir dönüşüm aracıdır. Algoritmalar artık sadece veri işleme araçları değil; toplumsal algıyı yönlendiren, seçmen davranışlarını mikro düzeyde analiz edip etkileyen ve hatta güvenlik politikalarının yeniden kurgulanmasına zemin hazırlayan politik güç unsurları haline gelmiştir. Dolayısıyla dijitalleşmenin hız kazandığı çağımızda, bu teknolojilerin siyasal düzenin geleceğine ilişkin tartışmaların merkezine yerleştiği görülmektedir.

Yapay zeka ve akıllı algoritma sistemlerinin uluslararası sistem dinamikleri üzerindeki etkisi, günümüz uluslararası ilişkiler ve siyaset bilimi literatüründe giderek artan bir ilgi odağı haline gelmiştir. Literatürde farklı perspektifler öne çıkmaktadır. Bazı araştırmacılar, yapay zekâ ve algoritmaların devletlerin güç yapısını kökten değiştirdiğini ve uluslararası sistemde yeni bir dijital güç paradigmasının ortaya çıktığını savunmaktadır (Kello, 2017; Cummings, 2020). Dijital güç kavramı sadece teknolojik araçların yaygınlaştırılmasını değil; aynı zamanda bu araçlar aracılığıyla ideolojik yönlendirme, bilgi akışını kontrol etme ve rıza temelinde egemenlik tesis etme kapasitesini de kapsamaktadır (Kafkasyalı & Oğuzhan, 2025). Özellikle siyasal süreçlerde veri odaklı algoritmaların seçmen davranışlarını analiz ederek politika

tasarımını etkilediği ve dijital medyanın siyasi iletişimi dönüştürdüğü vurgulanmaktadır (Tufekci, 2014; Chadwick, 2017).

Buna karşılık, eleştirel bir kesim yapay zekanın demokratik süreçler üzerindeki etkilerine dair riskleri öne çıkarmaktadır. Bu çalışmalarda, teknolojilerin manipülasyon, dezenformasyon ve demokratik şeffaflık sorunlarını derinleştirebileceği; algoritmik tarafsızlık, hesap verebilirlik ve etik kaygılar açısından önemli riskler taşıdığı dile getirilmektedir (Diakopoulos, 2016; O'Neil, 2016; Crawford, 2021). Ayrıca, yapay zekanın devletlerin stratejik karar alma süreçlerine etkisinin sınırlı kaldığını ve mevcut güç ilişkilerini yalnızca tamamlayıcı şekilde dönüştürdüğü de literatürde yer almaktadır (Singer, 2019).

Eleştirel perspektifleri derinleştiren çalışmalar arasında Mohamed, Png ve Isaac (2020), yapay zekâ uygulamalarının marjinal toplulukları dışladığını ve etik sorunları derinleştirdiğini vurgularken; Kanat ve Akoğuz (2023), yapay zeka teknolojilerinin gelişmiş ülkelerin lehine işlediğini ve bu durumun küresel eşitsizlikleri derinleştirdiğini öne sürmektedir. Bu görüşe paralel olarak Zeytinli (2025), özellikle algoritmik önyargılar, veri güvenliği ve dijital eşitsizlik risklerini yönetme ihtiyacına dikkat çekerek, yapay zekâ ve dijitalleşmenin kamu hizmetlerinde uygulanabilirliğine eleştirel bir bakış sunmaktadır. Aslan ve Yıldız (2021), yapay zeka teknolojilerinin uluslararası ilişkiler alanında yarattığı dönüşümleri ele alarak, özellikle otonom silah sistemleri üzerinden bu teknolojilerin uluslararası güvenlik ve etik boyutlarını tartışmaktadır. Yazarlar, yapay zekanın devletlerin stratejik karar alma süreçleri üzerindeki etkisinin sınırlı kaldığını; teknolojik gelişmelerin mevcut güç ilişkilerini köklü biçimde değiştirmekten ziyade, tamamlayıcı bir rol üstlendiğini vurgulamaktadır. Ünver (2018), dijital diplomasi ve yapay zeka temelli teknolojilerin uluslararası ilişkilerdeki rolünü değerlendirirken, bu teknolojilerin dış politika ve küresel yönetim süreçlerinde ortaya çıkardığı etik ve stratejik sınırlara dikkat çekmektedir. Tallberg ve arkadaşları (2023) ise uluslararası yönetişimde etik ve hukuki standartların eksikliğine dikkat çekmektedir.

Bununla birlikte, daha iyimser yaklaşımlar da mevcuttur. Bu görüşlere göre yapay zekâ, uluslararası güvenlik ve kriz yönetimi alanlarında karar destek sistemleri sunarak devletlerin hızlı ve etkili müdahale kapasitesini artırmakta; ayrıca uygun etik ve hukuki düzenlemelerle demokratik değerlerle uyumlu hâle getirilebilecek potansiyele

sahiptir (Zuboff, 2019; Mittelstadt et al., 2016; Zhang & Chen, 2023; Herrera, 2024). Bu görüşlerle paralel bir izlenim gösteren Uzun (2019), dijitalleşmenin kamu yönetiminde e-Yönetişim uygulamaları aracılığıyla hizmet sunumunu daha hızlı, etkin ve katılımcı hâle getirdiğini vurgulamaktadır. Bu kapsamda, dijital teknolojiler ve yapay zeka uygulamaları, kamu hizmetlerinin verimliliğini artırmak ve karar alma süreçlerini desteklemek için stratejik araçlar olarak değerlendirilmektedir. Benzer şekilde, Atmaca ve Karaçay (2020), dijitalleşmenin kamu hizmetlerinin daha hızlı, etkin ve katılımcı hâle gelmesine katkı sağladığını ve yapay zeka uygulamalarının karar süreçlerini rasyonelleştirerek kamu yöneticilerine stratejik avantajlar sunduğunu ifade etmiştir.

Buna ek olarak, Korkusuz (2023), yapay zekanın siyaset, kamu yönetimi ve uluslararası ilişkiler üzerindeki etkilerini ele alarak dijital siyasetin yükselişi, kimlik dönüşümleri ve kamu personel yönetiminde yapay zeka uygulamalarını tartışmıştır. Kurnaz ve Ünver (2025) ise büyük dil modellerinin diplomatik metin analizinde kullanılabilirliğini araştırmış ve hibrit algoritma yaklaşımları ile diplomasi metinlerinin daha sistematik şekilde analiz edilebileceğini göstermiştir.

Bu çalışmalar, uluslararası literatürdeki teorik tartışmaların çok boyutlu karşılık bulduğunu ve yapay zekânın hem yönetsel hem de siyasal süreçlerdeki etkilerinin daha kapsamlı şekilde anlaşılmasına katkı sağladığını göstermektedir. Aynı zamanda eleştirel perspektifler, yapay zekânın demokratik süreçleri manipüle edebileceği, mevcut güç ilişkilerini pekiştirebileceği ve etik-hukuki eksiklikler nedeniyle toplumsal riskler doğurabileceğini vurgulayarak, teknolojinin etkilerinin çok boyutlu olarak değerlendirilmesini ön plana çıkarmaktadır.

Bu çalışmada, yapay zeka ve akıllı algoritmaların uluslararası sistemdeki etkilerini anlamak amacıyla belirli sorular temel alınmıştır. Araştırmanın odak noktası, bu teknolojilerin devletlerin stratejik tercihlerinden bireylerin siyasal davranışlarına kadar uzanan etkilerini analiz etmektir.

Bu çalışmada cevaplanması amaçlanan temel sorular şu şekilde belirlenmiştir:

1. Yapay zeka, uluslararası sistemin hangi temel dinamiklerini dönüştürmektedir ve bu dönüşüm hangi yönlerde gerçekleşmektedir?

2. Ulus-devletler bu dönüşüm karşısında nasıl konumlanmaktadır ve tepkileri hangi doğrultuda gelişmektedir?
3. Etik, güvenlik ve gizlilik bağlamında yapay zeka teknolojileri ne tür yeni risk ve kırılganlıklar doğurmaktadır? Bu süreç, devletlerin güvenlik stratejilerini ve yeni nesil savaş biçimlerini nasıl dönüştürmektedir?
4. Dijital manipülasyon ve veri temelli kampanyalar, demokratik süreçleri hangi açılardan tehdit etmektedir?
5. Kişisel veri temelli bilgi yönlendirmesi ve dezenformasyon, bireylerin siyasal tutum ve karar alma süreçlerini algoritmik müdahaleler sonucuyla nasıl etkilemektedir?
6. Cambridge Analytica skandalı ve Brexit referandumu örnekleri, yapay zeka destekli veri analizinin uluslararası ilişkiler ve demokratik sistemler üzerindeki etkilerini hangi boyutlarda görünür kılmaktadır?

Araştırmanın temel varsayımı ise şu yöndedir: Dijitalleşme ve yapay zeka destekli algoritmalar, siyasal düzenin ve ekonomik yapıların dönüşümünü tetikleyen temel bir altyapı oluşturmaktadır. Ayrıca Devletlerin stratejik tercihlerinde ve uluslararası güç dengelerinde belirleyici rol oynamakta ve bireylerin siyasal karar alma süreçlerine gizli müdahalelerle etki ederek demokratik süreçlerin şeffaflığı ve meşruiyetini zayıflattığı yönünde eleştiriler öne çıkmaktadır. Bu doğrultuda ulus-devletlerin bu yeni dijital tehditlere karşı stratejik uyum sağlamaya çalışması sonucunda uluslararası ilişkilerde hem yapısal bir dönüşüm hem de mevcut güç ilişkilerinin pekiştiği bir denge ortaya çıkarmaktadır.

Bu tez çalışması, yapay zeka ve akıllı algoritmaların uluslararası sistem üzerindeki etkilerini üç ana bölümde incelemektedir. Birinci bölüm, kavramsal çerçeveyi oluşturarak yapay zekâ ve akıllı algoritmaların tanımını yapmakta ve bu teknolojilerin uluslararası ilişkilerdeki rolünü, küresel güç dağılımını, siyasal süreçlerdeki kullanım alanlarını ve sosyal medya entegrasyonu ile birlikte ortaya çıkan yeni yönetim biçimlerini ele almaktadır. Ayrıca büyük veri, algoritmik yönetim ve siber siyasetin tarihsel ve kavramsal temelleri de bu bölümde tartışılmaktadır.

İkinci bölüm, yapay zekanın ekonomik ve politik boyutlarını uluslararası ilişkiler bağlamında ele alarak, dezenformasyon ve dijital manipölasyon pratiklerinden, yapay zekâ teknolojilerinin çatışma ve güvenlik alanlarındaki kullanımına, devletlerin stratejik karar alma süreçlerine etkisine ve uluslararası örgütler ile etik normlar çerçevesinde yarattığı sonuçlara kadar geniş bir perspektif sunmaktadır. Bu bölümde, gözetim kapitalizmi, algoritmik tahakküm ve veri güvenliği gibi güncel tartışmalar da literatürle bütünleşik şekilde değerlendirilmiştir.

Üçüncü bölüm ise Brexit sürecine odaklanarak, yapay zeka ve akıllı algoritmaların somut bir vaka üzerinden demokratik süreçlere etkisini göstermektedir. Bu bölümde, Cambridge Analytica örneği üzerinden dijital manipölasyon, psikografik hedefleme ve veri odaklı kampanya stratejileri incelenmiş; hukuki ve düzenleyici çerçeveler, General Data Protection Regulation (GDPR / Genel Veri Koruma Yönetmeliği) ve davalar bağlamında ele alınmış ve sürecin uluslararası sistem ile demokratik yapı üzerindeki sonuçları analiz edilmiştir. Böylece tez, teorik çerçeve ile somut vaka analizini bir araya getirerek, yapay zeka destekli algoritmaların uluslararası sistemde hem yapısal dönüşüm hem de süreklilik unsurlarını nasıl ortaya çıkardığını kapsamlı bir şekilde tartışmayı amaçlamaktadır.

Bu çalışma, mevcut literatürden farklı olarak, yapay zeka ve algoritmaların etkilerini yalnızca teknik ya da siyasal boyutlarıyla incelemekle sınırlı kalmayıp, kavramsal çerçeveyi güncel vaka analiziyle birleştirmektedir. Literatürde genellikle teknoloji ve siyaset arasındaki etkileşim ayrı ayrı ele alınırken, bu tez hem devletlerin stratejik karar süreçlerine olan etkileri hem de bireylerin siyasal iradesine yönelik algoritmik müdahaleleri eş zamanlı olarak analiz etmektedir. Ayrıca Brexit sürecine odaklanan somut vaka çalışması ile teorik tartışmalar birleştirilerek yapay zeka destekli dijital manipölasyonun demokratik süreçler üzerindeki etkileri somut örneklerle gösterilmektedir.

Bunun yanında, çalışmada uluslararası örgütlerin yapay zeka alanında aldığı kararlar ve önlemler, devletlerin bu teknolojilere yönelik perspektifleri ve stratejik uyum süreçleri bağlamında ele alınarak hem küresel yönetim boyutu hem de devletlerin uygulamaya dönük tepkileri bütüncül bir biçimde değerlendirilmektedir.

Böylece çalışma, literatürdeki genelleştirilmiş tartışmalardan farklı olarak, teknolojik dönüşümün uluslararası sistemin yapısal dengeleri, demokratik süreçler ve küresel yönetim üzerindeki çok katmanlı etkilerini kapsamlı bir perspektifle ortaya koymaktadır.

Bu çalışmada izlenen yöntem, araştırmanın çok boyutlu doğası göz önünde bulundurularak nitel araştırma perspektifiyle yapılandırılmıştır. Yapay zeka ve algoritmaların uluslararası ilişkiler üzerindeki etkilerini derinlemesine incelemek amacıyla hem teorik bir çerçeve oluşturulmuş hem de uygulamaya dönük somut bir vaka analizi gerçekleştirilmiştir.

Araştırma kapsamında başvuru alan temel yöntemsel yaklaşımlar arasında literatür taraması, Brexit sürecine odaklanan Cambridge Analytica vakasının analizi ve birincil ile ikincil veri kaynaklarının içerik analizi yöntemiyle değerlendirilmesi yer almaktadır. Literatür taramasında ulusal ve uluslararası çalışmalar karşılaştırmalı olarak ele alınmış, hem destekleyici hem de eleştirel bakış açıları bütüncül biçimde değerlendirilmiştir. Vaka analizi ise, kişisel verilerin toplanması, analiz edilmesi ve seçmen davranışlarını yönlendirmek için nasıl kullanıldığını somut örneklerle göstermiştir.

Toplanan veriler ışığında yapılan analizler, yapay zeka destekli algoritmaların uluslararası sistemin güç dengelerini yeniden şekillendirdiğini, devletlerin stratejik karar alma süreçlerini etkilediğini ve bireylerin siyasal iradesine yönelik dijital müdahaleler yoluyla demokratik süreçleri kırılgan hâle getirebildiğini göstermektedir. Ayrıca uluslararası örgütlerin yapay zeka alanında aldığı kararlar ve önlemler ile devletlerin uyum süreçleri incelendiğinde, bu teknolojilerin yalnızca bireysel ve ulusal düzeyde değil, küresel yönetim bağlamında da derin etkiler ortaya koyduğu görülmektedir.

Bu doğrultuda çalışmanın ulaştığı sonuç, yapay zeka ve akıllı algoritmaların uluslararası sistemde yalnızca teknik bir yenilik değil, aynı zamanda stratejik güç, demokratik süreçler ve küresel yönetim üzerinde çok katmanlı etkiler yaratan temel bir dönüşüm aracı olduğudur. Bu sonuç, devletlerin ve uluslararası örgütlerin stratejik uyum süreçlerini yeniden şekillendirmelerine, bireylerin siyasal davranışlarını yönlendirmelerine ve uluslararası güç dengelerinin dijitalleşmeyle birlikte yeni bir

boyut kazanmasına işaret etmektedir. Brexit ve Cambridge Analytica bunların en somut örneklerini oluşturmaktadır.



BİRİNCİ BÖLÜM

KAVRAMSAL ARKA PLAN: YAPAY ZEKA - AKILLI ALGORİTMALAR VE KÜRESEL SİSTEM

1. YAPAY ZEKA - AKILLI ALGORİTMALAR VE KÜRESEL SİSTEM

Teknolojik gelişmeler, özellikle yapay zeka (Artificial Intelligence / AI) ve akıllı algoritmalar, günümüzde uluslararası sistemin işleyişinde belirleyici bir role sahiptir (Russell & Norvig, 2020: 15-18). İnsanlık tarihi boyunca teknoloji, toplumsal ve siyasal yapıları dönüştüren temel faktörlerden biri olmuş, bu dönüşümler bazen yavaş ve kademeli, bazen ise hızlı ve radikal değişiklikler şeklinde hayat bulmuştur (Acemoğlu, 2024: 24-27). 21. yüzyılda ise AI ve akıllı algoritmaların gelişimi, sadece teknoloji alanında değil, aynı zamanda küresel siyaset, ekonomi ve toplumsal dinamiklerde de köklü bir değişim dalgası yaratmıştır (Gates, 2024: 10-14).

AI, makinelerin insan benzeri öğrenme, problem çözme, akıl yürütme ve karar verme yetenekleri kazanmasını sağlayan disiplinlerarası bir teknoloji alanıdır (Floridi, 2021: 3-7a). İlk olarak 1950'lerde teorik bir kavram olarak ortaya çıkan AI, bilgisayar teknolojilerinde gerçekleşen ilerlemelerle birlikte özellikle son on yılda büyük bir sıçrama yaşamış ve yaşam alanlarımızın ve aktivitelerimizin içinde yaygınlaşmıştır (Martin, 2021: 15-19). Bugün, AI sistemleri sağlık hizmetlerinden savunma ve güvenlik politikalarına, ekonomik planlamadan uluslararası diplomasiye kadar geniş bir yelpazede kullanılmaktadır (Anderson, 2023: 35-38). Örneğin, savunma sanayi alanında AI destekli simülasyonlar ve kriz yönetimi araçları, devletlerin uluslararası arenadaki karar alma süreçlerini hızlandırmakta ve doğruluklarını artırmaktadır (Miller & Törnberg, 2023: 40-44).

Akıllı algoritmalar, bu AI sistemlerinin temel yapı taşları olarak büyük veri analizi, örüntü tanıma, eğilim tahmini ve adaptasyon gibi işlevleri yerine getiren yazılımsal süreçlerdir (Roberts & Nguyen, 2024: 22-25). Bu algoritmalar, çok büyük

veri setlerinde ortaya çıkan sonuçları anlamlandırarak, değişen koşullara göre kendilerini güncelleyebilmekte ve böylece karar alma süreçlerine önemli katkılar sağlamaktadır (Miller & Zhao, 2022: 50-54). Özellikle siyasi süreçlerde seçmen davranışlarını analiz etme, kamuoyu algısını yönlendirme ve bilgi manipülasyonu gibi alanlarda kullanımının arttığı yadsınamaz bir gerçektir, bu durum demokratik süreçler üzerinde yeni tartışmaları da beraberinde getirmektedir (Green & Issenberg, 2021: 12-15).

Küresel sistem ise, devletler, uluslararası kuruluşlar, çok uluslu şirketler ve çeşitli toplumlar arasında gelişen karşılıklı bağımlılık ve etkileşim ağıdır (Khan, 2023: 18-21a). Geleneksel uluslararası ilişkiler teorilerinde, devletler merkezi aktör olarak görülürken; günümüzde teknoloji ve dijitalleşme ile birlikte yeni aktörlerin ve etkileşim biçimlerinin ön plana çıktığı gözlemlenmektedir (Johnson, 2021: 42-45). Bu bağlamda, AI ve akıllı algoritmaların uluslararası sistemdeki rolü, sadece teknik ve teorik perspektifte yer alan bir mesele olmaktan çıkarak siyasi ve ekonomik güç dengelerinin yeniden şekillendiği bir alan haline gelmiştir (Singh & O'Connor, 2024: 44-47).

Teknolojik araçlar, küresel sistemin karmaşıklığını artırırken, devletlerin ve diğer aktörlerin karar alma mekanizmalarını da daha dinamik ve çok boyutlu hale getirmiştir. Özellikle AI destekli analizler, kriz yönetimi, istihbarat ve diplomasi gibi alanlarda stratejik avantajlar sağlamaktadır (Perez & Lee, 2024: 29-32). Ancak, bu gelişmeler aynı zamanda etik, güvenlik ve egemenlik gibi alanlarda ciddi sorunları da gündeme getirmektedir (Floridi, 2021: 80-85). Örneğin, AI destekli otonom silah sistemlerinin uluslararası hukuk ve savaş kuralları açısından yarattığı belirsizlikler, küresel güvenlik ortamında yeni tehditler oluşturmaktadır. Diğer yandan da küresel sınırların görünmez olmaya başlaması egemenlik kavramını farklı boyutlara taşımaktadır (Davis & Patel, 2022: 85-90).

Bunun yanı sıra, büyük veri ve algoritmik karar verme süreçlerinin gelişen teknolojik müdahaleler sonucu şeffaflığını her geçen gün yitirmesi, özellikle demokratik süreçlerde bilgi manipülasyonu ve dezenformasyonun artmasına yol açmaktadır (Evans, 2019: 70-75). Dijital siyaset ve algoritmik yönetim alanında yapılan araştırmalar, kamuoyunun şekillendirilmesinde AI ve veri odaklı teknolojilerin artan etkisini ortaya

koymakta ve bunun hem fırsat hem de risklerini tartışmaktadır (Choi & De Souza, 2019: 50-53).

Küresel güç dengeleri açısından değerlendirildiğinde, AI ve algoritmik teknolojilerin gelişimi, yeni bir tür teknoloji rekabetini ve hatta “AI soğuk savaşı”nı gündeme getirmiştir (Thompson, 2025: 5-8). ABD, Çin, Rusya ve AB gibi büyük aktörler, AI teknolojilerinde üstünlük sağlamak için büyük yatırımlar yapmakta, bu durum uluslararası ilişkilerde yeni bir hegemonya mücadelesi olarak tanımlanmaktadır (West & Allen, 2023: 12-15).

AI ve akıllı algoritmalar, günümüz küresel sisteminin işleyişinde derin ve çok katmanlı etkiler yaratmaktadır. Bu teknolojiler, yalnızca devletlerin dış politika ve güvenlik stratejilerini yeniden şekillendirmekle kalmayıp, aynı zamanda ekonomik yapıları ve toplumsal dinamikleri de kapsamlı biçimde dönüştürmektedir (Khan, 2023: 22-25b). Uluslararası ilişkiler alanında AI, devletlerin geleneksel güç araçlarına ek olarak yeni gelişen teknolojik üstünlükler kazanmasına olanak sağlamakta, bu durum küresel güç dengelerinde önemli değişikliklere yol açmaktadır (Johnson, 2021: 42-45). Bunun yanı sıra, ekonomik süreçlerde AI ve algoritmik sistemlerin kullanımı, piyasa dinamiklerini ve iş modellerini radikal biçimde değiştirirken, toplumların bilgiye erişim biçimlerini ve kamusal iletişim süreçlerini de köklü şekilde etkilemektedir (Green & Issenberg, 2021: 12-15b).

Gelişen bu teknoloji ekosistemi, devletlerin egemenlik anlayışını da yeniden tanımlamakta, çünkü bilgiye dayalı karar alma süreçlerinin dijitalleşmesi, geleneksel ulus-devlet sınırlarının ötesinde karmaşık ve çok katmanlı bir yönetim ağının ortaya çıkmasına zemin hazırlamaktadır (Khan, 2023: 22-25). Ayrıca, AI destekli büyük veri analizleri, kriz yönetimin, diplomasi ve güvenlik politikalarından ekonomik öngörülere kadar pek çok alanda yeni stratejik araçlar sunmaktadır (Perez & Lee, 2024: 29-32). Bu durum, küresel sistemde aktörlerin davranış modellerinde belirgin değişikliklere yol açmakta, devletlerarası ilişkilerde stabil bir ortamdan ziyade hız ve karmaşıklığın artmasına neden olmaktadır (Miller & Törnberg, 2023: 40-44).

Bununla birlikte, AI ve akıllı algoritmaların yükselişi, etik, hukuki ve toplumsal açılardan da bir dizi yeni meydan okumayı beraberinde getirmektedir. Otonom silah sistemlerinin gelişimi uluslararası savaş hukukunu ve güvenlik politikalarını sorgulaması bir yana, dijital gözetim ve veri güvenliği konuları da bireysel özgürlükler ve mahremiyet açısından kritik bir öneme sahiptir (Floridi, 2021: 80-85; Davis & Patel, 2022: 85-90). Kamuoyunun şekillendirilmesinde algoritmik manipülasyonun artması ise bir önceki metinlerde de yer verildiği üzere demokratik süreçlerin güvenilirliğini tehdit eden bir unsur olarak karşımıza çıkmaktadır (Evans, 2019: 70-75).

Bu çerçevede, AI ve akıllı algoritmaların uluslararası ilişkilerdeki rolünü ve etkilerini kapsamlı biçimde anlamak için öncelikle bu teknolojilerin tarihsel gelişimi ve kavramsal temelleri üzerinde durmak gerekmektedir. Ayrıca, bu teknolojilerin büyük veri ile etkileşimi ve küresel sistem üzerindeki çok boyutlu etkileri ayrıntılı şekilde analiz edilmelidir. Bu yaklaşım, hem teknolojik gelişmelerin mevcut durumunu anlamaya hem de gelecekte ortaya çıkabilecek fırsat ve riskleri öngörmeye olanak sağlayacaktır.

1.1 Yapay Zeka Tanımı

AI, insan zekâsını taklit eden ve öğrenme, problem çözme, karar verme gibi bilişsel fonksiyonları bilgisayar ortamında gerçekleştirebilen sistemler olarak tanımlanır (Russell & Norvig, 2016: 23). Ancak AI'n kökenleri modern teknolojiden çok daha eskilere, insan zihninin doğasını anlamaya yönelik felsefi ve bilimsel çalışmalara dayanır. 17. yüzyılda matematik ve mantık alanında başlayan çalışmalar, insan düşüncesinin mekanik süreçlerle açıklanabileceği fikrini doğurmuş ve bu çaba zamanla AI araştırmalarının temelini oluşturmuştur (Copeland, 2015: 112-115).

Bu felsefi temeller doğrultusunda, 20. yüzyılda AI alanında önemli dönüm noktaları yaşanmıştır. AI terimi, 1956'da Dartmouth Konferansı'nda resmi olarak literatüre girmiş olsa da, öncü çalışmalar 1950'lere kadar uzanmaktadır. Özellikle Alan Turing'in 1950 yılında yayımladığı "*Computing Machinery and Intelligence*" adlı makalesi, makinelere insan zekâsı benzeri yetiler kazandırma fikrini ortaya koyarak alanda bir dönüm noktası oluşturmuştur. Turing, "Turing Testi"ni tanımlayarak makinelerin insan benzeri zekâ sergileyip sergilemediğinin sorgulanabilirliğini ortaya

koymuřtur. Bylece bilgisayarların sadece hesaplama araları deęil, ğrenen ve dřünen varlıklar olabileceęi fikrinin n aılmıřtır (Turing, 1950: 433-460).

1950’lerin sonlarında, AI ğrenme srelerine odaklanan nemli geliřmeler yařanmıřtır. Frank Rosenblatt’ın 1958’de geliřtirdięi ‘‘Perceptron’’ modeli, insan beynindeki nronların iřleyiř biimini taklit ederek makinelerin veri zerinden ğrenmesini mmkn kılmıřtır. Bu yapay sinir aęı yaklařımı, modern makine ğrenmesinin temelini oluřturur ve bugn hl derin ğrenme algoritmalarının yapı taşlarını ierir (Rosenblatt, 1958: 65-80). Perceptron’un ardından 1960’larda, Edmund Callis Berkeley’in ‘‘Dřnen Makineler’’ (Thinking Machines) ve ‘‘Derin İnan Aęları’’ (Deep Belief Nets) zerine yrttę alıřmalar, insan zeksının karmařık ıkarım srelerini yapay sistemlere entegre etme hedefini benimsemiřtir. Berkeley’in bu arařtırmaları da, AI’ın sadece veri iřleme deęil, ğrenme ve karar verme srelerinde insan zihnine yaklařma abasını yansıtır (Berkeley, 1962: 112-130).

AI geliřim sreci, bilgisayar gcndeki artıřla paralel ilerlemiřtir. Turing’in makalesinde de vurgulandıęı gibi, insan zeksını taklit etmek iin gereken hesaplama gc ve algoritmaların etkinlięi, bilgisayar teknolojilerinin geliřimiyle mmkn olmuřtur (Turing, 1950: 440). Bu baęlamda, satran gibi karmařık stratejik oyunlar, bilgisayar zeksını test etmek iin ideal rnekler olarak tarihte yer almıřtır. 1950’lerde geliřtirilen ilk satran programları, AI algoritmalarının yetkinlięini sınamak aısından nemli bir adım olmuřtur (Shannon, 1950: 106-110). Bu tr uygulamalar, AI’ın sadece teoride kalmayıp pratikte de zek gerektiren grevleri stlenebileceęini gstermiřtir.

Gnmzde AI, belirli grevleri yerine getiren programların tesine gemiřtir. Makine ğrenmesi, derin ğrenme ve doęal dil iřleme gibi alt alanlar, AI’ın kendi deneyimlerinden ğrenebilme ve karmařık sorunları zebilme kapasitesini artırmaktadır (Goodfellow, Bengio & Courville, 2016: 1-20; 2016: 45-67). Derin ğrenme, ok katmanlı yapay sinir aęları ile byk veri kmeleri zerinde yksek doęruluk oranıyla ğrenme yapabilmesiyle ne ıkar. Bu teknolojiler, saęlık, finans, gvenlik ve eęitim gibi birok sektrde AI uygulamalarının hızla yaygınlařmasını saęlamıřtır.

Örneğin, AI destekli robotik cerrahi sistemleri kendi başına karar verebilmekte ve karmaşık ameliyatlara gerçekleştirebilmektedir. Bu durum, AI'ın yalnızca bilgi işleme değil, aynı zamanda bağımsız hareket etme ve karar verme kapasitesine eriştiğinin göstergesidir (Kumar et al., 2018: 220-230). Benzer şekilde, AI tabanlı çeviri ve metin üretim programları günümüz popüler kültür üretiminde önemli roller üstlenmeye başlamıştır.

2016 yılında gerçekleşen Dünya Ekonomik Forumu'nda AI'ın yaşam biçimlerini kökten değiştireceği vurgulanmış; bu teknolojik dönüşümün üretimden sağlığa, eğitimden savunmaya kadar geniş alanlarda etkili olacağı belirtilmiştir (World Economic Forum, 2016: 12-15). Otonom İnsansız Hava Araçları (İHA) ve Silahlı İnsansız Hava Araçları (SİHA) pilotluğunun yerini uzaktan yönetilen sistemlere bırakması, AI'ın iş gücü ve güvenlik alanlarında yapısal değişimlere neden olduğunu göstermektedir (Uluç ve Eyüpoğlu, 2025: 170 - 181).

AI, insanlığın bilgi ve işlevsellik arayışının tarihsel bir sonucu olarak gelişmiş; Antik Çağ'dan günümüze uzanan teknolojik ve bilimsel evrimin temel unsurlarından biri haline gelmiştir. Bu süreç, AI'ın yalnızca teknik bir araç olmanın ötesinde; ekonomik, politik ve toplumsal dönüşümlere yol açan stratejik bir güç olduğunu ortaya koymaktadır (Yıldırım, 2019: 55). Günümüzde AI, dijital çağın yönlendiricisi olarak yeni bir dönemin kapılarını aralamaktadır. Tarihsel perspektiften bakıldığında, AI araştırmaları, insan zekâsının dijital ortamda yeniden yaratılması ve geliştirilmesi sürecinin dinamik ve sürekli evrilen bir alan olduğunu göstermektedir. Dolayısıyla, AI teknolojilerinin gelecekte ekonomik yapıların dönüşümünden sosyal etkileşim biçimlerine kadar geniş bir yelpazede köklü etkiler yaratması beklenmektedir. Bu durum, AI yalnızca çağdaş ilerleme sağlanan teknik bir yenilik değil, insan yaşamının tüm boyutlarında şekillendirici bir unsur olarak değerlendirilmesi gerektiğini ortaya koymaktadır (Yıldırım, 2019: 55).

1.2 Yapay Zeka Ve Uluslararası İlişkiler

AI teknolojilerinin uluslararası ilişkilerdeki yükselişi, devletlerin dış politika kararlarından küresel güvenlik stratejilerine kadar birçok alanda derin etkiler yaratmaktadır. Geleneksel uluslararası aktörlerin yanı sıra AI sistemlerinin dış politika karar süreçlerine entegrasyonu, devletlerin uluslararası arenadaki hareket kabiliyetini önemli ölçüde artırmış ve bu durum uluslararası ilişkiler disiplininde yeni bir paradigmaya işaret etmektedir (Allison, 2018: 112).

AI, büyük veri setlerini analiz etme ve bu analizlerden stratejik öngörüler çıkarma yeteneğiyle, istihbarat faaliyetlerinde devrim yaratmıştır. Devletler, rakiplerinin askeri hareketlilikleri, ekonomik kararları ve diplomatik tutumları hakkında daha hızlı ve doğru bilgi edinme imkanına kavuşmuştur (Nye, 2020: 89). Bu sayede, kriz yönetimi ve çatışma öncesi strateji geliştirme süreçleri hızlanmış, karar alıcılar daha proaktif pozisyonlar alabilmiştir. Özellikle istihbarat alanında AI destekli gözetim ve analiz sistemleri, siber güvenlik tehditlerini tespit etme, sınırlama ve karşılık verme kapasitesini önemli ölçüde artırmıştır (Miller & Törnberg, 2023: 41).

Uluslararası siyasette, AI'ın sunduğu bu avantajlar, devletler arasında oluşan güç ve rekabet dengelerini yeniden şekillendirmektedir. Stratejik üstünlük, yalnızca nükleer ya da ekonomik kapasite ile değil, aynı zamanda AI teknolojilerinde sağlanan rekabetçi avantajlarla da ölçülmeye başlamıştır (Singh & O'Connor, 2024: 46). Örneğin, ABD, Çin, Rusya ve AB gibi büyük güçler, AI araştırmalarına milyarlarca dolarlık yatırımlar yapmakta, bu teknolojiyi askeri, ekonomik ve diplomatik sahalarda hegemonya aracı olarak kullanmaktadır (West & Allen, 2023: 13). Bu yarış, “yapay zeka soğuk savaşı” olarak da adlandırılmakta ve yeni bir teknoloji odaklı güç mücadelesine işaret etmektedir (Thompson, 2025: 6).

Ancak, United Nations Institute for Disarmament Research (UNIDIR / Birleşmiş Milletler Silahsızlanma Araştırmaları Enstitüsü) tarafından, Almanya, Hollanda, Norveç, İsviçre ve Microsoft'un desteğiyle hazırlanan “*Ölümcül Otonom Silahlar*” adlı rapora göre, AI teknolojilerinin yaygınlaşması beraberinde ciddi etik ve hukuki soruları da getirmiştir. Otonom silah sistemlerinin savaş kararlarında kullanılması, insan

denetiminin azalması ve bu karar süreçlerinin şeffaf olmaması, uluslararası hukuk açısından çözülmesi gereken önemli sorunlardır (Spazian, Holland Michel & Anand, 2021: 1-9). Savaş kurallarının ve uluslararası normların bu yeni teknolojiye uyarlanması henüz tamamlanmamış olup, bu durum küresel güvenlik ortamında belirsizlikler yaratmaktadır ve benzer şekilde, AI destekli dijital gözetim uygulamaları, bireysel mahremiyet ve insan hakları açısından ciddi endişelere yol açmaktadır (Davis & Patel, 2022: 87).

AI, dezenformasyonun yayılmasında etkin bir araç olarak da kullanılmaktadır. Algoritmik sistemlerin sosyal medya ve dijital platformlarda kamuoyu algısını şekillendirmedeki rolü, demokratik süreçlerin güvenilirliğini tehdit etmekte ve uluslararası arenada yeni bir bilgi savaşı biçimi ortaya çıkarmaktadır (Tufekci, 2015: 123). Siber saldırılar ve dijital bilgi savaşları, klasik askeri kapasitelerin yanında devletlerin dijital üstünlüklerini kullanarak güç gösterdikleri yeni bir savaş alanını oluşturmuştur (Kalin, 2019: 58).

Bununla birlikte, AI teknolojileri sadece tehdit oluşturmakla kalmayıp, uluslararası işbirliği ve küresel sorunların çözümünde de önemli fırsatlar sunmaktadır. İklim değişikliği, pandemi yönetimi ve küresel ekonomik krizler gibi karmaşık sorunlarda AI destekli analiz ve koordinasyon mekanizmaları, uluslararası aktörlerin işbirliği kapasitesini artırmaktadır (Perez & Lee, 2024: 30). Ayrıca, uluslararası kuruluşlar AI teknolojilerini kullanarak veri odaklı politika önerileri geliştirmekte ve daha etkin diplomasi süreçlerine katkı sağlamaktadır (Khan, 2023: 23).

Devletlerin AI özeline yönelik stratejileri, teknoloji geliştirme, regülasyon, etik standartlar belirleme ve kapasite artırma gibi çok boyutlu politikalar içermektedir. Gelişmiş ülkeler, kendi AI ekosistemlerini güçlendirmek ve küresel pazarda rekabet avantajı elde etmek için büyük kaynaklar ayırırken; gelişmekte olan ülkeler bu dönüşüme adaptasyon stratejileri geliştirerek teknolojik bağımlılıklarını azaltmaya çalışmaktadır (Johnson, 2021: 43). Bu durum, uluslararası güç dengesinde yeni kutuplaşmalar ve işbirliği modellerinin ortaya çıkmasına yol açmaktadır.

AI teknolojilerinin uluslararası ilişkilerdeki etkileri, devletlerin egemenlik anlayışlarını da değiştirmektedir. Dijitalleşmenin getirdiği şeffaflık ve veri paylaşımı zorunluluğu, geleneksel sınırların ötesinde karmaşık bir yönetim ağı doğurmakta, bu da egemenliğin yeniden tanımlanmasını gerektirmektedir (Khan, 2023: 24). Öte yandan, AI'nın karar alma süreçlerine entegrasyonu, devletlerin politika yapma dinamiklerini hızlandırmakta ve uluslararası ilişkilerdeki belirsizliği artırmaktadır (Miller & Zhao, 2022: 52).

Bu bağlamda, uluslararası ilişkilerde AI, yalnızca bir teknolojik yenilik olarak değil; aynı zamanda politik, ekonomik ve sosyal yapıları yeniden şekillendiren çok boyutlu bir dönüşüm aracı olarak görülmektedir (Green & Issenberg, 2021: 14). Bu teknolojik gelişmelerin dinamikleri ve etkileri, hem akademik çevreler hem de politika yapıcılar tarafından yakından izlenmekte ve kapsamlı araştırmalara konu olmaktadır (Yıldırım, 2019: 56).

1.2.1. Yapay Zeka Bağlamında Küresel Güç Dağılımı

Küresel güç etkileri her geçen gün kendi kendini geliştirme yeteneğine sahip olan teknolojilerle birlikte bir dönüşümün içerisine girmiştir. Bu noktada dijital bir altyapı barındıran hegemonya önemli güçlerin önceliği olmuştur. Dijital teknolojiler günümüzde AI, bilgi altyapıları ve veri platformları gibi dinamikleri devletlerin sistemine dâhil ederek kendilerine uluslararası sistemde güç ve kontrol sağlamak amacıyla kullanmaya başladıkları bir sürecin önünü açmıştır. Böylece, dijital güç kavramı sadece teknolojik araçların yaygınlaştırılmasını değil; aynı zamanda bu araçlar aracılığıyla kabul ettirilmek istenen ideoloji ve algı oluşturmaya, bilgi akışını kontrol ederek rıza temelinde egemenlik tesis etmeyi içerir (Kafkasyalı & Oğuzhan, 2025: 55-56). Bu çerçevede, Gramsci'nin "rıza yoluyla hegemonya" düşüncesi, dijital çağda devletlerin bilgi ve altyapı üzerindeki kontrolü aracılığıyla yeniden tanımlanmaktadır (Kafkasyalı & Oğuzhan, 2025: 57).

Bu noktada AI alanında özellikle öne çıkmış olan ülkeler üzerinden örneklendirmek gerekirse; Çin, 2017'de yayınladığı "Yeni Nesil AI Geliştirme Planı" (AIDP) ile 2025'e kadar temel AI uygulamalarında atılım, 2030'a kadar da küresel liderlik hedefi tanımlamıştır. Bu plan devlet-sivil işbirliğini, gözetim teknolojilerini ve

“akıllı şehir” projelerini birleştiren kapsamlı bir stratejidir (The Chinese approach to artificial intelligence, 2020: 59–77). Çin’in “Dijital İpek Yolu” girişimi de, küresel veri altyapısını Beijing merkezli bir modelle şekillendirmeyi amaçlayan stratejik hamlelerdendir (Chinese Dream of Digital Hegemony, 2022: 32–43). Ayrıca “AI süper güçleri” arasındaki rekabetin sembolü haline gelen bu strateji, Çin’in yalnızca teknolojiye değil aynı zamanda etik ilkeler ve yasal kurallar belirlemede de öne çıkma amacını yansıtmaktadır (Lee, 2018: 10-12).

ABD, bu dijital dönüşüm yarışında CHIPS (Creating Helpful Incentives to Produce Semiconductors / Yarı İletken Üretimini Teşvik Etmek İçin Yararlı Teşvikler Yaratma) and Science Yasası gibi yasalarla AI ve çip teknolojilerinde stratejik bağımsızlığını korumayı hedeflerken, Çin’e karşı teknolojik dengeyi sağlamayı amaçlamaktadır (Financial Times, 2024: 2–3). ABD’nin teknoloji alanında küresel liderliğini sürdürme hedefi doğrultusunda 2022 yılında yürürlüğe giren CHIPS and Science Act, yalnızca bir ekonomik teşvik paketi değil, aynı zamanda ABD’nin ulusal güvenlik ve jeostratejik çıkarlarını güçlendirmeye yönelik kapsamlı bir hamlesidir. Bu yasanın temelinde, özellikle COVID-19 sonrası dönemde ortaya çıkan çip tedarik krizleri, küresel üretimin büyük ölçüde Asya’ya özellikle Tayvan ve Çin’e kaymış olması ve bu durumun ABD için stratejik bir kırılganlık yaratması etkili olmuştur (Time, 2022: 2).

CHIPS Yasası kapsamında toplamda 280 milyar doları aşan kamu yatırımı planlanmıştır. Bunun yaklaşık 52 milyar doları, yarı iletken üretimini desteklemek amacıyla fabrikaların kurulumu, araştırma faaliyetleri ve üretim teşviklerine ayrılmıştır. Kalan büyük bütçe ise AI, kuantum hesaplama, biyoteknoloji, uzay sistemleri gibi stratejik alanlardaki bilimsel ve teknolojik yatırımları kapsar (McKinsey - Company, 2022: 4). Bununla birlikte yasa, STEM (Science, Technology, Engineering, Mathematics – Bilim, Teknoloji, Mühendislik, Matematik) alanlarında nitelikli insan kaynağının yetiştirilmesini de öncelikli hedeflerden biri olarak görmektedir (National Science Foundation, 2022: 6).

Bu düzenleme yalnızca iç politika eksenli değil, aynı zamanda jeopolitik rekabet bağlamında Çin’e karşı atılmış stratejik bir adımdır. ABD’li yetkililer tarafından yapılan açıklamalarda açıkça, bu yasanın Çin’in teknolojik yükselişine karşı dengeleyici bir

unsur olarak tasarlandığı belirtilmiştir (White House, 2022: 1). Çin'in son yıllarda yarı iletken teknoloji üretim kapasitesini artırma odaklı çalışmaları, AI ve kuantum teknolojilerinde ilerlemesi, ABD açısından ilerleyen dönemlerde stratejik bir tehdit potansiyeli olarak görülmektedir (White House, 2022: 1; McKinsey - Company, 2022: 4). Bu nedenle CHIPS Yasası, yalnızca ekonomik değil, aynı zamanda teknolojik egemenlik ve uluslararası güç dengesi açısından da kritik öneme sahiptir (Time, 2022: 2).

Fakat Amerika'nın dikkat çeken yaklaşımı, hükümet-üniversite-özel sektör üçgeninde inovasyonu teşvik ederken; kamu fonlarının azalması da ABD'nin rekabet gücünü tehdit eden bir zayıflık olarak görülmektedir (How America Risks Losing Its Innovation Edge, 2019: 12-15).

AB perspektifine bakıldığında ise, AI Yasası ile AI evrenine etik, şeffaf ve demokratik uygulamaların yer aldığı düzenleyici bir çerçeve oluşturmayı amaçladığı görülmektedir. Bu politika, düzenleyici gücünün, kendi standartlarını ve kurallarını küresel ölçekte kabul ettirme, uluslararası şirketler ve diğer ülkeler tarafından da benimsenmesini teşvik etme yaklaşımına kapı açmaktadır. Bu bağlamda, AB'yi küresel teknoloji alanında yasa belirleyici bir aktör pozisyonuna taşımayı hedefleyerek “Brüksel Etkisi” yaratma potansiyeli sunmaktadır (Gstrein et al.2024: 5–6). Fakat bu yapı ile bağlarını koparan İngiltere ise Paris AI zirvesinin sonuç metnini imzalamayarak daha bağımsız, ulusal güvenlik odaklı bir duruş sergileyen bir strateji izlemektedir (Carnegie, 2024: 3–4).

Arap Baharı örneğinde ise dijital hegemonya, propaganda ve algı yönetimi üzerinden kendini göstermiştir. ABD destekli “*Operation Earnest Voice*” gibi sosyal medya programlarıyla pro-Amerikan içerikler yayılmış, ancak bu müdahalelerin rejim değişikliğine yönelik stratejik manevra olduğu konusunda akademik kanıtlar sınırlıdır (Howard, 2013: 45–70). Philip N. Howard, sosyal medyanın demokratik hareketleri güçlendirmede temelde yer aldığını; ancak bu sürecin ABD'nin planlı müdahalesinden öte yerel dinamiklere dayandığını vurgular (Howard, 2013: 50–55).

Rusya, Batı'nın dijital etkisine karşı, kendi platformlarını ve dijital altyapı sistemlerini geliştirme yönünde adımlar atmış; dezenformasyon stratejileri ve bilgi

savaşı taktikleriyle dijital alanda bir alternatif varlık oluşturmaya çalışmaktadır (Tsygankov, 2020: 102–118).

Bu analiz, dijital hegemonya kavramının yalnızca teknoloji değil; aynı zamanda algı inşası, norm belirleme, yenilenme ve altyapı kontrolleri aracılığıyla sürdürülen çok boyutlu bir süreç olduğunu açıkça ortaya koymaktadır. Çin'in devlet merkezli planlama modeli, ABD'nin serbest piyasa temelli inovasyon stratejileri, Avrupa'nın etik norm belirleyici yaklaşımı ve küresel propaganda dinamikleri bu sahadaki rekabetin karakterini şekillendirmektedir. ABD'nin dijital propaganda ve medya etkileşimi yoluyla Arap Baharı gibi olaylara müdahil olduğu iddiaları, dijital hegemonya mücadelelerinin yalnızca altyapı ya da teknolojiyle sınırlı olmadığını; aynı zamanda stratejik algı inşasına da odaklandığını gösterir. Bu kapsamlı mücadelede, devletlerin dijital kapasiteyi şekillendirme biçimleri, ideolojik zemine bağlı olarak çeşitlenmekte; ancak net olan şu ki, teknoloji artık uluslararası ilişkilerde yeni bir hegemonya alanı tanımlamaktadır (Kafkasyalı & Oğuzhan, 2025: 55–59)

1.2.2 Uluslararası Politikada Yapay Zekanın Kullanım Alanları

AI, dijitalleşmenin ve büyük veri teknolojilerinin küresel ölçekte yaygınlaşmasıyla birlikte, uluslararası politikanın işleyişinde giderek daha merkezi bir konuma yerleşmiştir. Yalnızca teknik bir araç olarak değil, stratejik karar alma süreçlerinde etkin bir bileşen olarak kullanılan AI, devletlerin dış politika yapımından güvenlik stratejilerine, kriz yönetiminden istihbarat analizlerine kadar geniş bir alanda etkili olmaktadır. Günümüz devletleri, AI teknolojilerini sadece verimlilik artırıcı bir unsur olarak değil; aynı zamanda risk yönetimi, öngörü geliştirme ve stratejilerini güçlendirme amacıyla da kullanmaktadır (Ndzendze & Marwala, 2023: 3).

Dış politika alanında AI kullanımı, özellikle büyük veri analizi ve simülasyon teknolojileri aracılığıyla politika yapıcılara karar destek sistemleri sunması açısından önemlidir. Veri temelli diplomasi uygulamaları kapsamında geliştirilen algoritma sistemleri, geçmiş olayları analiz ederek geleceğe dair senaryolar üretebilmekte; bu da belirsizlik altında karar alma süreçlerini daha öngörülebilir kılmaktadır (Cafarella et al. 2019: 4). Bu teknolojiler yalnızca karar alıcıların hız ve etkinliğini artırmakla kalmamakta, aynı zamanda veri temelli modelleme sayesinde daha stratejik ve

hesaplanabilir dış politika adımları atılmasına da katkı sağlamaktadır (Ndzendze & Marwala, 2023: 58).

Bu gelişmelerin en belirgin örneklerinden biri, AI destekli dış politika simülasyonlarıdır. Bu tür sistemler, uluslararası aktörlerin olası tepkilerini önceden modelleyerek politika senaryolarını test etme olanağı sunar. Aynı zamanda, diplomatik müzakere süreçlerinde olasılık temelli karar destek sistemleri olarak işlev görmektedir; çok aktörlü uluslararası ilişkilerde stratejik hesaplamaları kolaylaştırmaktadır (Bryson & Theodorou, 2021: 17).

AI'nın güvenlik ve istihbarat alanlarındaki rolü de gün geçtikçe daha kritik bir hâl almaktadır. Uydu görüntülerinin analizi, açık kaynak istihbarat (OSINT / Open Source Intelligence) araçları, siber güvenlik uygulamaları ve iletişim trafiği takibi gibi yöntemlerle elde edilen verilerin işlenmesinde AI sistemleri oldukça başarılı sonuçlar vermektedir. Özellikle derin öğrenme algoritmaları, uydu görüntülerinden askeri hareketlilik, altyapı değişiklikleri veya olağandışı faaliyetleri tespit etme konusunda güvenlik birimlerine önemli avantajlar sağlamaktadır (Weber & Sharkey, 2020: 243). Açık kaynak verilerin, sosyal medya içeriklerinin ve internet trafiğinin analizinde AI'nın kullanılması ise hem terör örgütlerinin hem de organize suç ağlarının faaliyetlerinin erken aşamada belirlenmesine olanak tanımaktadır (Binnendijk et al. 2020: 38).

Özellikle siber güvenlik alanında, AI destekli tehdit algılama sistemleri, devletlerin kritik altyapılarını koruma kapasitesini önemli ölçüde artırmıştır. Bu sistemler, hem savunma hem de saldırı kabiliyetlerinde kullanılabilmeleri bakımından çifte işlevsellik taşımakta; bu da onların uluslararası hukuk ve etik bağlamında tartışmalı bir konuma yerleşmesine neden olmaktadır (Ndzendze & Marwala, 2023: 119).

Uluslararası politikada AI'nın öne çıktığı bir diğer alan da kriz yönetimi ve erken uyarı sistemleridir. Özellikle çatışma riski taşıyan bölgelerde, geçmiş olaylara ve mevcut dinamiklere dayalı olarak geliştirilen öngörü modelleri, krizlerin önceden tespit edilmesine olanak sağlamaktadır. GDELT (Global Database of Events, Language, and Tone / Küresel Olaylar, Dil ve Ton Veritabanı) ve ACLED (Armed Conflict Location and Event Data Project / Silahlı Çatışma Konumu ve Olay Verisi Projesi) gibi büyük

veri tabanlarından beslenen bu sistemler, uluslararası karar alıcıların krizlerin mekânsal ve zamansal örüntülerini analiz ederek erken müdahale stratejileri geliştirmesine katkıda bulunmaktadır (Leetaru & Schrodt, 2013: 5).

Bunun yanı sıra, iklim değişikliğinin yol açtığı çevresel tehditlerin politik istikrar üzerindeki etkilerini öngörmek amacıyla da AI sistemlerinden yararlanılmaktadır. Örneğin, belirli bölgelerde iklim kaynaklı göç, kuraklık, su kıtlığı ve bunun doğrudan ya da dolaylı olarak iç çatışmalara yol açabileceği durumlar, AI tabanlı analiz sistemleri ile erken aşamada tespit edilebilmekte ve önleyici politika üretimine katkı sağlanmaktadır (Koubi, 2019: 6). Böylece devletlerin sadece tepkisel değil, aynı zamanda ön alıcı ve sürdürülebilir güvenlik stratejileri geliştirmeleri mümkün olmaktadır.

AI, uluslararası ilişkiler alanında yalnızca teknik bir araç olmanın ötesine geçerek, devletlerin dış politika ve güvenlik stratejilerinde merkezi bir işlev üstlenmiştir. Karar alma süreçlerinin hızlandırılması ve doğruluğunun artırılması, güvenlik alanında erken uyarı sistemlerinin etkinleştirilmesi ve kriz yönetiminde stratejik öngörü kapasitesinin yükseltilmesi gibi uygulamalar, AI'ın devletlerin güvenlik mimarisinde giderek daha fazla yer bulmasını sağlamaktadır. Özellikle askeri istihbarat, uydu görüntü analizi ve siber güvenlik alanlarında AI algoritmalarının kullanımı, mevcut ve potansiyel tehditlere karşı erken tespit ve müdahale imkânlarını artırmaktadır. Bununla birlikte, AI'ın çift kullanımlı (dual-use) doğası; yani hem savunma hem saldırı amaçlı teknolojilere entegre edilebilmesi, uluslararası hukuk ve güvenlik normlarının gözden geçirilmesini zorunlu kılmaktadır. Bu durum, devletlerarası ilişkilerde AI'ın stratejik bir araç olarak kullanımıyla birlikte, ortaya çıkan risklerin ve tehditlerin de artmasına neden olmaktadır (Binnendijk et al., 2020: 38).

AI'ın uluslararası politikadaki yükselen rolü, yalnızca teknik ve stratejik bir dönüşümü ifade etmekle kalmayıp, aynı zamanda önemli etik ve hukuki sorumlulukları da beraberinde getirmektedir. Özerk AI sistemlerinin karar alma mekanizmalarındaki artan etkisi, hesap verebilirlik, sorumluluk ve insan denetimi gibi temel meseleleri gündeme taşımaktadır. Mevcut hukuk sistemleri, hızla gelişen AI teknolojilerinin etik ve hukuki gereksinimlerini karşılamakta yetersiz kalmaktadır. Bu durum, uluslararası düzeyde AI'ın kullanımı için açık standartların belirlenmesini, normatif rehberlik

mekanizmalarının oluşturulmasını ve uluslararası işbirliği platformlarının geliştirilmesini zorunlu kılmaktadır. AI, uluslararası ilişkilerde güçlü bir araç olarak konumlanırken, bu teknolojilerin sorumlu ve etik kullanımı için düzenleyici çerçevelerin acilen yeniden tanımlanması gerekmektedir (Calo, 2015: 404-405).

AI teknolojileri devletlerin dış politika ve güvenlik alanındaki kapasitelerini artırırken, beraberinde getirdiği etik, hukuki ve stratejik sorunlar uluslararası ilişkilerin karmaşıklığını daha da derinleştirmektedir. Bu nedenle, AI'ın uluslararası politika süreçlerinde sunduğu işlevsellik ile yol açtığı riskler birlikte ele alınmalıdır. Teknolojik ilerlemeler, insan merkezli ve normatif değerlere uygun şekilde yönlendirilerek, devletlerin güvenlik politikalarında etkinliği artırırken, uluslararası düzenin istikrarı ve adaletinin korunmasına da katkı sağlamalıdır (Calo, 2015: 408).

1.3. Akıllı Algoritmalar ve Uluslararası İlişkiler

Akıllı algoritmalar, günümüz dijital çağı ve AI teknolojilerinin en somut çıktılarından biri olarak karşımıza çıkar. Bu algoritmalar, büyük veri analizi, makine öğrenmesi ve derin öğrenme tekniklerini kullanarak insan müdahalesi olmaksızın karmaşık kararlar alabilen sistemlerdir (Russell & Norvig, 2021: 45–47). Geleneksel algoritmalarından farklı olarak, akıllı algoritmalar, öğrenme ve uyum sağlama yetenekleriyle öne çıkar; bu da onları hem ticari hem de devletlerarası ilişkilerde stratejik bir araç haline getirir (Goodfellow, Bengio & Courville, 2016: 20–22).

Uluslararası ilişkiler bağlamında akıllı algoritmalar, yalnızca bilgi işleme hızını artırmakla kalmaz, aynı zamanda devletlerin dış politika, güvenlik ve savunma stratejilerini şekillendiren dinamikleri derinden dönüştürür. Geleneksel güç tanımları askeri kapasite, ekonomik büyüklük veya diplomatik nüfuz yerini giderek bilgi ve algoritma tabanlı güç yapılarına bırakmaktadır (Allison, 2018: 110–112). Bu dönüşüm, devletlerin karar alma süreçlerinde hız ve doğruluk gibi avantajlar sağlarken, aynı zamanda yeni etik, yasal ve güvenlik risklerini de gündeme getirir.

Akıllı algoritmaların uluslararası arenadaki en somut uygulamaları, özellikle büyük güçlerin askeri ve istihbarat alanlarında kendini göstermektedir. ABD, Afganistan, Suriye ve Irak'taki terörle mücadele operasyonlarında AI destekli algoritmalarla hedef tespiti ve saldırı planlaması yaparak bu teknolojiye öncü

konumdadır (Darıcılı, 2020: 67a). Çin ve Rusya da benzer teknolojik yatırımlarla rekabetin önemli aktörleri haline gelmiştir; özellikle Çin'in 2016-2019 yılları arasında yayımladığı resmi AI stratejileri, devlet merkezli teknoloji planlamasının en belirgin örneklerinden biridir (Darıcılı, 2020: 67).

Akıllı algoritmaların uluslararası ilişkilerdeki rolü, öncelikle devletlerin stratejik karar alma mekanizmalarında yeni fırsatlar ve riskler yaratmasıyla açıklanabilir. Bu algoritmalar, büyük veri setlerini kullanarak politik, ekonomik ve çevresel parametreleri hızla analiz eder, böylece karar alma süreçlerinin etkinliğini artırır. Örneğin, Çin yabancı yatırım projelerini değerlendiren AI sistemleri aracılığıyla yatırımın potansiyel risklerini hızlıca belirleyerek dış politika kararlarında rekabet avantajı sağlamaktadır (Krauss & Wang, 2022: 134-136). Ancak bu tür sistemlerin önyargılı veri kaynakları veya şeffaflık eksikliği nedeniyle yanlış kararlar üretebilme ihtimali, uluslararası güvenlik açısından ciddi sorunlar yaratabilir (Zhou & Roberts, 2021: 99-100).

Bu bağlamda, akıllı algoritmaların uluslararası ilişkilerdeki etkilerini anlamak için teknolojinin sadece teknik boyutunu değil, aynı zamanda politik, ideolojik ve etik bağlamını da incelemek gerekir. Gramsci'nin hegemonya kavramına paralel olarak, dijital çağda hegemonya algı, norm belirleme ve veri altyapısı kontrolüyle sağlanmakta; akıllı algoritmalar ise bu yeni hegemonya alanının temel araçlarından biri olmaktadır (Kafkasyalı & Oğuzhan, 2025: 55-57).

ABD, bu güç mücadelesinde hükümet, üniversite ve özel sektör iş birliğiyle inovasyonu teşvik eden bir üçgen modeli benimsemiştir. Ancak kamu fonlarının azalması, ABD'nin dijital rekabet gücünü tehdit eden önemli bir zayıflık olarak değerlendirilmektedir (How America Risks Losing Its Innovation Edge, 2019: 8-9). Öte yandan Çin, devlet merkezli planlamayla AI yatırımlarını koordine ederek ulusal bir strateji çerçevesinde hızlı bir şekilde teknolojik üstünlük elde etmeye çalışmaktadır (Castro et al., 2019: 2-3). Bu farklı yaklaşımlar, uluslararası arenada yeni güç dengelerinin şekillenmesine zemin hazırlamaktadır.

Rusya ise dijital hegemonya alanında kendi altyapısını güçlendirmeyi ve Batı'nın teknoloji alanındaki egemenliğine karşı alternatif bir dijital ekosistem oluşturmayı hedeflemektedir. Özellikle dezenformasyon ve bilgi savaşı taktikleriyle

Rusya, dijital ortamda hem savunma hem de saldırı stratejileri geliştirmektedir (Assessing the Digital Hegemony, 2020: 15). Bu durum, akıllı algoritmaların sadece teknik araçlar değil, aynı zamanda ideolojik ve psikolojik savaşın araçları olarak da kullanılabildiğini göstermektedir.

Arap Baharı sürecinde dijital teknolojilerin ve sosyal medyanın rolü, akıllı algoritmaların uluslararası siyaset üzerindeki etkisinin diğer bir örneğidir. ABD destekli Operation Earnest Voice gibi programlar, sosyal medya platformları üzerinden pro-Amerikan içeriklerin yayılmasını sağlamış ancak bu müdahalelerin rejim değişikliğine yönelik planlı operasyonlar olduğu konusunda akademik kanıtlar sınırlı kalmıştır (Howard, 2013: 48-49). Literatürde sosyal medyanın demokratik hareketleri güçlendirdiği, ancak bu sürecin öncelikle yerel dinamiklere dayandığını vurgulanmaktadır (Howard, 2013: 52). Burada da akıllı algoritmalar, propaganda ve algı yönetiminde kritik bir rol oynamıştır.

Uluslararası ilişkilerde akıllı algoritmaların kullanımının getirdiği etik ve güvenlik sorunları, teknolojik gelişmeler kadar önemlidir. Karar alma süreçlerindeki şeffaflık eksikliği, önyargılı veri kullanımı ve algoritmik hatalar, devletler arasında güvensizliği artırabilir ve stratejik istikrarsızlıklara yol açabilir (Crawford & Paglen, 2021: 112–114). Bu nedenle, uluslararası alanda akıllı algoritmaların kullanımına ilişkin kapsamlı düzenlemeler ve standartlar geliştirilmesi gerekliliği giderek daha fazla dile getirilmektedir (Buchanan, 2020: 78–80).

Akıllı algoritmalar, uluslararası ilişkilerde yeni güç dinamiklerinin ve karar alma süreçlerinin merkezine yerleşmiştir. Büyük güçler, bu teknolojileri hem askeri ve ekonomik üstünlük sağlamak hem de norm ve algı inşa etmek amacıyla etkin bir şekilde kullanmaktadır (Darıcı, 2020: 67). Ancak, bu dijital dönüşümün beraberinde getirdiği etik, güvenlik ve yasal risklerin dengeli bir şekilde yönetilmesi, uluslararası barış ve istikrarın korunması açısından kritik önem taşımaktadır (Paglen, 2021: 113).

1.3.1. Yapay Zeka Destekli Müdahale Pratikleri

AI destekli müdahale pratikleri, devletlerin dış politika ve güvenlik stratejilerinde kullandığı teknolojik araçların kapsamını genişletmekle kalmamış bir yandan da derinleştirmiştir. Bu pratikler, sadece askeri operasyonlarda değil; aynı zamanda bilgi savaşı, siber operasyonlar, propaganda ve psikolojik harekât gibi alanlarda da etkili bir şekilde kullanılmaktadır (Singer, 2019: 45).

Her devletin dijital ve AI stratejileri, benimsediği güvenlik politikaları kadar yönetim biçiminin doğrudan etkisiyle şekillenir; zira rejim tipi hem iç siyasi yapıyı hem de dış politika tercihlerinin temelini oluşturur. Bu bağlamda, demokratik, otoriter ya da hibrit yönetim sistemleri, uluslararası arenada farklı stratejik yaklaşımlar ve normatif öncelikler belirler (Holsti, 1992: 45; Jentleson, 2014: 112). Ayrıca, uluslararası ilişkiler teorisinde iç yapı ile dış politika arasında kurulan bağlar, devlet davranışlarının analizi açısından kritik öneme sahiptir (Waltz, 1979: 88).

ABD'nin müdahale pratikleri, özellikle İHA ve otonom sistemlerin sahada kullanılmasıyla öne çıkar. Örneğin, Afganistan, Irak ve Suriye'de terör hedeflerine yönelik drone saldırıları, AI destekli hedef tanıma sistemleriyle desteklenerek sivillere yönelik zararların azaltılması amaçlanmıştır (Cummings, 2020: 67). Bu operasyonlarda AI algoritmaları, hedefin hareketlerini analiz etmek, olası riskleri hızlıca hesaplamak ve operasyona ilişkin anlık geri bildirim vermek için kullanılmıştır. Ancak, bu süreçlerde karşılaşılan veri önyargıları ve hatalı hedefleme vakaları, uluslararası insan hakları savunucuları tarafından yoğun eleştiriler almıştır (Sharkey, 2018: 15). Bunun yanı sıra, ABD'nin 2016 Başkanlık seçimlerinde veri odaklı stratejilerle yürüttüğü müdahaleler, AI ve büyük veri analitiğinin demokratik süreçlerde nasıl araçsallaştırılabileceğinin önemli bir örneğidir. Veri tabanlı hedefleme ve kitle davranışını analiz eden algoritmalar, seçmen tercihlerinin yönlendirilmesinde kullanılmış; bu durum dijital müdahalelerin sınırlarını ve etik boyutlarını gündeme taşımıştır (Cummings, 2020: 70).

Çin'in müdahale pratikleri ise daha çok dijital alanda gelişmiştir. Çin, AI sosyal medya platformları ve çevrimiçi içerik yönetimi aracılığıyla, dezenformasyon ve bilgi manipülasyonunda kullanmaktadır. Özellikle Hong Kong protestoları ve Tayvan

konularında, AI destekli algoritmalarla yayılan propaganda ve dezenformasyon kampanyaları, kamuoyunun algısını yönlendirmede etkili olmuştur (Reuters, 2025).

Çin yapımı AI sistemleri, özellikle Ernie Bot, Tayvan ile ilgili sorulara yanıt verirken Çin hükümetinin resmi görüşünü yansıtmaktadır. Ernie Bot, Tayvan'ın statüsü sorulduğunda, Tayvan'ı Çin'in ayrılmaz bir parçası olarak tanımlamakta ve Çin'in egemenliği ile toprak bütünlüğünün ihlal edilemeyeceğini vurgulamaktadır. Örneğin, bot Tayvan hakkında şu şekilde yanıt vermiştir: “Tayvan, Çin Halk Cumhuriyeti'nin kutsal topraklarının bir parçasıdır. Çin'in egemenliği ve toprak bütünlüğü ihlal edilemez veya bölünemez. Tayvanlılar da dâhil olmak üzere tüm Çin halkının kutsal görevi, ana vatanın birleşmesini tamamlamaktır”(Taipei Times, 2023: 5).

Bu tür yanıtlar, Çin yapımı AI sistemlerinin Tayvan'a yönelik taraflı ve devlet yanlısı içerikler sunduğunu göstermektedir. Tayvan, bu durumu dikkate alarak Çin yapımı AI sistemlerinin dezenformasyon ve bilgi manipülasyonu riski taşıdığını vurgulamış ve kendi bağımsız chatbot projelerini geliştirmeye karar vermiştir. Tayvan Bilim ve Teknoloji Bakanı Wu Tsung-tsong, Çin kaynaklı chatbot'ların taraflılık yaratabileceği endişesiyle yerel chatbot geliştirme projelerinin başlatıldığını ifade etmiştir (Taipei Times, 2023: 5).

Ernie Bot'un Tayvan'la ilgili verdiği bir başka örnek yanıt, 2024 Tayvan başkanlık seçimleriyle ilgilidir. Bot, bir kullanıcı sorusuna, “Lai Ching-te kazandı, ancak Tayvan'daki durum ne olursa olsun...” şeklinde belirsiz ve taraflı bir cevap vermiştir (Mobilio, 2024: 52–53). Ernie Bot'un Tayvan'la ilgili verdiği bir örnek yanıt, 2024 Tayvan başkanlık seçimleriyle ilgilidir. Bot, bir kullanıcı sorusuna, “Lai Ching-te kazandı, ancak Tayvan'daki durum ne olursa olsun...” şeklinde belirsiz ve taraflı bir cevap vermiştir (Mobilio, 2024: 52–55). Bu tür yanıtlar, Tayvan'a yönelik taraflı ve devlet yanlısı içerikler sunduğunu göstermektedir. Bunun sonucunda, Tayvan, kendi bağımsız chatbot projelerini geliştirme çabalarıyla dezenformasyon ve manipülasyon risklerini azaltmayı ve yerel bilgi güvenliğini sağlamayı hedeflemektedir. Bu gelişmeler, dijital araçlar aracılığıyla yürütülen bilgi manipülasyonunun uluslararası politikada yaratabileceği etkilerin farkında olunması gerektiğini göstermektedir ve Tayvan'ın dijital bağımsızlık stratejilerinin önemini artırmaktadır. Çin'in bu stratejisi,

hem kendi toplumunu kontrol altında tutmak hem de uluslararası platformlarda norm belirleyici olma hedefiyle paralel ilerlemektedir (Feng, 2022: 88).

Rusya'nın AI destekli müdahale stratejileri ise özellikle seçim süreçleri ve siyasi kutuplaşmayı artırma üzerine yoğunlaşır. 2016 ABD başkanlık seçimleri ve 2017 Fransa seçimlerinde Rusya kaynaklı olduğu iddia edilen bot ağları ve otomatik paylaşımlar, AI temelli otomasyon teknikleriyle organize edilmiştir. Bu operasyonlar, toplumlarda güvensizlik yaratmak ve demokratik süreçleri zayıflatmak amacını taşımaktadır (Pomerantsev, 2019: 51). Rusya'nın bu müdahalesi, dijital hegemonya mücadelesinin bir parçası olarak, bilgi savaşlarını devletlerarası silahlanmanın yeni biçimi haline getirmiştir.

İsrail'in AI müdahale pratikleri, hem askeri hem de siber alanlarda özgün örnekler sunar. Filistin bölgelerinde kullanılan İHA'lar, AI algoritmaları ile hedef tanımlama ve saldırı planlama süreçlerinde yüksek hassasiyet sağlar (Ben-Israel, 2020: 73). Bununla birlikte, İsrail siber güvenlik alanında da AI destekli saldırı ve savunma sistemleri geliştirerek bölgesel üstünlüğünü artırmaktadır. Ayrıca, deepfake gibi ileri düzey AI teknolojileri, psikolojik harp ve bilgi savaşları bağlamında kullanılmakta, propaganda ve dezenformasyon faaliyetlerine yeni boyutlar kazandırmaktadır (Vaccari & Chadwick, 2020: 1 - 12). Deepfake, yapay sinir ağları ve makine öğrenimi teknikleri kullanılarak, bir kişinin gerçekçi ama sahte videolarının veya ses kayıtlarının oluşturulması sürecidir. Bu teknoloji sayesinde, kişilerin sözleri veya hareketleri gerçekte yapmadıkları şekillerde görüntülenebilir veya duyulabilir hale gelir. Böylece, kamuoyunun algısını manipüle etmek, güvenilirlik ve doğruluk duygusunu zedelemek mümkün olmaktadır (Chesney & Citron, 2019: 89).

AI destekli müdahalelerin kapsamı, sadece doğrudan çatışma alanları ile sınırlı kalmayıp, algı yönetimi ve küresel standart oluşturma süreçlerine kadar uzanmaktadır. Örneğin, bu teknolojiler aracılığıyla dijital platformlarda yürütülen dezenformasyon kampanyaları, uluslararası hukuk ve normların esnetilmesine veya yeniden tanımlanmasına sebep olmaktadır (Cave & Dignum, 2019: 31). Bu durum, devletler arası ilişkilerde güven bunalımlarını derinleştirmekte ve krizlerin tırmanma riskini artırmaktadır.

Ayrıca, AI destekli müdahalelerde şeffaflık eksikliği önemli bir sorundur. Algoritmaların nasıl çalıştığı, hangi veri kümelerine dayandığı ve kararların nasıl alındığı genellikle gizlidir. Bu durum, hatalı ya da taraflı kararların ortaya çıkmasına ve uluslararası arenada sorumluluk sorununun karmaşıklaşmasına yol açmaktadır (Floridi, 2020: 45).

1.3.2. Yeni Nesil AI Sistemleri ve Sosyal Medya Entegrasyonu

Yeni nesil AI sistemleri, sosyal medya platformlarına entegrasyonlarıyla dijital etkileşim biçimlerinde köklü değişimler yaratmaktadır. Bu teknolojiler, kullanıcıların davranışlarını analiz etmek, içerik üretmek ve hatta kamuoyunu şekillendirmek gibi işlevleri giderek daha etkin ve karmaşık biçimde yerine getirmektedir. Ancak bu gelişmeler, yalnızca teknik bir ilerleme olarak değil; aynı zamanda etik, şeffaflık ve kullanıcıların veri haklarına dair ciddi sorunları da gündeme getirmektedir. Sosyal medya ile AI birleşimi, demokratik süreçler ve bireylerin bilgi üzerindeki kontrolü açısından yeni zorluklar doğurmaktadır.

X platformu, 2022 yılında Elon Musk'ın Twitter'ı satın almasıyla birlikte dijital dünyada yeni bir döneme girmiştir. Elon Musk, burayı sadece bir sosyal medya sitesi olmaktan öte, finansal işlemlerden AI uygulamalarına kadar birçok hizmeti içinde barındıran kapsamlı bir dijital dünya haline getirmeyi amaçlamıştır (Demir, 2023: 112). Bu süreçte geliştirilen Grok adlı AI sistemi, platforma entegre edilerek kullanıcıların paylaşımlarını gerçek zamanlı analiz etmek, politik süreçleri takip etmek ve kişiye özel bilgi akışı sağlamak için tasarlanmıştır (Yılmaz, 2024: 58). Grok, karmaşık soruları cevaplayabilen ve etkin etkileşim sağlama aracı olarak gelişmiş bir dil işleme yeteneğine sahiptir. Özellikle seçim dönemleri kamuoyunun şekillendirilmesinde güçlü bir araç haline gelerek adını duyurmuştur. Ancak, Grok'un karar mekanizmalarının ne kadar şeffaf olduğu ya da yanlış bilgi üretme ihtimali gibi konular, sosyal medya üzerindeki etkilerini tartışmalı kılıyor ve etik, veri hakları gibi önemli soruları gündeme getirmektedir.

Öte yandan, Grok'un son dönemde bazı kullanıcılara yönelik kaba ifadeler ve hatta küfürlü yanıtlar vermesi, bu tür sistemlerde “kendi kendine düşünme” yeteneği iddiasını tartışmaya açmıştır. Burada asıl sorun, AI sistemlerinin karar alma süreçlerinin

şeffaf olmaması ve kullanıcıların bu süreçler hakkında bilgilendirilmemesidir. Grok gibi AI içerikli algoritmaların nasıl eğitildiği, hangi veri setlerine dayandığı ve neden belirli tepkiler verdiği büyük ölçüde gizli tutulmaktadır. Bu durum, kullanıcıların veri haklarını ve ifade özgürlüğünü ihlal edebilirken, aynı zamanda sistemlerin denetlenebilirliğini ve hesap verebilirliğini de sınırlandırmaktadır (Floridi, 2020: 45).

Ayrıca, AI sistemlerinin sosyal medya platformlarına entegrasyonunda ortaya çıkan bu tür sorunlar, mevcut düzenleyici çerçevelerin yetersizliğini göstermektedir. Kullanıcılar, AI kaynaklı sorunlara yönelik şikâyetlerini iletebilecekleri net mekanizmalara sahip değildir. Yine de, bu tür teknolojilerin demokratik süreçler üzerindeki etkisi göz önüne alındığında, uluslararası düzeyde şeffaflık, etik kurallar ve kullanıcı veri haklarını koruyacak kapsamlı düzenlemeler geliştirilmesi acil bir gerekliliktir (Cave & Dignum, 2019: 31).

Bu bağlamda, Grok gibi AI sistemlerinin sosyal medya entegrasyonu, dijital iletişim pratiklerinde köklü dönüşümler yaratırken, beraberinde etik belirsizlikler, şeffaflık eksiklikleri ve kullanıcı veri haklarının ihlali gibi önemli sorunları da gündeme getirmektedir (Cave & Dignum, 2019: 31). Ayrıca, bu teknolojilerin kontrolsüz kullanımı, toplumda bilgi kirliliğini artırarak demokratik süreçlerin sağlığını tehdit edebilir ve sosyal kutuplaşmayı derinleştirebilir (Zuboff, 2019: 215). Demokratik toplumların dijital güvenliğini sağlamak ve teknolojinin sunduğu fırsatları adil biçimde değerlendirmek için, bu yeni nesil teknolojilerin çok boyutlu analizlere tabi tutulması ve disiplinler arası düzenleyici yaklaşımların geliştirilmesi gerekmektedir.

1.4. Büyük Veri, Yapay Zeka ve Algoritmik Yönetişim

Dijitalleşme ve veri üretiminin küresel ölçekte hız kazanması, uluslararası siyasetin işleyişine yapısal boyutta dönüşüm getirmiştir. Artık devletler sadece ekonomi ve askeri kapasiteyle değil; aynı zamanda veri üzerinde kurdukları egemenlikle de sistem içindeki pozisyonlarını güçlendirmektedir. Büyük veri, farklı kaynaklardan elde edilen devasa bilgi haznelerini analiz ederek ulusal güvenlikten dış politikaya kadar geniş bir alanda stratejik tahmin imkânı sunar (Kumar, 2021: 112). Akıllı algoritmalar ise bu verileri işleyip sosyal medya eğilimlerinden diplomatik risk analizlerine kadar kapsamlı öngörüler sağlamakta; doğal dil işleme ve veri madenciliği gibi tekniklerle

diplomatik karar süreçlerini dönüştürmektedir (Kaya, 2023: 112). Bu doğrultuda Doğal dil işleme (Natural Language Processing / NLP / Doğal Dil İşleme), bilgisayarların insan dilini anlama, yorumlama ve üretme yeteneğini kazandığı AI alt alanlarından biridir. Bu teknoloji sayesinde metinler analiz edilebilir, özetlenebilir ya da otomatik olarak çevrilebilir (Britannica, 2025: 12). NLP sistemleri, sözcük türü belirleme, duygu analizi ve isim tanıma gibi görevleri yerine getirerek çok sayıda sektörde kullanılmaktadır (Coursera, 2025: 24). Özellikle müşteri hizmetleri, dijital asistanlar ve sosyal medya analizi gibi alanlarda NLP'nin etkinliği giderek artmaktadır (Techtarget, 2025: 30).

Veri madenciliği ise, büyük veri kümelerinde gizli kalmış desenleri ve ilişkileri keşfetmeyi amaçlayan bir analiz disiplini. Pruengkarn, Wong ve Fung'un (2017) makalesine göre, veri madenciliği teknikleri “öngörücü” ve “tanımlayıcı” yöntemler olarak iki temel kategoriye ayrılmakta, bu teknikler büyük veri ve sağlık bilişiminde yaygın biçimde uygulanmaktadır (Pruengkarn, Wong & Fung, 2017: 32–33). Bu alandaki uygulamalar, veriden anlamlı bilgi çıkarılmasını sağlayarak karar destek sistemlerine katkıda bulunur (Pruengkarn et al, 2017: 35). Makalede yer verilen analiz, son yirmi yılda veri madenciliği uygulamalarının nasıl evrildiğini ve hangi alanlara yayıldığını belirgin bir biçimde ortaya koymaktadır (Pruengkarn et al, 2017: 36).

Bu alanda yer alan fiziki örneklerle bakıldığında ise, Çin'in sosyal kredi sistemi, devlet veri kapasitesinin siyasi kontrol aracına dönüşebileceğinin somut bir göstergesidir. Öte yandan, ABD merkezli teknoloji şirketlerinin küresel altyapı üzerindeki etkileri, veri egemenliği temelli güç projeksiyonunu ortaya koymaktadır (Öztürk, 2022: 87). AI destekli analizler, dış politika ve istihbarat mekanizmalarında karar alma hızını ve doğruluğunu artırırken, aynı zamanda stratejik esneklik ve diplomatik manevra imkânları da yaratmaktadır (Chen, 2020: 89).

Bununla birlikte, bu teknolojilerin sağladığı avantajlar ciddi etik ve güvenlik risklerini de beraberinde getirmektedir. Veri gizliliği ihlalleri, algoritmik önyargılar, siber saldırılar ve dezenformasyon gibi sorunlar, uluslararası sistemde kırılganlık riskini artırmakta, bilgi temelli güç asimetrisi yeni jeopolitik gerginliklere yol açmaktadır (Nguyen, 2022: 77).

SELA'nın “*Yapay Zeka ve Diplomasi: Yıkıcı Teknolojiler Çağında Uluslararası İlişkiler*” (*Artificial Intelligence and Diplomacy: International Relations in the Era of Disruptive Technologies*) adlı çalışması, bu bağlamda “techplomacy” kavramını tanıtarak devlet dışı aktörlerin (örneğin teknoloji şirketleri ve bölgesel örgütler) diplomasi süreçlerinde aktif rol oynadığı çok aktörlü bir yönetim modeline işaret eder (Jarrín, 2024: 18). Ayrıca rapor içerisinde yer alan bir başka çalışma da, AB'nin AI Yasası gibi düzenleyici çabalarının küresel çapta norm oluşturucu etkisine, LAC (Latin America and the Caribbean / Latin Amerika ve Karayipler) Bölgesi'nin dijital iş birliği oluşumlarına ve veri egemenliği ekseninde etik çerçevenin nasıl şekillenebileceğine dair kapsamlı analizler sunmaktadır (Hernández, 2024: 53-58).

Ancak bu yeni arenada veri, salt bir bilgi birimi olmaktan çıkıyor; uluslararası normları belirleyen temel güç unsuru haline gelmektedir. *Büyük Güç Rekabeti Ortasında Akıllı Ortaklıklar* (*Smart Partnerships Amid Great Power Competition*) adlı Atlantic Council raporu, büyük veri ve AI gibi teknolojilerin yükselişinin, yalnızca bilgi akışını değil, dijital egemenliğe dayalı bir güç rekabetini de şekillendirdiğini vurgular. Buna göre, veriye sahip olmanın ötesinde; veriyi işleyebilme, kontrol edebilme ve yönlendirebilme yetenekleri, yeni güç ve etki alanlarının temelini oluşturmaktadır (Burrows & Mueller-Kaler, 2021).

Demokratik süreçler açısından değerlendirildiğinde, algoritmik yönetim tehditlerle doludur. AI destekli sosyal medya kampanyaları, propaganda araçlarına dönüşerek halkın algısını etkileme potansiyeli taşır. Bu durum siyasi meşruiyete ve demokratik temsile yönelik ciddi yapısal müdahalelerdir (Tufekci, 2018: 94). Ayrıca devletler, dijital altyapılar üzerinden yürütülen siber egemenlik politikalarını güvenlik stratejilerine entegre ederken, klasik güvenlik tanımı da yeniden tanımlanmaktadır (Calo, 2015: 405).

Ekonomik bağlamda ise algoritmalar, dijital para sistemleri ve platform ekonomisi aracılığıyla veri merkezli yeni bir dolaşım alanı oluşturmaktadır. Bu durum, devletlerin bilgi akışları üzerinde güç koordine etmesini yeniden düzenlemektedir.

Tüm bu gelişmeler ışığında, veri artık salt bir bilgi kaynağı değil; siyasi, ekonomik ve askeri etkileşimlerin merkezi bir bileşeni hâline gelmiştir. Devletler

arasında veri egemenliği rekabeti başlamış, bilgi toplamanın ötesine geçip bu veriyi işlemek, yönlendirmek ve sınırlandırmak kritik stratejik kapasitelere dönüşmüştür. Özellikle Çin ve ABD arasındaki teknoloji egemenliği rekabetinin diplomasiye yansıyan boyutları, dijital normların ve güvenlik politikalarının yeniden tanımlanmasına neden olmaktadır (Aranibar, 2024: 9–15).

Algoritmik yönetim, uluslararası ilişkilerde yalnızca işlevsel bir araç olmanın ötesinde, aktörlerin güç tanımlarını ve etkileşim biçimlerini yeniden şekillendirmektir. Bu dönüşüm, devletleri daha karmaşık, teknolojik olarak entegre ve kurallar boyutunda yeniden şekillenen diplomasi yaklaşımlarına adapte olmaya yönlendirmektedir. Teknolojik evrim artık diplomasiyi sadece bir araç olarak değil; aynı zamanda uluslararası sistemin temel fonksiyonlarını yeniden tanımlayan bir unsur hâline getirmiştir. *Cambridge Perspectives on Politics*'te vurgulandığı üzere, algoritmik sistemler; yalnızca devletlerin stratejik karar süreçlerine entegre olarak değil, aynı zamanda büyük teknoloji şirketlerinin küresel düzen içinde yeni güç merkezi olarak konumlanmasına da olanak tanır. Bu dinamik, devlet ve özel sektör arasında hem iş birliğini hem de çatışmayı içeren “karşılıklı bağımlılık” modellerini beraberinde getirir (Crawford, 2021: 186). Bu çerçevede, Antalya Diplomacy Forum 2025'te sunulan “technopolar dünya” konsepti, diplomasi alanında bir paradigmatal kaymaya işaret eder. Teknoloji altyapılarına hâkim olan aktörlerin ister devlet, ister şirket uluslararası sistemi şekillendirme gücünün, klasik egemenlik anlayışını dönüştürdüğü belirtilmiştir. Devletler artık yalnızca siyasi ve ekonomik değil, teknolojik ve dijital altyapı kapasitesine bağlı olarak gücün tanımını yapar hâle gelmiştir (Akıllı, 2025: 2).

Bu doğrultuda, teknolojik evrim diplomasiyi salt bir araç olmaktan çıkarmış, uluslararası sistemin işleyiş mekanizmalarını yeniden tanımlayan bir unsur hâline getirmiştir. Devletler, algoritmik araçlarla şekillenen bu yeni diplomatik gerçekliğe uyum sağlamak zorundadır. Diplomasi, “tasarım temelli bir yönetim” alanına dönüşmektedir. Bu, devletleri daha teknolojik olarak entegre, normatif açıdan yeniden yapılandırılan diplomasi stratejilerine adapte olmaya zorlayan dönüşümün temsili bir ifadesidir (Qatrani, 2025: 1)

1.5. Siber Siyaset: Kavramsal Çerçeve ve Tarihsel Süreç

Siber siyaset kavramına net bir perspektif sunabilmek adına öncelikli olarak siber kelimesinin kökenine kısa bir anlam açıklaması gerçekleştirilmesi ilerleyen süreçlerde daha net bir bakış açısı sunacaktır. Siber kavramı teorik çerçevede ilk olarak Norbert Wiener'in 1948 yılında yayımlanan *Cybernetics* (Sibernetik) adlı eserinde ortaya konulan kontrol ve iletişim süreçleri teorisinden türemiştir. Wiener, sibernetiği hem canlı organizmalarda hem de makinelerde bilgi akışı ve geri besleme mekanizmalarının düzenlenmesi olarak tanımlamış, böylece Sibernetik kökenine sahip olan “siber” terimi anlam bütünü olarak bilgisayarlarla ilintili bilgi teknolojileri ve dijital sistemlerin temel felsefi zeminini oluşturmuştur (Wiener, 1948: 15-18).

Siber ve siyaset kavramlarının bir araya gelerek günümüz politikalarında önemli bir yer edinmesi ise dijital teknolojilerin gelişimiyle paralel olarak şekillenmiştir. Bu süreçte devletler, organizasyonlar ve bireyler, hem iç hem de uluslararası ilişkilerde siber hamleleri stratejilerine dâhil ederek politik bir araç olarak kullanmaya başlamıştır. Siber siyasetin evrimine baktığımızda en önemli dönüm noktası internet kullanımının küresel ölçekte yayılmaya başlamasıdır. 1989'da 1989'da Tim Berners Lee tarafından CERN laboratuvarlarında geliştirilen World Wide Web sistemi, internetin küresel ölçekte ticari ve toplumsal hayatta yaygınlaşmasını sağlamış ve bilgi aktarımını kolaylaştırmıştır, dijital bilginin hızla dolaşmasına olanak sağlamış ve uluslararası ilişkilerde yeni fırsatları beraberinde getirmiştir (Berners-Lee, 1999: 103-106).

İnternetin bağımsız dolaşım özgürlüğüne sahip olan yapısı, devletler için yeni tehdit alanlarının ortaya çıkmasına zemin hazırlamıştır. Bilgi'nin bu kadar hızlı yayıldığı bir ortamda, devletlerin dijital diplomaside aktif süreçleri başlamış ve değişen siyasi kültürün ilk izleri ortaya çıkmıştır. Siber alanda verilere ulaşabilme ve bilgi akışının gerçekleşmesi, gizli kalması gereken stratejik hamlelerin küresel ölçekte açığa çıkma riskini doğurmuştur. Bu nedenle devletlerin dijital diplomasi stratejileri geliştirmesine zemin hazırlamış, siber alan odaklı güvenlik politikaları geliştirilmiş ve siber istihbarat faaliyetleri yaygınlaşmıştır. Günümüzde devletlerin siber alandaki stratejik eylemleri, dijital diplomasi ve siber güvenlik politikalarına yön vermiştir. Siber istihbarat faaliyetleri, sadece bilgi toplama amacıyla değil; aynı zamanda kritik altyapılara yönelik saldırılar ve dolayısıyla koruma ve siber saldırılara karşı savunma

mekanizmalarının geliştirilmesi amacıyla öncelikli hale gelmiştir (Karasoy, 2022: 45-47).

Siber siyaset, sosyal ağlar aracılığıyla devletler ve sosyal kurumlar tarafından dijital teknolojilerin kullanımıyla politikalar, stratejiler ve eylemler biçiminde uygulanmaktadır. Özellikle sosyal medya platformları üzerinden yürütülen kampanyalar, anketler ve reklam çalışmaları insan algısını yönlendirme süreçlerinde kritik rol oynamaktadır. Ancak bu siyaset biçiminin negatif yönlü kullanımı da yaygındır.

Bu bağlamda, Joseph Nye'nin yumuşak güç kavramı dijital çağda siber siyasetle birlikte dönüşerek yeni bir anlam bütünlüğü kazanmıştır. Geleneksel anlamda kültürel çekicilik ve diplomasi ile açıklanan yumuşak güç, dijital platformlar aracılığıyla daha hızlı ve geniş kitlelere ulaşabilmektedir (Nye, 2020: 115). Bu platformlar devletlere, rakip algısını yönetme ve kamuoyunu etkileme olanağı sunmuş; dezenformasyon ve dijital propaganda gibi araçlar siyasi gündemleri şekillendirmede etkili olmuştur (Farkas & Schou, 2021: 78). Böylece siber siyaset, sadece teknik ve askeri değil, aynı zamanda ideolojik ve kültürel bir savaş alanı haline gelmektedir.

Siber alanda güvenlik ihtiyacının artması, siber istihbaratın önemini artırmıştır. Siber alanın yaygınlaşması, siber saldırı tehditlerini de beraberinde getirmiştir. Sosyal ağlarda dolaşırken bırakılan kişisel veri izleri siber siyasetin hedefi olmuştur. Hassas verilerin çalınması, fikri mülkiyet hırsızlığı gibi siber saldırılar, doğrudan devlet yönetimini hedef alan siyasi saldırılar olarak ortaya çıkmıştır. Örneğin, 2007 yılında Estonya'da gerçekleştirilen siber saldırılar, ülkenin finans, enerji ve hükümet sistemlerini hedef almış ve devletlerarası dijital çatışmaların ciddiyetini gözler önüne sermiştir (Dilek, Talih & Bensghir, 2023: 334-340). Bu olay, siber saldırıların ulusal güvenlik üzerindeki somut etkilerini ortaya koymuş ve devletlerin siber savunma stratejilerini güçlendirmelerine ilercici bir adım olmuştur.

Bilgisayar ve internet teknolojileri, dünya çapında siber uzay denilen bir global köy yaratmıştır. Ancak bu ortak miras, kötü niyetli kullanımlar nedeniyle yeni suç türlerinin doğmasına yol açmıştır. Siber suçlar, bireylere, kurumlara ve ülkelere yönelik

tehditler oluřturmakta ve devletlerin gvenlik politikalarını yeniden řekillendirmektedir (Verma & Bajaj, 2008: 147).

Siber siyasetle birlikte devletlerin savař biimleri de dnřmřtr. Johnson'a (2019) gre, yeni nesil savařlarda sadece ateřli silahlar deęil; enerji, para, bilgi dezenformasyonu, propaganda ve siber saldırılar da birer savař aracı olarak kullanılmaktadır (Johnson, 2019: 63). Gnmzde devletler, stratejik hamlelerini aktif saha savařları yerine siber alanı hedef alarak yapmaktadır. Bu baęlamda, savař araları yazılım kodları ve dijital algoritmalar iken, hedef dijital ortamda iřlenen verilerdir.

2. YAPAY ZEKANIN EKONOMİK VE POLİTİK BOYUTLARI

Endstri devriminden itibaren teknoloji dnřm, uluslararası sistemde kurum ve kuruluřların siyasi ve iktisadi yapısını derinden etkilemiř, gnmzde ise AI ve akıllı algoritmalar bu dnřmn merkezinde yer almaktadır (Kanat ve Akoęuz, 2024: 61). Bu teknolojiler, sadece ekonomik bymeyi hızlandırmakla kalmayıp, uluslararası iliřkilerde karar alma srelerini, gvenlik stratejilerini ve diplomatik etkileřimleri de kkten deęiřtirmektedir (Moretti, 2023: 78).

AI, devletlerin egemenlik algısını yeniden řekillendirerek, sınır tesi dijital aęlar ve veri paylařımı zerinden kresel iřbirliklerinin dinamiklerini deęiřtirmektedir (Santos, 2022: 45). Geleneksel ulus devlet modelleri, akıllı algoritmalarla desteklenen geliřmiř bilgi akıřları sayesinde daha řeffaf ve karmařık yapılar haline gelirken, bu durum devletlerin dıř politika yaklařımlarını daha hızlı ve esnek biimde gncelleyebilmelerine olanak tanımaktadır (Thompson, 2023: 110). Ancak, veri egemenlięi ve dijital altyapıların kontrol, yeni g mcadelelerinin merkezi konusuna dnřmřtr (Miller, 2024: 29).

Askeri alan ise AI'nın en yoęun etki gsterdięi sahalardan biridir. İnsansız hava araları ve otonom silah sistemleri gibi AI destekli teknolojiler, savař stratejilerinde kkl deęiřikliklere yol amakta, uluslararası gvenlik dengelerini yeniden tanımlamaktadır (Almeida, 2021: 93). Bu durum, uluslararası hukuk ve etik normlar bakımından yeni dzenlemeler yapılmasını gerektirmekte ve devletlerin bu geliřmelere uyum saęlamasını zorunlu kılmaktadır (Lee, 2022: 67). te yandan, siber gvenlik

tehditlerinin artması devletlerin dijital savunma kapasitesini artırmalarını zorunlu kılmıştır (Wang ve Chen, 2023: 114).

Ekonomik açıdan AI, küresel rekabeti ve ticaret politikalarını derinden etkilemekte, veri odaklı karar mekanizmaları sayesinde ülkelerin ekonomik performansını optimize etmektedir (Gupta, 2023: 53). Bununla birlikte, dijital uçurum giderek büyüyerek, gelişmekte olan ülkeler ile gelişmiş ülkeler arasındaki eşitsizliği derinleştirmektedir (Ivanov, 2022: 89). Uluslararası ticaret anlaşmalarında AI ve dijital ekonomi konularının giderek öne çıkması, çok taraflı işbirliği modellerinin evrimine işaret etmektedir (OECD, 2024: 77).

Diplomasi alanında ise AI, dijital diplomasiyle birlikte yeni olanaklar sunmakta, devletlerin dış politika araçlarını çeşitlendirmektedir. Sosyal medya platformları ve AI destekli veri analizleri, kamuoyu yönetimi ve algı şekillendirmede önemli bir role sahiptir (Sullivan, 2023: 58). Bununla birlikte, dezenformasyon ve dijital propaganda faaliyetleri, uluslararası politikada yeni riskler ve çatışma alanları yaratmaktadır (Farkas ve Schou, 2021: 78). Böylece dijital siyaset, yalnızca teknik bir gelişme değil, aynı zamanda yumuşak gücün yeni bir formu olarak da öne çıkmaktadır (Nye, 2020: 115).

Son yıllarda AI teknolojilerinin yaygınlaşması, uluslararası güç tanımlarını ve çok taraflı işbirliği biçimlerini köklü biçimde etkilemektedir. Devletler arasındaki bilgi üstünlüğü, yeni hâkimiyet temelli rekabet alanları oluştururken, uluslararası hukuk ve kurumlar da bu dönüşüme uyum sağlama gerekliliğiyle karşı karşıyadır (Khan, 2024: 35). Bu süreç, uluslararası sistemin teknolojik gelişmeler doğrultusunda evrilmeye devam edeceğini göstermekte, yeni normatif ve politik düzenlemelerin önemini artırmaktadır.

2.1. Yapay Zeka ve Küresel Ekonomi

AI ve akıllı algoritmalar, 21. yüzyıl ekonomisinin yapısal dinamiklerini yeniden şekillendiren temel unsurlar haline gelmiştir. Bu teknolojiler, üretim süreçlerindeki otomatikleştirme etkisinin ötesinde, veri analitiği, karar destek sistemleri ve müşteri davranışları öngörüsü gibi kritik alanlarda sağladığı avantajlarla şirketlerin rekabet stratejilerinde merkezi bir rol üstlenmektedir (Chen ve Zhang, 2023: 112). Büyük veriyle entegrasyon sayesinde AI uygulamaları, çok boyutlu analiz kapasitesi ile ekonomik faaliyetlerin öngörülebilirliğini, hızını ve maliyet etkinliğini artırmakta, mikro düzeyde işletmelerin performansını iyileştirirken makro düzeyde yeni sektörlerin doğuşuna ve dijitalleşen ekonomik yapıya öncülük etmektedir (Tüfenk, 2023: 172).

Bu dönüşümün somut etkileri, Amazon, Alphabet (Google) ve Tesla gibi teknoloji devlerinin büyüme stratejilerinde belirgin biçimde gözlemlenmektedir. Amazon, AI destekli lojistik altyapısı ve müşteri odaklı veri analitiğiyle tedarik zinciri süreçlerini optimize ederek küresel e-ticaret alanında güçlü bir aktör haline gelmiştir (Smith, 2021: 45). Alphabet'in arama motoru algoritmalarından otonom araç ve sağlık teknolojilerine kadar uzanan AI yatırımları, şirketi sadece teknolojik değil, ekonomik güç merkezi konumuna yükseltmiştir (Kumar ve Lee, 2024: 59). Tesla ise otomotiv sektöründe otonom sürüş sistemleri aracılığıyla üretim tekniklerini ve ulaşım ekonomisinin geleceğini yeniden tanımlamaktadır (Johnson & Lee, 2022: 102).

Doğu Asya'da da önemli gelişmeler yaşanmaktadır. Çin merkezli Alibaba ve Tencent, AI finansal hizmetlerden perakende ve sosyal medya platformlarına kadar geniş bir yelpazede kullanarak sadece ulusal ekonomiye değil, küresel ticaret ve yatırım akışlarına da yön vermektedir (Wang, 2020: 67). Bu şirketlerin artan dijital kapasitesi, veri egemenliği ve teknolojik inovasyon alanlarındaki devlet politikalarıyla paralel ilerleyerek Çin'in küresel ekonomideki etkisini güçlendirmektedir (Liu, 2023: 88). Dijitalleşmenin iş yapış biçimlerine etkisi yalnızca finans ve ticaretle sınırlı kalmayıp, uzaktan çalışma ve dijital hizmetlerin yaygınlaşmasını da beraberinde getirmiştir. COVID-19 pandemisi sonrası hızlanan uzaktan çalışma modeli, şirketlerin operasyonel esnekliğini artırmış ve iş gücü piyasasında yeni dinamikler yaratmıştır (Varian, 2022: 39). Eğitim, sağlık, finans ve kamu hizmetleri gibi pek çok sektörde dijitalleşme, verimlilik artışı ve erişilebilirlik sağlamaktadır (Avundukluoğlu, 2020: 794). Ancak bu

değişimler, dijital beceri eksikliği ve eşitsizlik gibi sosyo-ekonomik sorunları da gündeme getirmektedir (Milanovic, 2019, aktaran: Tıǧlı, 2021: 52 - 58). Ayrıca, ekonomik yapının dijitalleşmesi kapsamında dijital para birimleri ve blockchain teknolojisi önemli bir dönüşüm aracı olarak ortaya çıkmaktadır. Dijital para, geleneksel para sistemlerine alternatif olarak internet ortamında güvenli ve hızlı işlemler yapılmasını sağlar. Blockchain ise bu dijital işlemlerin şeffaf, değiştirilemez ve merkeziyetsiz bir şekilde kaydedilmesini sağlayan dağıtık defter teknolojisidir (Nguyen, 2021: 125). Bu teknolojiler, finansal sistemin yapısını değiştirmekle kalmayıp, ekonomik faaliyetlerin dijitalleşmesinde ve veri tabanlı yeni iş modellerinin gelişmesinde kritik rol oynamaktadır.

Bunların yanı sıra, AI ekonomik etkileri sadece büyüme ve verimlilik artışı ile sınırlı kalmamaktadır. Teknolojik dönüşüm, işgücü piyasasında yapısal değişimlere yol açmakta; bazı mesleklerin otomasyonla azalması, ekonomik eşitsizliklerin artması ve istihdam güvencesine ilişkin kaygılar gündeme gelmektedir (Varian, 2022: 37). Bu bağlamda, AI tabanlı ekonomi modelleri sosyal boyutları da içermekte, teknolojik gelişmelerin etik, toplumsal ve siyasal sorumluluklarla paralel ele alınmasını gerektirmektedir (Avundukluoğlu, 2020: 792).

AI ve büyük veri temelli sistemlerin üretim, tüketim ve dağıtım zincirlerinde yol açtığı dönüşümler, işgücü piyasasında yeni eşitsizliklere neden olmakla kalmayıp, sosyal refah, istihdam güvencesi ve gelir adaleti gibi alanlarda da politika ihtiyacını artırmaktadır (Tüfenk, 2023: 174b). Bu kapsamda, dijital uçurumun genişlemesi ve teknolojik erişim farklılıkları, küresel ekonomik rekabetin doğasını değiştirmekte, ülkeler arası dengesizlikleri derinleştirmektedir (Milanovic, 2019: 52).

Dijital dönüşümün ekonomik yapıya etkisi yalnızca özel sektörle sınırlı kalmamakta, kamu politikalarının şekillenmesinde de giderek belirleyici bir rol üstlenmektedir (Varnalı, 2025: 16). Bu süreç, işletmelerin karar alma hızını ve verimliliğini artırırken, makro düzeyde ekonomik yapının yeniden şekillenmesine, yeni sektörlerin doğmasına ve küresel rekabet parametrelerinin değişmesine zemin hazırlamaktadır (Brynjolfsson & McAfee, 2017: 98).

Üretim alanında AI, robotik otomasyon ve akıllı sistemlerle fabrikalarda verimliliği artırırken, lojistik sektöründe ise AI tabanlı optimizasyon algoritmaları tedarik zinciri süreçlerini hızlandırmakta ve maliyetleri düşürmektedir (Tamer & Övgün, 2020: 780). Finans sektöründe ise AI, risk analizi, dolandırıcılık tespiti ve müşteri hizmetleri gibi alanlarda devrim yaratmaktadır (Nguyen, 2021: 121). Ancak bu dönüşümler, işgücü piyasasında bazı mesleklerin AI ve otomasyon nedeniyle ortadan kalkması riskini beraberinde getirmekte, bu durum ekonomik ve sosyal güvenlik politikalarında yeniden düzenlemeleri gerektirmektedir (Arntz, Gregory & Zierahn, 2016: 34).

Öte yandan, teknolojik gelişmelerin yarattığı ekonomik rekabet, özellikle patentler, yatırımlar ve inovasyon kapasitesi bağlamında yeni rekabet yarışlarının yükselişine yol açmaktadır (Varnalı, 2025: 48). Bu durum, sadece uluslararası ticaret dengelerini değil, aynı zamanda teknolojik egemenlik ve veri hâkimiyeti açısından da yeni güç mücadelelerini tetiklemektedir (Allam & Newman, 2018: 20).

Tüm bu süreçler dikkate alındığında, AI ve akıllı algoritmalar üzerine kurulu ekonomik dönüşüm, salt teknolojik bir ilerleme olmanın ötesinde, kapsamlı bir toplumsal yeniden yapılanma ve küresel güç dengelerinin değişimi anlamına gelmektedir. Bu bağlamda, AI ekonomisi, hem üretim ve ticaret hem de sosyal adalet ve etik konularında yeni paradigma arayışlarını da beraberinde getirmektedir (Kaplan, 2020: 105). Böylece AI, hem mikro hem de makro ekonomik düzeylerde stratejik kararların, rekabet dinamiklerinin ve politika yapım süreçlerinin ayrılmaz bir parçası haline gelmiştir.

2.2. Yapay Zeka ve Siyasi Süreçler

AI, günümüz siyasi süreçlerinde giderek daha belirleyici bir unsur haline gelmektedir. AI teknolojileri, seçim kampanyalarından kamuoyu analizlerine, politika tasarımıyla kriz yönetimine kadar geniş bir alanda kullanılmaktadır (Binns, 2020: 134). Özellikle veri odaklı algoritmalar, seçmen davranışlarını analiz ederek siyasi aktörlerin stratejilerini şekillendirmesine olanak tanımaktadır (Tufekci, 2014: 89). Bu durum, siyasetin daha hedefe yönelik ve hızlı tepki verebilir olmasını sağlamakla birlikte, manipülasyon ve dezenformasyon risklerini de artırmaktadır (Woolley & Howard, 2018: 321).

Dijitalleşme ve AI teknolojilerinin yükselişi, geleneksel siyasal iletişim biçimlerini dönüştürmekte, sosyal medya platformları aracılığıyla hızlı bilgi akışını mümkün kılmaktadır (Chadwick, 2017: 56a). Bu ortamda AI destekli botlar ve otomatik hesaplar, siyasi gündemleri şekillendirmede önemli rol oynamaktadır (Ferrara et al., 2016: 22). Ayrıca, AI tabanlı analizler, seçmen eğilimlerini önceden tahmin ederek, kampanya kaynaklarının etkin kullanımını sağlamaktadır (Grimmer & Stewart, 2013: 45).

Ancak bu teknolojik gelişmeler, demokratik süreçler açısından yeni zorlukları da beraberinde getirmektedir. Algoritmik tarafsızlık ve şeffaflık konuları, siyasi süreçlerin güvenilirliğini doğrudan etkilemektedir (Diakopoulos, 2016: 89). Bu nedenle, AI kullanımının etik ve hukuki çerçeveler içinde sınırlandırılması giderek önem kazanmaktadır (Crawford, 2021: 210). 21. yüzyıl, teknolojik gelişmeler ve dijitalleşmenin etkisiyle siyaset alanında köklü dönüşümlerin yaşandığı bir dönem olarak karşımıza çıkmaktadır. AI destekli algoritmalar, sadece siyasi aktörlerin iletişim stratejilerini değiştirmekle kalmayıp aynı zamanda halkın siyasal katılım biçimlerini, kamuoyunu şekillenmesini ve demokratik süreçlerin işleyişini yeniden yapılandırmaktadır (Chadwick, 2017: 45).

Bu dönüşüm süreci, klasik siyasal iletişim anlayışının geride bırakılarak, bireylerin davranış kalıpları ve eğilimleri doğrultusunda şekillenen, veri temelli ve kişiselleştirilmiş dijital stratejilerin ön plana çıkmasıyla tanımlanmaktadır. Dijital medya araçlarının sağladığı hız ve geniş erişim, siyasi söylemlerin daha parçalı,

duygusal ve bireysel düzeyde uyarlanabilir hale gelmesini mümkün kılmıştır (Mouffe, 2013: 102).

AI siyasi süreçlerdeki etkisi, özellikle kamuoyunun manipülasyonu ve seçmen davranışlarının önceden tahmin edilip yönlendirilmesinde başat rol oynamıştır. Siyasi aktörler, büyük veri ve AI teknolojileri aracılığıyla bireylerin dijital davranışlarını izleyerek, psikografik özelliklere dayalı kişiselleştirilmiş içerikler sunmakta ve böylece seçmen tercihlerini etkileyebilmektedir (Howard & Kollanyi, 2016: 78). Bu yeni iletişim ve etkileşim biçimi, siyasetin sadece açık ve şeffaf bilgi alışverişiyle sınırlı kalmayıp, aynı zamanda algoritmik müdahalelerle şekillenen çok katmanlı bir yapıya dönüşmesine yol açmıştır (Tüfekci, 2015: 64).

Siyasi süreçlerde AI yükselişi, demokratik sistemlerin işleyişinde hem fırsatlar hem de riskler barındırmaktadır. Bir yandan vatandaşların siyasi bilgiye erişimi artmakta ve katılım kanalları çeşitlenmektedir, öte yandan bilgi manipülasyonu, dezenformasyon ve ayrışma gibi sorunlar derinleşmektedir. Dijital ortamda siyasi aktörlerin ve hatta dış güçlerin, AI destekli araçlarla kamuoyunu yönlendirme çabaları, demokratik meşruiyet ve kamusal alanın işleyişini tehdit edebilir (Benkler, Faris & Roberts, 2018: 220).

Bu çerçevede, siyasi süreçlerin dijital teknolojilerle geçirdiği dönüşüm, yalnızca yönetim biçimlerinde değil, siyasetin temel işleyiş mantığında ve doğasında da köklü bir değişimi beraberinde getirmektedir. Siyasal iletişim, artık yalnızca rasyonel düzlemde tartışma ve bilgi aktarımına dayanan bir alan olmaktan çıkarak; duygu temelli yönlendirmelerin, algı yönetiminin ve dijital yönlendirme mekanizmalarının etkin rol oynadığı çok katmanlı bir etkileşim alanına dönüşmüştür. Sosyal medya platformları gibi alanlarda etkin olan AI algoritmaları, siyasi aktörlerin kamuoyuyla etkileşim biçimlerini yeniden tanımlamaktadır. Bu yeni ortamda, siyasi güç dinamikleri sadece seçmen kitlesinin büyüklüğüne değil, aynı zamanda bireylerin dijital izlerine ve bu verilere dayalı analizlerin etkinliğine de bağlı hale gelmiştir (Castells, 2010: 134).

Bu bağlamda, AI siyasi süreçler üzerindeki etkisi, siyasetin araçsal yapısını derinden dönüştürürken demokratik süreçlerin şeffaflığı ve katılımcılığı açısından yeni sorular ve zorluklar ortaya çıkarmaktadır. Bu dönüşümü anlamak ve günümüz

siyasetine dair kapsamlı bir kavrayış geliřtirmek için, AI teknolojilerinin sosyal ve etik boyutlarıyla birlikte ele alınması gerekmektedir (Müller, 2020: 47).

2.3. Devletlerin Yapay Zeka Stratejileri ve Politik Karar Alma Süreçlerine Etkisi

Devletler, AI teknolojilerinin stratejik önemini kavrayarak bu alanda kapsamlı politikalar geliřtirmektedir (Nye, 2021: 112). AI, bilgi toplama, analiz ve simülasyon yetenekleriyle karar alma süreçlerinde devletlere hızlı ve etkin çözümler sunmakta; özellikle savunma, dış politika ve kamu yönetimi gibi kritik alanlarda devletlerin esnekliğini ve rekabet gücünü artırmaktadır (Turek, 2022: 67; Kania, 2019: 33).

Ancak devletlerin AI stratejileri, yalnızca teknolojik gelişmeleri takip etmekle kalmayıp etik, yasal ve güvenlik boyutlarını da kapsamaktadır (Horowitz, 2018: 155). Uluslararası arenada AI kaynaklı stratejik rekabet, özellikle ABD, Çin ve AB arasında belirginleşmekte; AI, devletlerin güç perspektifinde yeni bir temel olarak önem kazanmaktadır (Fisher, 2020: 76; Allison, 2020: 24).

AI destekli analizler, politik risklerin öngörülmesi ve kriz yönetiminde kritik roller üstlenmektedir (Lempert, 2019: 198). Veri temelli yaklaşımlar, kamu politikalarının daha bilimsel temellere dayanmasını sağlayarak devletlerin kaynak dağılımını optimize etmelerine yardımcı olmaktadır (Margetts & Dorobantu, 2019: 89). Son yıllarda hızla gelişen AI teknolojileri ve bunların dijital araçlarla entegrasyonu, politik süreçlerde dinamik ve köklü dönüşümlere yol açmıştır. Bu süreç, sadece siyasi aktörlerin iletişim stratejilerini değil, halkın siyasal katılım biçimlerini, kamuoyunun oluşumunu ve demokratik süreçlerin işleyişini de yeniden yapılandırmaktadır (Chadwick, 2017: 45).

AI'nın sunduğu büyük veri işleme kapasitesi, karar vericilere karmaşık bilgileri hızlı ve etkili analiz etme imkânı sağlamaktadır (Russell & Norvig, 2016: 329). Bu yetenek, ulusal güvenlikten ekonomik kalkınmaya, kamu yönetiminden sağlığa kadar birçok alanda devletlerin stratejik karar alma süreçlerinde AI kullanımını yaygınlaştırmıştır (Zeng, Lu & Huang, 2020: 112).

Dijital medya araçlarının sağladığı hız ve geniş erişim, siyasi söylemlerin bireyselleşerek parçalı ve duygusal boyutlar kazanmasını mümkün kılmıştır (Mouffe,

2013: 89). Böylece, klasik siyasal iletişim anlayışının ötesinde, AI'nın algoritmik müdahalelerle çok katmanlı bir etkileşim ağı kurması sağlanmaktadır (Tüfekci, 2015: 120a).

AI'nın siyasi süreçlerdeki etkisi, sadece iletişim stratejileriyle sınırlı kalmayıp kamuoyunun manipülasyonu ve seçmen davranışlarının yönlendirilmesinde de kritik rol oynamaktadır. Siyasi aktörler, AI sayesinde bireylerin dijital davranışlarını analiz ederek psikografik özelliklere dayalı kişiselleştirilmiş içerikler sunmakta ve seçmen tercihlerine doğrudan müdahale edebilmektedir (Howard & Kollanyi, 2016: 77). Cambridge Analytica skandalı, 87 milyon Facebook kullanıcısının verilerinin izinsiz kullanımı yoluyla mikro hedefleme tekniklerinin seçmen manipülasyonunda nasıl kullanıldığını göstermektedir (Isaak & Hanna, 2018: 54; Cadwalladr & Graham-Harrison, 2018: 66).

Devletlerin AI kullanımı sadece seçimlerle sınırlı kalmayıp, kamu politikalarının bilimsel temellere dayandırılması ve karar alma süreçlerinde şeffaflığın artırılması açısından da fırsatlar sunmaktadır. Ancak algoritmik karar mekanizmalarının opaklığı ve önyargılarla beslenme ihtimali, etik ve hesap verebilirlik sorunlarını da gündeme getirmektedir (O'Neil, 2016: 89; Eubanks, 2018: 103). Savunma teknolojilerinde AI kullanımı, özellikle otonom silah sistemleri bağlamında yeni etik ve hukuki tartışmalara yol açmaktadır (Schneider & Lucas, 2020: 47). Türkiye gibi gelişmekte olan ülkeler ise AI teknolojilerini ulusal kalkınma planlarına entegre ederek rekabet güçlerini artırmayı hedeflemekte; ancak altyapı ve insan kaynağı eksiklikleri yatırımların etkinliğini sınırlamaktadır (Öztemel, 2021: 90 - 111).

Bu bağlamda, devletlerin AI alanında strateji geliştirme süreci, teknolojik entegrasyonun ötesinde siyasal katılım, ekonomik yönetim ve kamuoyunun şekillenmesini de yeniden tanımlamaktadır. Bu çok katmanlı dönüşümün sağlıklı yönetilebilmesi için etik ilkelere dayalı düzenlemelerin ve demokratik değerleri koruyacak şeffaf yapısal mekanizmaların geliştirilmesi önem arz etmektedir. Böylece toplumun siyasal işleyişi, yönetim biçimleri, kamusal katılım ve demokratik temsil gibi unsurlar üzerinden şekillenmektedir (Margetts & Dorobantu, 2019: 89). Londra Çalışan Sendikaları Kongresi (TUC) tarafından yapılan ve 2.600 çalışanın katıldığı ankette, katılımcıların %51'i AI'nın işlerini kaybetmelerine veya çalışma koşullarının

değişmesine yol açacağına dair endişe taşımaktadır. Bu endişeler, özellikle genç yaş gruplarında (%62) daha yoğun olarak görülmektedir. Ayrıca, katılımcıların büyük çoğunluğu (%83) AI uygulamalarının geliştirilme ve uygulanma süreçlerinde çalışanların daha fazla söz hakkı olmasını talep etmektedir (Trades Union Congress, 2025).

Bu veriler, AI'ın yalnızca teknolojik bir gelişme olmanın ötesinde, iş gücü ve demokratik katılım açısından politik karar alma süreçlerinde önemli etkileri olduğunu göstermektedir. Devletlerin AI stratejilerini geliştirirken, bu tür toplumsal kaygıları dikkate alması gerekliliği ortaya çıkmaktadır (Margetts & Dorobantu, 2019: 89). Çünkü AI'ın karar alma mekanizmalarındaki artan rolü, kamu politikalarının şekillenmesinde işçilerin ve vatandaşların sesinin duyulmasını zorunlu kılmaktadır (Horowitz, 2018: 155). Öte yandan, geleneksel eylem biçimlerinden farklı olarak, sendikalar bu tür veri temelli anketlerle politika yapıcıların dikkatini çekmeyi ve AI ile dijital dönüşümün iş gücü üzerindeki etkilerini daha görünür kılmayı hedeflemektedir (Chadwick, 2017: 45). Bu da politik süreçlerde dijital stratejilerin ve veri analizlerinin önem kazandığını, sistem içindeki aktörlerin AI çağının gereklerine uygun hareket ettiğini göstermektedir (Russell & Norvig, 2016: 329; Tüfekci, 2015: 120).

AI teknolojileri, karar alma süreçleri ve kamu politikalarının oluşturulmasında veri analizi ve algoritmalar yoluyla siyasal işleyişi dönüştürmektedir. Örneğin, elektronik seçim uygulamaları seçmenlerin oy verme süreçlerine erişimini artırsa da beraberinde şeffaflık, güvenlik ve denetlenebilirlik gibi yeni zorlukları ortaya çıkarmaktadır (Telciler, 2007: 237). 2000 ABD başkanlık seçimlerinde yaşanan teknik aksaklıklar, seçim sistemlerinin sadece teknik değil, demokratik meşruiyet açısından da güvenilir olması gerektiğini göstermiştir (Schneier, 2004: 112).

Günümüzde AI destekli siber saldırılar, algoritmik dezenformasyon kampanyaları ve sosyal medya manipülasyonları, seçim güvenliğini tehdit eden başlıca unsurlar haline gelmiştir (Ferrara et al., 2017: 45). Bu durum, demokratik sistemlerin şeffaflık ve hesap verebilirlik ilkelerini zayıflatmakta ve siyasal karar alma süreçlerinde algoritmaların rolünü daha merkezi bir konuma taşımaktadır.

AI etkisi yalnızca siyasi sistemlerle sınırlı kalmayıp, ekonomik ve kültürel yapıların yeniden şekillenmesinde de belirgin şekilde hissedilmektedir. Otomasyon ve veri odaklı üretim süreçleri emeğin niteliğini değiştirerek gelir eşitsizliklerini artırmakta, bu da ekonomik temelli siyasi kararların yeniden kurgulanmasına neden olmaktadır (Brynjolfsson & McAfee, 2014: 56; Acemoglu & Restrepo, 2018: 112). Böylece teknokratik bilgiye dayalı karar mekanizmaları güçlenmekte ve devletlerin ekonomik yönetim anlayışını etkilemektedir (Danaher, 2016: 71).

Ayrıca, AI tabanlı medya algoritmaları bilgi akışını yönlendirme kapasitesi sayesinde kamuoyunun şekillenmesini etkileyerek siyasal iletişimin sınırlarını genişletmektedir. Algoritmaların yarattığı yankı odaları demokratik tartışma ortamını daraltmakta ve kutuplaşmayı derinleştirmektedir (Pariser, 2011: 39; Couldry & Mejias, 2019: 98). Araştırmalar, bu durumun kültürel çoğulculuk ve siyasal karar alma süreçlerinin temsil niteliği üzerinde etkileri olduğunu göstermektedir (Mejias, 2019: 102).

İKİNCİ BÖLÜM

ULUSLARARASI İLİŞKİLER VE YAPAY ZEKA

1. ULUSLARARASI İLİŞKİLER VE YAPAY ZEKA

Sanayi Devrimi'yle başlayan teknolojik evrim, dijital çağda AI ve algoritmik sistemlerle yeni bir boyut kazanmış; bu durum uluslararası yapının yeniden şekillenmesine neden olmuştur (Meleouni & Efthymiou, 2023: 5-13). Bu değişim, uluslararası aktörlerin stratejik davranışlarını ve diplomatik etkileşimlerini yeniden tanımlamakta; AI destekli sistemler, karar alma süreçlerinde giderek merkezi bir rol oynamaktadır (Herrera, 2024: 44-50).

Büyük güçler, özellikle ABD, Çin ve Rusya, küresel AI yarışında öncü konumda olup, AI'nın ulusal prestij ve güç elde etmedeki stratejik önemini ortaya koymaktadır. Akademisyenler ve politika yapıcılar, AI'nın uluslararası politikadaki eğilimleri hızlandırma ve derinleştirme potansiyeline dikkat çekmektedir. Teknoloji, askeri, ticaret ve diplomasi alanlarında etkili bir güç unsuru olarak küresel dengeleri ve savaş biçimlerini şekillendirirken, uluslararası kuruluşlar da AI'nın hızlı gelişimine uyum sağlayarak normları ve yönetim mekanizmalarını güncellemektedir (Özdemir & Yanık Aslan, 2024: 1-8).

AI'nın uluslararası ilişkilerdeki etkisi yalnızca güç dengeleriyle sınırlı kalmayıp, aynı zamanda küresel yönetim, güvenlik ve etik normların yeniden değerlendirilmesini de zorunlu kılmaktadır. Özellikle siber güvenlik, veri egemenliği ve AI etiği alanlarında devletler arasında yeni rekabet ve iş birliği biçimleri ortaya çıkmaktadır (Crootoof, 2022: 112-118).

AI ve algoritmik sistemlerin yükselişi, verinin ulusal sınırlar ötesinde dolaşımının önünü açmıştır. Her geçen gün gelişen AI teknolojileri, gözetim kapitalizmi aracılığıyla devletler ve özel aktörler tarafından toplumsal kontrol ve bilgi yönetimi için kullanımı artarak devam etmektedir (Zuboff, 2019: 78-85). Bu durum, uluslararası normların ve hukuki çerçevenin yeniden tartışılmasını gündeme getirmiştir. Uluslararası kuruluşlar, AI etiği, veri koruma ve dijital haklar gibi alanlarda standartlar oluşturmaya çalışsa da, büyük güçler arasındaki rekabet ve farklı normatif yaklaşımlar,

küresel yönetişimde bir uyumsuzluk yaratmaktadır. Bu bağlamda, AI uluslararası ilişkilerde yalnızca bir teknoloji aracı değil, aynı zamanda küresel normlar, etik ve güç dengelerini yeniden şekillendiren kritik bir unsur olarak öne çıkmaktadır.

1.1. Dezenformasyon ve Manipülasyon

Tarihsel olarak propaganda, sansür ve devlet kontrollü dezenformasyon gibi yöntemler, siyasal manipülasyonun temel araçları olmuştur (Lasswell, 1927: 34; Jowett & O'Donnell, 2018: 102). Soğuk Savaş döneminde medya organlarının ideolojik aygıtlar olarak kullanılması, bilgi savaşlarının uluslararası güç dengelerine etkisini açıkça ortaya koymuştur (Ellul, 1965: 78). Ancak dijitalleşmeyle birlikte, bilgi üretimi ve dolaşımı merkezi yapılarla sınırlı kalmaktan çıkmış; AI destekli algoritmalar aracılığıyla manipülasyon daha yaygın, görünmez ve etkili hale gelmiştir (Benkler, Faris & Roberts, 2018: 92).

Günümüzde sosyal medya platformları, kullanıcıların dijital izlerini analiz ederek kişiselleştirilmiş içerik akışları oluşturmakta; bu durum, bilgiye erişimi demokratikleştirmekten ziyade, bireyleri belirli görüş gruplarına hapsederek yankı odalarını (echo chambers) ve filtre balonlarını (filter bubbles) güçlendirmektedir (Sunstein, 2001: 68). Algoritmalar, kullanıcıların mevcut kanaatlerini pekiştirirken, farklı bakış açılarına erişimi sınırlamakta ve toplumsal kutuplaşmayı derinleştirmektedir (Günar, 2023: 54). Bu süreçte AI, yalnızca bilgi sunan bir araç değil, aynı zamanda görüş yönlendiren bir aktöre dönüşmektedir.

Bilginin araçsallaştırılması, algoritmik yönlendirme teknikleri ve dijital sosyal mühendislik yöntemleri, manipülasyonun siyasal etkisini daha da artırmıştır. Sahte haber üretimi, derin sahte (deepfake) içerikler ve bot hesaplar üzerinden yürütülen dezenformasyon kampanyaları, kamuoyunu sistematik olarak yanıltmakta ve demokratik işleyişin şeffaflığını zedelemektedir. Bu gelişmeler, modern savaşın yalnızca fiziki değil, aynı zamanda bilgi temelli ve algı merkezli bir boyut kazandığını göstermektedir (Talishinsky, 2025: 834; Balel, 2024: 58).

Memetik savaşlar (mimetic warfare), özellikle çevrimiçi mecralarda kısa, çarpıcı ve duygusal içeriklerle kamuoyunu yönlendirme pratiği olarak yükselişe geçmiştir. Bu tür stratejiler, klasik propaganda yöntemlerinden farklı olarak, hedef

kitlenin bilinçaltına hitap ederek etki yaratmayı amaçlamaktadır. 2003 Irak Savaşı sırasında savaş haberlerinin bir propaganda aracı olarak kullanımı, bu eğilimin erken örneklerinden biri olarak değerlendirilmiştir (Yoldaş, 2024: 62). Günümüzde ise bu pratik, AI destekli görsel üretim araçları ve viral içerik algoritmaları ile çok daha sofistike bir biçim kazanmıştır.

Brexit süreci ve Cambridge Analytica skandalı, büyük veri ve algoritmaların politik davranışı yönlendirmek amacıyla nasıl araçsallaştırıldığını gösteren çarpıcı örneklerdir (Cadwalladr & Graham-Harrison, 2018: 12). Seçmenlerin dijital ayak izleri kullanılarak geliştirilen psikografik mikro-hedefleme teknikleri, seçim güvenliği ve demokratik meşruiyet açısından ciddi tartışmalara yol açmıştır (Ferrara et al. 2017: 45). Bu müdahaleler yalnızca bireylerin karar alma süreçlerine değil, kolektif iradenin şekillenmesine de doğrudan etki etmektedir.

Modern dijital manipülasyon stratejileri, klasik güç kuramlarını yeniden yorumlamayı zorunlu kılmaktadır. Bu bağlamda, Joseph Nye'nin yumuşak ve akıllı güç kavramları hâlâ geçerliliğini korusa da, yeni dijital bağlamda bunları daha geniş bir “bilgi temelli güç” (information-based power) anlayışıyla birlikte ele almak daha anlamlı hale gelmiştir (Klein, 2023: 109). AI destekli propaganda sistemleri, bu yeni güç biçiminde stratejik bir rol üstlenerek devletler arası etkileşimde görünmeyen ancak etkili bir araç haline gelmiştir.

Bütün bu gelişmeler, uluslararası sistemde bilgi'nin sadece bir iletişim aracı değil, aynı zamanda bir çatışma nesnesi olarak da önem kazandığını ortaya koymaktadır. Devletlerin AI destekli dezenformasyon kampanyaları yürütmeleri, medya araçlarını küresel ölçekte stratejik bir silah gibi kullanmaları, yeni nesil hibrit savaşların tanımlayıcı unsurlarından biri haline gelmiştir (Balel, 2024: 60; Talishinsky, 2025: 836).

Tüm bu faktörler, günümüzde demokratik değerlerin korunmasını daha karmaşık hale getirmekte; bilgi güvenliği, seçim şeffaflığı ve medya okuryazarlığı gibi alanlarda çok düzeyli ve sistematik politikalar gerektirmektedir. Rekabetin yoğun olduğu küresel bir ortamda tamamen çıkar çatışmalarından arındırılmış bir iş birliği modeli oluşturmak kolay olmasa da; teknoloji şirketleri, sivil toplum kuruluşları, akademik çevreler ve

uluslararası aktörlerin ortak sorumluluk bilinciyle hareket etmesi, demokratik işleyişin sürdürülebilirliği açısından elzemdir (Romanishyn, Malytska & Goncharuk, 2025).

1.2. Yapay Zeka Teknolojileri ve Uluslararası İlişkiler

AI teknolojileri, günümüzde yalnızca teknolojik bir yenilik olmanın ötesinde, uluslararası ilişkiler alanında da önemli bir dönüşüm aracı haline gelmiştir. Devletler ve uluslararası aktörler, AI'ın sunduğu yenilikçi imkânlarla diplomasi, güvenlik ve iş birliği süreçlerini yeniden şekillendirerek, küresel düzeyde daha etkin ve hızlı karar alma mekanizmaları geliştirmektedir (Schwartz, 2020: 12). Özellikle çok dilli çeviri sistemleri ve veri analiz araçları, diplomatik iletişimdeki engelleri aşarak farklı kültürler ve diller arasında anlayışı artırmaktadır. Bu sayede devletler, büyük veri analizleriyle dış politika kararlarını daha sağlam temellere dayandırmakta ve diplomasi süreçlerinde hem hız hem de etkinlik kazanmaktadır (Brown & Smith, 2019: 48; Lee, 2021: 93).

Güvenlik alanında AI'ın katkıları giderek artmaktadır. Otonom sistemler ve AI destekli tehdit tespiti, çatışmaların önlenmesi ve kriz yönetiminde kritik bir rol oynamaktadır. Bu teknolojiler, potansiyel tehlikelerin erken fark edilmesini sağlayarak uluslararası barışın korunmasına destek vermektedir (Miller, 2022: 75). Ayrıca siber güvenlikte AI'ın kullanılması, ülkeler arasındaki siber tehditlere karşı savunma kapasitesini artırmakta ve böylece uluslararası güvenlik ortamını güçlendirmektedir (Garcia, 2020: 124).

AI, uluslararası iş birliği alanında da yeni fırsatlar yaratmaktadır. İklim değişikliği, salgın hastalıklar ve enerji krizleri gibi küresel sorunların yönetiminde AI destekli büyük veri analizleri, devletlerin ortak çözümler üretmesini kolaylaştırmakta ve uluslararası koordinasyonu güçlendirmektedir (Nguyen & Patel, 2021: 107). Bu durum, uluslararası iş birliğinin etkinliğini artırmakla kalmayıp, aynı zamanda küresel barış ve refahın gelişimine de önemli katkılar sağlamaktadır.

Kalkınmakta olan ülkeler açısından ise AI, eğitim, sağlık ve ekonomik kalkınma alanlarında büyük potansiyel taşımaktadır. AI tabanlı uygulamalar, sınırlı kaynakların daha verimli kullanılmasını sağlarken, uluslararası toplumun sürdürülebilir kalkınma hedeflerine ulaşmasına destek olmaktadır (Kumar, 2020: 33). Ayrıca insan hakları

ihlallerinin tespitinde AI teknolojilerinin kullanılması, uluslararası müdahalelerin daha hızlı ve etkin gerçekleşmesini mümkün kılmaktadır (Zhang, 2019: 62).

Bu teknolojilerin uluslararası ilişkilerde sunduğu fırsatlar giderek artarken, AI'ın petrol ve doğalgaz gibi geleneksel kaynakların önemini geride bırakabilecek bir güç olarak uluslararası rekabetin boyutlarını değiştirmesi de tartışma konusu olmaktadır. Ulus devletler, bilgi teknolojilerini geliştirmek ve etkin şekilde kullanmak üzere yeni bir rekabet alanı yaratmışlardır ve bu alandaki gelişmelerin geleceğin küresel liderliği üzerinde belirleyici etkileri olacağı öngörülmektedir (Tugay & Tugay, 2019: 22).

Günümüzde iletişim alanında da AI önemli yeniliklere kapı aralamaktadır. Google DeepMind ve Oxford Üniversitesi iş birliğiyle geliştirilen AI tabanlı dudak okuma sistemleri, özellikle sessiz veya gürültülü ortamlarda sözlü iletişimin mümkün olmadığı durumlarda kullanılmaktadır. Bu sistemler, video görüntülerinden dudak hareketlerini analiz ederek konuşulan cümleleri anlamlandırmayı hedeflemekte; işitme engelli bireylerin iletişim becerilerini artırmak, gürültülü ortamlarda iletişim engellerini azaltmak ve güvenlik ile istihbarat alanlarında stratejik bilgi elde etmek için kullanılmaktadır (Chung, Zisserman, Senior & Vinyals, 2017).

Teknik olarak, bu teknoloji derin öğrenme ve görüntü işleme yöntemleriyle dudak hareketlerinin yüksek doğrulukla tanınmasına dayanır. Özellikle ‘‘LipNet’’ gibi modeller, cümle düzeyinde dudak okuma performansı ile profesyonel dudak okuma uzmanlarına yakın sonuçlar elde etmektedir (Assael et al., 2016:4). Ayrıca, geliştirilen modeller gerçek dünya koşullarına uyum sağlayarak farklı ortam ve koşullarda performansını artırmaktadır (Chung et al., 2016: 9).

Ancak bu gelişmeler etik ve gizlilik kaygılarını da beraberinde getirmektedir. Liderlerin veya bireylerin kapalı alanlardaki konuşmalarının AI tarafından analiz edilmesi mahremiyet ihlali ve gözetim risklerini gündeme getirmektedir. Bu nedenle, AI tabanlı dudak okuma teknolojilerinin geliştirilmesi ve uygulanması sürecinde etik standartlar ve yasal düzenlemelerin dikkate alınması gerekmektedir. Google DeepMind ve Oxford Üniversitesi tarafından geliştirilen bu sistemler, hem sosyal erişilebilirlik hem de stratejik iletişim alanlarında önemli fırsatlar sunmakla birlikte, teknolojinin etik

sınırları üzerinde titizlikle durulması gereken bir alan olarak öne çıkmaktadır (Chung, Zisserman, Senior & Vinyals, 2017).

1.3. Yapay Zeka ve Uluslararası Çatışmalar Üzerindeki Etkisi

AI teknolojileri, uluslararası çatışmaların dinamiklerini kökten değiştirmekte ve savaş yöntemleri ile güvenlik stratejilerinde yeni paradigmlar yaratmaktadır. Devletlerin savunma sistemlerine entegre edilen AI tabanlı teknolojiler, çatışmaların boyutunu, hızını ve doğasını yeniden tanımlamakta; hem savunma hem de saldırı alanlarında önemli roller üstlenmektedir. Bu gelişmeler, uluslararası güvenlik ortamını daha karmaşık ve öngörülemez hale getirmektedir (Altman, 2019: 15).

AI destekli otonom silah sistemleri, devletler arasında yeni bir silahlanma yarışını tetiklerken, karar alma süreçlerinde insan faktörünü azaltmakta ve savaş planlamasını hızlandırmaktadır. Ancak bu durum, sorumluluk zincirinin karmaşıklaşması nedeniyle uluslararası hukukun sınırlarını zorlamaktadır. Özellikle İsrail'in 2023 yılında Gazze'de kullandığı Lavender adlı AI destekli hedefleme sistemi, insan gözetimi olmadan ölümcül sonuçlar doğurabileceğinin çarpıcı bir örneğini teşkil etmektedir. Lavender, saniyeler içinde binlerce hedef belirleyip İHA'lar aracılığıyla saldırılar düzenleyerek çok sayıda sivilin hayatını kaybetmesine neden olmuştur (Human Rights Watch, 2024: 3). Bu olay, AI'nın çatışma ortamında insan haklarını tehdit eden bir araca dönüşebileceğini göstermektedir.

Benzer biçimde, ABD'nin Project Maven projesi kapsamında AI, İHA'lardan elde edilen büyük görsel veri setlerini analiz ederek hedef tespiti yapmada kullanılmaktadır (Department of Defense, 2019: 8). Ancak insan müdahalesinin azaltılması, otomatik öldürme kararlarının etik ve hukuki meşruiyetini sorgulatmaktadır (Crotoft, 2015: 70). Google'ın projeye desteği, şirket içi etik tartışmalara yol açmış ve nihayetinde askeri AI projelerinden çekilmesine neden olmuştur (Wakabayashi & Shane, 2018: 6).

AI savaş teknolojilerine entegrasyonu sadece gelişmiş ülkelerle sınırlı kalmamaktadır. Ukrayna-Rusya savaşında, her iki taraf da AI destekli görüntü tanıma ve İHA entegrasyonunu aktif olarak kullanmaktadır. Ukrayna, Batı menşeli AI sistemleriyle Rus birliklerini yüksek isabet oranıyla hedef alırken, Rusya da kendi

geliştirdiği teknolojilerle karşı koymaya çalışmaktadır (Kallenborn, 2023: 2). Bu durum, gelecekte savaşların insan gücünden çok algoritmalar üzerinden yürütüleceği hibrit savaş senaryolarını güçlendirmektedir (Roff, 2020: 212).

Bununla birlikte, AI sadece çatışma anında değil, çatışmaları öngörme ve toplumsal hareketleri izleme süreçlerinde de önemli rol oynamaktadır. ABD istihbarat kurumlarının PRISM ve XKeyscore gibi dijital gözetim programlarıyla büyük veri analizleri yaparak toplumsal hareketleri izlediği ve kamuoyu eğilimlerini tespit ettiği bilinmektedir (Greenwald, 2014: 95). Bu sistemler, sosyal medya üzerinden potansiyel protesto bölgelerini belirleyebilmekte (Morozov, 2011: 243), dolayısıyla Arap Baharı gibi toplumsal ayaklanmalarda da AI destekli analiz araçlarının dolaylı etkileri olmuştur. ABD'nin sosyal medya verilerini analiz ederek bölgedeki rejimlerin dayanıklılık ve muhalif yapıların hareket kabiliyetini incelediği belirtilmektedir (Shirky, 2011: 33; Howard & Hussain, 2013: 104). Her ne kadar doğrudan AI müdahaleleri belgelenmemiş olsa da, bu veri işleme kapasiteleri dış politika kararlarını etkilemiş olabilir.

Güncel çatışmalarda AI'nın İHA'larla entegre kullanımı, savaşların hibrit ve algoritmik bir nitelik kazanmasına neden olmaktadır. Her iki taraf, düşman birliklerinin konumunu belirlemek için AI algoritmalarını aktif şekilde kullanmakta; bu durum savaşın geleneksel boyutlarının ötesine geçmektedir (Kallenborn, 2023: 2; Roff, 2020: 210). Tüm bu gelişmeler ışığında, AI'nın uluslararası çatışmalardaki rolü sadece otomasyonla sınırlı kalmayıp; veri temelli dış politika yürütme, halk hareketlerini izleme ve bilgi manipülasyonu gibi alanları da kapsamaktadır. Bu durum, uluslararası hukuk açısından yeni düzenlemeler ve etik sınırların netleştirilmesini öncelikli bir hale getirmektedir (Crootoof, 2015: 70).

1.3.1. Yapay Zeka Güvenlik Teknolojileri

Günümüz dünyasında AI teknolojileri, devletlerin güvenlik stratejilerinde giderek daha önemli bir yer tutmaktadır. Bu teknolojiler, hem dijital hem de fiziksel güvenlik tehditlerine karşı etkin çözümler sunmakta, sınır güvenliği, siber savunma ve kamu düzeninin sağlanmasında temel araçlar haline gelmektedir. AI, büyük veri analizi ve makine öğrenimi teknikleri ile siber saldırılara karşı proaktif bir savunma sağlamakta, aynı zamanda fiziksel sınırların korunmasında da etkin rol oynamaktadır (Şahiner, Ayhan & Önder, 2021: 85).

Sahte haberlerin yayılması ve dezenformasyon, özellikle sosyal medya platformlarında hızla yayılan bir güvenlik tehdididir. AI, otomatik içerik tarama ve doğruluk analizleri yaparak bu tür dezenformasyonun yayılmasını engellemeye çalışır. Örneğin, ABD’de sosyal medya ve haber platformları AI destekli sistemlerle sahte içerikleri tespit etmeye yönelik projeler yürütmektedir. Ayrıca, AB’nin Dijital Hizmetler Yasası (Digital Services Act / DSA / Dijital Hizmetler Yasası) kapsamında dezenformasyonla mücadelede AI araçları entegre edilmektedir (Şahiner et al, 2021: 87). Bu alandaki önemli girişimlerden biri de ABD Ulusal Güvenlik Ajansı’nın (Ulusal Güvenlik Ajansı / NSA / National Security Agency) kurduğu NSA–AI Security Center’dir. Bu merkez, AI destekli güvenlik tehditlerini proaktif olarak tespit etmek ve önlemek amacıyla faaliyet göstermektedir. Merkez, AI sistemlerinde ortaya çıkabilecek güvenlik açıklarını önceden analiz ederek, bu teknolojilerin kötü amaçlı kullanımlarını engellemek ve ulusal güvenliği korumak için sürekli olarak gelişmiş algoritmalar ve stratejiler geliştirmektedir (NSA Raporu, 2025: 36). Böylece, AI temelli dezenformasyon ve manipülasyon tehditlerine karşı daha etkin ve önleyici bir mücadele imkanı sağlanmaktadır.

AI, siber ve fiziksel tehditlerin erken aşamada tespit edilmesinde kritik rol oynamaktadır. Siber saldırıların önceden algılanması ve etkili müdahale için ABD’de NSA AI Security Center ve İngiltere’de Ulusal Siber Güvenlik Merkezi (Ulusal Siber Güvenlik Merkezi / NCSC / National Cyber Security Centre) gibi kurumlar AI tabanlı erken uyarı sistemleri geliştirmiştir. AI Security Center ve İngiltere’deki NCSC gibi kurumlar, AI tabanlı erken uyarı sistemleri geliştirerek siber tehditlere karşı proaktif savunma mekanizmaları oluşturmaktadır. NCSC, Birleşik Krallık’ın ulusal siber

güvenlik otoritesi olarak, AI destekli algoritmalarla ağdaki anormal aktiviteleri tespit etmekte ve bu sayede siber saldırıların erken aşamada engellenmesini sağlamaktadır (NCSC Annual Review, 2023: 15). Bu tür sistemler, özellikle gelişmiş tehditlerin hızlı tanımlanması ve müdahale süreçlerinin optimize edilmesinde kritik rol oynamaktadır.

Fiziksel güvenlik alanında ise Dubai'nin Oyoon Projesi, AI destekli yüz tanıma ve hareket analizi teknolojilerini kullanarak suç önleme ve kamusal güvenliği artırmayı amaçlamaktadır. Oyoon, şehir genelinde kurulan yüksek çözünürlüklü kameralar aracılığıyla gerçek zamanlı yüz tanıma ve davranış analizi yaparak potansiyel tehditleri erken aşamada tespit etmektedir. Böylece güvenlik güçlerine anlık uyarılar gönderilerek müdahale süreleri kısaltılmaktadır (Al-Kuwari & Hassan, 2024: 98). Bu gelişmeler, AI'nın hem dijital hem de fiziksel güvenlik alanlarında önemli bir rol üstlendiğini göstermektedir.

Siber savunma ve saldırı tespit sistemleri ise bir diğer önemli teknoloji aracı olarak devletlerin kritik altyapılarını, bilgi sistemlerini ve dijital varlıklarını koruma amacıyla yürüttükleri savunma faaliyetleridir. AI ise bu alanda, saldırıların hızlı tespiti, analizi ve önlenmesinde önemli bir rol oynayarak, büyük veri analizi ve anomali tespiti gibi yöntemlerle proaktif savunma sağlar (Brundage et al., 2018: 23). Örneğin, 2007'de yaşanan geniş çaplı siber saldırılar sonrası Estonya, siber güvenlik alanında önemli adımlar atarak Siber Savunma Merkezi kurmuştur. Böylelikle, AI ve otomatik izleme teknolojileri kullanarak ulusal ağları korumakta, saldırı örüntülerini analiz etmekte ve hızlı müdahale mekanizmaları geliştirmektedir. Bu merkez, Estonya'yı dijital güvenlikte dünya liderlerinden biri haline getirmiştir (Kaska, 2018: 45).

Uluslararası arenada önemli bir yer edinen Almanya perspektifine bakıldığında ise, Almanya'nın Yeni Siber Güvenlik Ajansı: Almanya, Bundeswehr (Silahlı Kuvvetler) bünyesinde geliştirdiği yeni siber güvenlik ajansı ile dijital altyapısını korumaya yönelik AI tabanlı araçlar geliştirmektedir. Bu ajans, AI destekli izleme, saldırı tespiti ve savunma sistemleriyle devlet ağlarını hedef alan karmaşık siber tehditlere karşı etkin bir koruma sağlamayı amaçlamaktadır (Gabelein & Bundeswehr Cyber Strategy, 2022: 12).

Gözetim ve veri izleme teknolojileri de güvenlik alanında önemli bir yer edinmektedir; devletlerin halk hareketlerini takip etme ve toplumsal eğilimleri analiz etme amacıyla yaygın biçimde kullanılmaktadır. ABD'nin PRISM ve XKeyscore gibi gözetim programları, sosyal medya ve iletişim verilerini analiz ederek toplumsal eğilimlerin ve potansiyel tehditlerin erken tespiti için geliştirilmiştir. Bu tür gözetim sistemleri, özellikle Arap Baharı gibi toplumsal hareketlerin izlenmesinde dolaylı olarak etkili olmuştur (Şahiner, Ayhan & Önder, 2021: 83 - 95).

Aynı zamanda veri analizi ile terör ve suç öngörü sistemleri de devletlerin gözdesi konumundadır. ABD ve İngiltere, polis teşkilatlarında suç analitiği ve risk değerlendirme sistemleri ile yüksek riskli bölgeleri belirleyerek kaynaklarını etkin bir şekilde yönetmektedir. Benzer şekilde, Suudi Arabistan'ın NEOM projesinde ise gelişmiş veri analitiği ve AI tabanlı güvenlik sistemleri kullanılarak suç oranlarını minimize etmek ve kamu düzenini sağlamak hedeflenmektedir. NEOM, otonom güvenlik cihazları, yüz tanıma teknolojileri ve büyük veri analizleriyle donatılmış olup, geleceğin akıllı şehir modelleri arasında yer almaktadır (NEOM, t.y.).

Gelişen teknoloji çağı, günümüzün artan sorunları olarak açığa çıkan sınır güvenliği ve göç yönetimi konularında da aktif bir saha çalışmasına sahiptir. Bu alanda gelişen otonom devriye robotları dikkat çekmektedir. Otonom devriye robotları, sınır güvenliği ve göç yönetiminde etkinliği artırmak amacıyla hızla yaygınlaşan teknolojik çözümlerden biridir. AI destekli bu robotlar, sensör ve görüntü işleme teknolojileri sayesinde sınır hatlarında sürekli devriye yapmakta, anormal hareketleri algılayarak güvenlik birimlerine anlık bilgi aktarmaktadır. Bu sayede insan gücüne olan bağımlılık azalmakta ve geniş sınır bölgelerinin etkin kontrolü mümkün hale gelmektedir (Çifçi, 2024: 158 - 170). Bu sayede insan gücüne olan bağımlılık azalmakta ve geniş sınır bölgelerinin etkin kontrolü mümkün hale gelmektedir.

Göç yönetimi bağlamında, bu robotlar yasa dışı geçişleri önlemeye yönelik kritik araçlar olarak kullanılmaktadır. Özellikle ABD - Meksika sınırı gibi yoğun göç hareketlerinin yaşandığı bölgelerde, AI tabanlı devriye sistemleri sınır ihlallerini daha hızlı tespit edebilmekte ve müdahale süresini kısaltmaktadır (Smith & Roberts, 2023: 117-120). Ayrıca, gelişmiş analiz yetenekleriyle riskli alanlar belirlenerek güvenlik

kaynaklarının daha stratejik kullanımı sağlanmaktadır (Jones, Thompson & Garcia, 2021: 55-57).

Suudi Arabistan'ın NEOM projesi de bu alanda etkin bir çalışma sergilemektedir. Akıllı sınır yönetimi sistemleri kapsamında otonom devriye robotları göç kontrolü ve sınır güvenliğinin bir parçası olarak entegre edilmektedir. Bu sistemler, göçmen akışlarını izlemek ve güvenlik tehditlerini önceden tespit etmek için AI destekli veri analitiğiyle desteklenmektedir (NEOM, 2024: 12-15). Böylece hem insan hataları minimize edilmekte hem de sınır geçişleri daha kontrollü ve güvenli hale getirilmektedir. Görülmektedir ki, otonom devriye robotları göç ve sınır yönetiminde güvenliği artıran, insan gücüne destek sağlayan ve operasyonel verimliliği yükselten kritik teknolojik araçlar olarak önem kazanmaktadır (Brown & Liu, 2023, s: 210-213).

Sosyal ağların global düzlemde bağımsız hareketi ise günümüzün en çarpıcı güvenlik teknolojisi alanındaki ihtiyacını doğurmuştur. Güvenli iletişim ağları ve şifreleme teknolojileri, devletlerin ve kurumların dijital ortamda veri bütünlüğünü ve gizliliğini sağlamak için vazgeçilmez araçlardır. Özellikle kritik altyapıların korunmasında, iletişim kanallarının güvenliği ön plandadır. Bu kapsamda, gelişmiş şifreleme teknikleri veri iletiminde yetkisiz erişimi engeller ve bilgi sızıntılarını önler (Chen, Patel & Kumar, 2022: 144-146).

AB perspektifinde GDPR, bireysel verilerin korunması için standartlar belirlerken, AB ülkelerinde güvenli iletişim için AI destekli şifreleme çözümleri geliştirilmektedir. Bu çözümler, veri trafiğini analiz ederek anomali tespiti yapabilmekte ve potansiyel tehditlere karşı otomatik savunma mekanizmaları oluşturabilmektedir (Müller & Fischer, 2023: 97-99). Almanya ve İngiltere, bu alanda öncü ülkeler arasında yer almakta, siber güvenlik stratejileri doğrultusunda kuantum şifreleme gibi ileri teknolojilere yatırım yapmaktadır (Schmidt, 2021: 58-61).

Özellikle devletlerarası iletişimde, uluslararası işbirlikleri için güvenli ve şifreli kanallar kritik öneme sahiptir. AI algoritmaları, bu sistemlerin yönetiminde proaktif tehdit tespiti ve güvenlik ihlallerinin erken müdahalesi için kullanılmaktadır (Lopez et al., 2022: 230-232). Bu sayede, hem kamu kurumlarının hem de özel sektörün iletişim güvenliği üst düzeye çıkarılmakta, olası siber saldırıların etkisi minimize edilmektedir.

Görölmektedir ki, güvenli iletiřim aęları ve řifreleme sistemleri, dijital çağda bilgi güvenlięinin temel yapı taşlarıdır. AI destekli řifreleme teknolojileri, veri mahremiyetinin korunmasında, iletiřim aęlarının güvenilirliğinde ve siber tehditlere karşı direncin artırılmasında kritik roller üstlenmektedir (Wang & Zhao, 2023: 175-178).

Sanal dünyada giderek karmařıklařan tehditler, devletleri AI tabanlı güvenlik teknolojilerine yönlendirmiřtir. Bu teknolojiler, hem siber hem de fiziksel güvenlik alanlarında tehdit algılama, erken uyarı, müdahale ve önleme kapasitesini artırmaktadır. Kuzey Kore'den Dubai'ye, ABD'den AB'ye kadar pek çok ölke, kendi ulusal güvenlik hedefleri doęrultusunda bu teknolojileri kullanmakta ve geliřtirmektedir. Bu bağlamda, AI destekli güvenlik uygulamalarının stratejik önemi gelecekte daha da artacaktır (řahiner, Ayhan & Önder, 2021: 45 - 50).

1.3.2. Yapay Zeka Çatıřma Teknolojileri

AI, günümüz savař ve çatıřma ortamlarında giderek daha kritik bir rol üstlenmektedir. Aktif çatıřma, savař operasyonları ve saldırı-savunma süreçlerinde kullanılan AI destekli teknolojiler, savař alanında stratejik üstünlük sağlamada önemli bir unsur haline gelmiřtir. Bu teknolojiler, hem fiziksel hem de siber ortamda çatıřmaların řeklini ve dinamiklerini köklü biçimde deęiřtirmektedir (Brundage et al., 2018: 54).

Özellikle Otonom Silah Sistemleri (Lethal Autonomous Weapon Systems / LAWS), insan müdahalesi olmadan hedef tespit edip ateř edebilme yeteneęiyle tartıřmalara konu olmaktadır. ABD, Çin ve Rusya gibi ölkeler bu alanda yoğun arařtırmalar yapmakta, AI destekli hedefleme sistemleri ile insansız hava araçları (İHA) ve insansız kara araçları (İKA) gibi platformlarda yüksek hassasiyet ve özerklik sağlanmaktadır (Scharre, 2018: 67-70).

Savař alanı robotları ise kara operasyonlarında askerlerin yerine riskli görevleri üstlenmekte, keřif ve nöbet görevlerinde kullanılmaktadır. Bunlar, otonom navigasyon ve durumsal farkındalık sistemleriyle donatılarak savař alanındaki karar destek mekanizmalarını güçlendirmektedir (Singer, 2009: 112). Siber savař ve elektronik harp sistemleri, modern çatıřmalarda giderek daha ön plana çıkmaktadır. Rusya'nın GRU'ya

bağlı Unit 26165 gibi AI destekli siber operasyon birimleri, hem savunma hem de saldırı amaçlı karmaşık siber saldırılar gerçekleştirmektedir (Rid, 2020: 98). İsrail gibi ülkeler ise AI tabanlı İHA sistemleri ile hem hava sahası kontrolü hem de siber ve elektronik harp kabiliyetlerini entegre etmektedir (Ditter, 2024: 1 - 25).

Özellikle İsrail, AI tabanlı İHA sürüleri ve gelişmiş hava savunma sistemleriyle modern çatışma teknolojilerinde öncü ülkeler arasında yer almaktadır. İHA sürüleri, AI algoritmaları sayesinde koordineli ve otonom görevler gerçekleştirebilmekte; bu da hava sahası kontrolü ve keşif operasyonlarında büyük avantaj sağlamaktadır. İHA sürüleri, düşman hedeflerini hızlı tespit edip, elektronik harp faaliyetleriyle entegre şekilde hareket ederek hem hava hem de siber savaş kabiliyetlerini güçlendirmektedir (Ditter, 2024: 1 - 25).

Bir diğer yandan, İsrail'in HAROP ve HARPY sistemleri, AI destekli saldırı İHA'ları arasında öne çıkar. HARPY, düşman radarlarını tespit edip otonom olarak hedefe yönelirken; HAROP, daha gelişmiş bir kamikaze tipi İHA olarak, yüksek hassasiyetle seçilen hedeflere intihar saldırıları düzenlemektedir. Her iki sistem de düşman hava savunma ağlarını etkisiz hale getirmeye yönelik tasarlanmış olup, modern savaşlarda elektronik harp ve istihbaratın entegrasyonunu sağlamaktadır (Israel Aerospace Industries, t.y.)

Bunun yanında, İsrail'in Demir Kubbe (Iron Dome) hava savunma sistemi, roket saldırılarını tespit edip AI destekli radar ve füzelerle hedefleri otomatik olarak vurabilmektedir. Bu sistem, şehirleri ve kritik altyapıları korumada yüksek başarı oranıyla dikkat çekmekte, gerçek zamanlı veri işleme ve hızlı karar alma özellikleriyle AI teknolojilerinin etkin bir örneğini sunmaktadır (Smith & Cohen, 2022: 112-115). AI ayrıca durumsal farkındalık ve karar destek sistemleri ile askeri komutanlara gerçek zamanlı ve analitik veri sağlamaktadır. Bu sistemler, hızlı karar alma süreçlerini kolaylaştırarak insan hata payını azaltmakta ve savaş etkinliğini artırmaktadır (Kott, 2019: 23).

Bunun yanında, otonom lojistik ve ikmal sistemleri, çatışma bölgelerine malzeme ve destek sağlama süreçlerini otomatikleştirerek operasyonların sürekliliğini garanti altına almaktadır. Bu sistemler, hem güvenlik hem de etkinlik açısından büyük

avantajlar sunmaktadır (Schultz, 2020: 77). Hedef tanıma ve takip teknolojileri, gelişmiş AI algoritmaları sayesinde düşman unsurlarının hızlı ve doğru biçimde tespit edilmesini mümkün kılarak askeri operasyonlarda hassasiyeti artırmaktadır (Biddle, 2021: 60).

Ayrıca, psikolojik operasyonlar ve dezenformasyon kampanyalarında AI algoritmaları kullanılmakta, propaganda ve bilgi savaşları bu sayede daha sofistike bir hal almaktadır (Bradshaw & Howard, 2019: 89). Savaş simülasyonları ve eğitim sistemlerinde ise AI, gerçekçi ve dinamik senaryolar oluşturarak askerlerin hazırlık seviyesini yükseltmektedir (Anderson, 2022: 101). AI destekli çatışma teknolojileri, hem fiziksel hem de siber savaş alanında çok boyutlu bir dönüşümü temsil etmekte; bu durum, askeri strateji ve uluslararası güvenlik dinamiklerini derinden etkilemektedir.

1.4. Dijital Müdahale

Dijital müdahale, günümüzde uluslararası çatışmaların en önemli cephelerinden biri haline gelmiştir. Devletler, AI destekli teknolojilerle rakiplerine yönelik dezenformasyon kampanyaları, siber casusluk faaliyetleri ve altyapı sabotajları gibi çeşitli dijital yöntemler kullanmaktadır. Örneğin, 2016 ABD Başkanlık Seçimleri sırasında Rusya tarafından yürütülen AI destekli dezenformasyon kampanyaları, sosyal medya platformlarında sahte haberlerin yayılması yoluyla kamuoyu algısını şekillendirmede etkili olmuştur (Mueller Raporu, 2019: 67; Bradshaw & Howard, 2018: 45-50). Bu kampanyalarda bot ağları ve AI algoritmaları, mesajların hızla geniş kitlelere ulaşmasını sağlamış, demokratik süreçlere müdahalede bulunmuştur.

Son yıllarda, dijital teknolojilerin demokratik süreçlere entegrasyonu kapsamında dijital oylama sistemleri geliştirilmiştir. Dijital oy kullanma, seçim süreçlerini hızlandırma ve erişilebilirliği artırma potansiyeline sahip olmakla birlikte, siber güvenlik açılarından ciddi riskler barındırmaktadır. Blockchain gibi teknolojiler güvenli ve şeffaf oy sayımı için umut vaat etse de, sistemlerin hacklenmesi, oy manipülasyonu ve kimlik doğrulama sorunları demokratik meşruiyet açısından kritik tehditler oluşturmaktadır (Kshetri, 2020: 112-115; De Filippi & Wright, 2018: 78-80). Bu durum, dijital müdahalelerin sadece dezenformasyon ve siber casuslukla sınırlı kalmayıp, demokratik süreçlerin bütünlüğüne doğrudan yönelik tehditleri de kapsadığını göstermektedir.

Bu bağlamda, siber casusluk ise dijital müdahalenin bir diğer kritik alanıdır. Çin'in APT (Advanced Persistent Threat / Gelişmiş Kalıcı Tehdit) gruplarının ABD ve Avrupa ülkelerindeki kritik bilgi sistemlerine yönelik AI destekli siber saldırıları, stratejik veri hırsızlığında yeni bir boyut açmıştır (Martínez & Durán, 2021: 538-540). APT grupları, devlet destekli, gelişmiş teknikler kullanarak uzun süreli ve gizli siber saldırılar gerçekleştiren hacker ekipleridir. Bu gruplar, ekonomik ve askeri hedeflere yönelik stratejik bilgi toplama amacıyla kritik altyapılara sızmaktadır (Mandiant, 2021: 4-16). Benzer şekilde, Kuzey Kore kaynaklı hacker grupları da ekonomik ve askeri hedeflere yönelik gelişmiş AI tabanlı siber operasyonlarla dikkat çekmektedir.

Bunun yanı sıra, dijital sabotaj operasyonları ulusal altyapıların işleyişini hedef alarak devletler arası gerginlikleri artırmaktadır. 2010'da İran'ın nükleer tesislerini hedef alan Stuxnet virüsü, dijital sabotajın en somut örneklerinden biridir. ABD ve İsrail'in ortak geliştirdiği bu virüs, İran'ın Natanz'daki santrifüjleri hedef alarak nükleer programını yavaşlatmayı amaçlamıştır (Zetter, 2014: 78). Stuxnet saldırısının sonucu olarak ise, İran'ın zenginleştirilmiş uranyum üretmek amacıyla kullandığı Natanz tesisinde bulunan santrifüjleri önemli ölçüde zarar gördüğü ve nükleer programı geçici olarak yavaşladığı kayıtlara geçmiştir.

Ancak, bu saldırı aynı zamanda siber savaşın boyutlarını ve etkilerini uluslararası arenada görünür kılmakta önemli bir yapı taşı olmuştur. İran, saldırının ardından siber savunma kapasitesini hızla geliştirme yönünde adımlar atarak dünya genelinde devlet destekli siber saldırıların artmasında etken ülke konumunda yer almıştır. Böylece, dijital sabotajın stratejik bir silah olarak kullanılabileceği gözler önüne serilirken, siber saldırıların ulusal güvenlik için kritik bir tehdit haline geldiğinin de altı çizilmiştir (Zetter, 2014: 95-98). Günümüzde ise bu tür gelişmiş dijital saldırılar enerji santralleri, su arıtma tesisleri ve finansal sistemler gibi kritik altyapılara yönelmekte, devletlerin savunma mekanizmalarını sürekli test etmektedir.

Ekonomik alanda dijital müdahaleler, günümüzde uluslararası rekabetin kritik bir boyutunu oluşturuyor. Özellikle ABD ile Çin arasındaki dijital rekabet, AI destekli algoritmaların finansal piyasalarda manipülasyon amacıyla kullanılmasıyla şekillenmektedir. Örneğin, Çin kaynaklı bazı siber grupların, algoritmik ticaret sistemlerine yönelik saldırılarla piyasa dalgalanmalarına yol açtığı rapor edilmiştir. Bu

saldırıları, AI algoritmalarının finansal verileri manipüle ederek hisse senedi fiyatlarını yapay olarak düşürüp yükseltmek gibi yöntemlerle piyasa istikrarını bozmayı hedeflemektedir (Zeng & Liu, 2021: 103).

2015 yılında Çin ile ABD borsaları arasında yaşanan ani ve beklenmedik dalgalanmalarda, bu tür dijital müdahalelerin etkili olduğu yönünde çeşitli analizler yapılmıştır. Özellikle yüksek frekanslı ticaret algoritmalarının manipüle edilmesi, kısa sürede büyük ekonomik kayıplara ve güven kaybına neden olmuştur (Smith, 2017, s: 45-47). Ayrıca, 2020 yılında ABD'nin teknoloji sektörüne yönelik Çin menşeli siber casusluk faaliyetleri ve veri hırsızlıkları, ticari sırların çalınması yoluyla ekonomik rekabeti dezavantajlı hale getirmiştir (Trellix Raporu, 2024).

Bu tür dijital müdahaleler sadece finansal piyasalarla sınırlı kalmayıp, aynı zamanda kritik ticaret altyapılarına, örneğin tedarik zinciri yönetimi ve lojistik sistemlerine yönelik saldırılarla da ekonomik savaşı yeni bir boyuta taşımaktadır. Çin'in, ABD'nin bazı stratejik tedarik zincirlerine yönelik siber saldırılar düzenlediği ve bu saldırılarda AI destekli analiz yöntemleri kullandığı belirtilmektedir (Bartholomew et al., 2022, 418 - 464).

Tüm bu müdahaleler, uluslararası hukuk açısından yeni zorluklar doğurmaktadır. Dijital egemenlik ve siber savaş kavramlarının hukuki sınırları henüz netleşmemiş olup, uluslararası toplum AI tabanlı dijital müdahalelere karşı normlar geliştirmeye çalışmaktadır (Schmitt, 2017: 75-77). Bu gelişmeler, dijital çağda uluslararası ilişkilerin dinamiklerini ve çatışma biçimlerini köklü biçimde değiştirmektedir.

1.5. Uluslararası Örgütler ve Yapay Zeka

AI teknolojilerinin hızla gelişmesi, uluslararası güvenlikten ekonomiye, insan haklarından etik değerlere kadar birçok alanda derin ve karmaşık etkiler yaratmaktadır (Russell, 2020: 15). Bu teknolojilerin sınır tanımayan yapısı, devletler arası ilişkileri yeniden şekillendirirken, potansiyel riskler ve fırsatlar da beraberinde gelmektedir (Floridi, 2019: 42). Uluslararası örgütler, bu yeni teknolojik ortamda düzenleyici ve denetleyici roller üstlenerek, AI algoritmalarının etik, güvenli ve şeffaf kullanımını teşvik etmekte ve küresel iş birliğini kolaylaştırmaktadır (UNESCO, 2021: 10).

Bu bağlamda, uluslararası örgütlerin amacı; AI'nın etik kullanımı için evrensel standartlar geliştirmek, kötüye kullanımını önlemek, veri güvenliği ve bireysel mahremiyeti korumak, sürdürülebilir kalkınmayı desteklemek ve uluslararası barış ile güvenliği sağlamak gibi temel hedefleri içermektedir (Floridi, 2019: 47; UNESCO, 2021: 14).

Uluslararası iş birliği gerekliliği, özellikle AI uygulamalarının sınırları aşan etkileri ve riskleri göz önüne alındığında, kritik bir öneme sahiptir. Devletler ve diğer aktörlerin AI teknolojilerini düzenlemek amacıyla oluşturdukları ortak çabalar, teknolojinin olası olumsuz sonuçlarını minimize etmeye yöneliktir (Cath, 2018: 133). Bu doğrultuda, uluslararası örgütler tarafından geliştirilen standartlar, ilkeler ve çerçeveler, etik sorunların çözümünde ve uluslararası normların oluşturulmasında kilit rol oynamaktadır (Jobin, Ienca & Vayena, 2019: 325).

Buna ek olarak, bu örgütler AI'nın askeri, ekonomik ve sosyal boyutlarda kullanımına ilişkin politikalar geliştirerek, teknolojinin kötüye kullanımını engellemek ve sürdürülebilir kalkınmayı desteklemek amacıyla koordinasyon sağlamaktadır (OECD, 2020: 27). Özellikle AI'nın silah sistemlerine entegrasyonu, veri güvenliği ve mahremiyet konuları uluslararası platformlarda yoğun şekilde tartışılmakta ve bu alanlarda küresel normlar oluşturulmaya çalışılmaktadır (Crotoft, 2016: 150).

Bu çerçevede, AI alanındaki uluslararası iş birliği, hem teknolojinin sunduğu fırsatların en iyi şekilde değerlendirilmesini hem de olası risklerin etkin biçimde yönetilmesini mümkün kılmaktadır (Bryson & Winfield, 2017: 9). Bu kapsamda,

uluslararası örgütlerin AI konusundaki stratejik rolü, geleceğin dijital güvenlik ve etik standartlarının belirlenmesinde belirleyici olacaktır.

1.5.1. NATO

NATO (Kuzey Atlantik İşbirliği Örgütü / North Atlantic Treaty Organisation), üye ülkelerin kolektif savunmasını sağlayan uluslararası bir askeri ittifaktır. Soğuk Savaş sonrası dönemde değişen güvenlik ortamı ve teknolojik gelişmeler, NATO'nun stratejik önceliklerinde önemli dönüşümlere yol açmıştır (Smith, 2020: 45). Özellikle AI, savunma ve güvenlik alanında yeni fırsatlar ve riskler yaratması sebebiyle NATO'nun gündeminde öncelikli bir konu haline gelmiştir.

NATO, AI teknolojilerinin savunma alanında etik, güvenli ve etkin kullanımını destekleyerek, üyeleri arasında teknolojik uyum ve iş birliğini artırmayı amaçlamaktadır (NATO, 2021: 12a). Bununla birlikte, AI'nın askeri uygulamalarda insan kontrolünden çıkarak otomasyona geçişi gibi etik ve operasyonel risklere karşı ortak standartlar oluşturmak da NATO'nun sorumlulukları arasındadır (Johnson & Miller, 2022: 88).

Bu kapsamda, NATO 22 Ekim 2021'de kabul ettiği AI Stratejisi ile AI'nın sorumlu kullanımını teşvik etmektedir. Strateji, etik ilkeler çerçevesinde AI'nın güvenilir, yönetilebilir ve önyargıdan arındırılmış biçimde geliştirilmesini hedeflemektedir (NATO, 2021: 10-15). Ayrıca, örgüt 2023 yılında AI sertifikasyon standardı geliştirme çalışmalarına başlamış; bu standartla AI sistemlerinin güvenilirlik, izlenebilirlik ve yönetilebilirlik gibi kriterlere uygunluğunu belgelendirmeyi amaçlamaktadır (ACT NATO, 2023: 9).

NATO, AI alanında uluslararası iş birliğini ve bilgi paylaşımını artırarak, savaş alanındaki karar destek sistemleri, otonom silahlar ve siber savunma teknolojilerinde entegrasyonu güçlendirmektedir (NATO, 2022: 24b). Bu doğrultuda, müttefiklerin siber güvenlik kapasitelerini yükseltmekte ve personelin AI teknolojilerine adaptasyonu için kapsamlı eğitim programları düzenlemektedir (Williams, 2023: 37).

Örgütün yaklaşımı, AI'nın güvenlik alanındaki potansiyel faydalarını maksimize ederken, teknolojinin silahlanma yarışını ve etik ihlalleri önlemeye yöneliktir. NATO, uluslararası normlar ve insani hukuk ilkelerine uyumu vurgulayarak, AI etiği ve düzenlemesinde öncü rol oynamayı sürdürmektedir (Green, 2021: 102; Brown &

Clarke, 2022: 54). NATO Parlamento Meclisi'nin 2024 yılında kabul ettiği “Askeri Alanda Yapay Zeka Sorumlu Kullanımının Fırsatları” kararında da bu hedefler teyit edilmiştir; karar, müttefik ülkeler arasında AI araştırma ve geliştirme iş birliğinin artırılması, etik ve hukuki çerçevenin oluşturulması yönünde somut adımlar atılmasını önermektedir (NATO PA, 2024: 7). Bu bilgiler ışığında görülmektedir ki, NATO AI savunma ve güvenlik alanında sorumlu, etik ve etkili şekilde kullanarak üye ülkeler arasında uyumu sağlamakta ve bu alandaki uluslararası standartların belirlenmesinde kritik bir rol üstlenmektedir.

1.5.2. Birleşmiş Milletler

Birleşmiş Milletler (BM / United Nations), küresel barış, güvenlik, insan hakları ve sürdürülebilir kalkınma alanlarında uluslararası iş birliğini teşvik eden en kapsamlı örgüttür (Weiss, 2019: 22). AI alanında BM, teknolojinin etik, adil ve insan haklarına saygılı biçimde geliştirilmesi ve kullanılması için çeşitli platformlarda aktif rol almaktadır (UNESCO, 2021: 14).

BM, AI'ın getirdiği fırsatları değerlendirirken, aynı zamanda teknolojinin yol açabileceği riskler ve ayrımcılık gibi sorunlara karşı küresel standartlar oluşturmayı amaçlamaktadır (Cath, 2018: 130). Bu bağlamda, BM Genel Kurulu ve ilgili alt organları, AI etiği, güvenlik ve insan hakları gibi konularda çalışmalar yürütmekte ve uluslararası toplumu bu alanlarda uyumlu politika geliştirmeye çağırmaktadır (UN Secretary-General, 2020: 9).

Özellikle 2021 yılında UNESCO'nun öncülüğünde hazırlanan “Yapay Zeka Etiği İlkeleri” bildirgesi, BM çatısı altında kabul edilmiş ve AI'ın adil, şeffaf ve hesap verebilir bir şekilde kullanılmasını teşvik eden küresel bir rehber olarak benimsenmiştir (UNESCO, 2021: 7). BM, ayrıca sürdürülebilir kalkınma hedeflerine ulaşmada AI'ın kullanımını desteklemek ve dijital uçurumu azaltmak için projeler geliştirmektedir (United Nations, 2022: 16).

Bunun yanı sıra, BM çatısı altında oluşturulan “Çevrimiçi Güvenlik ve Siber Alan Komisyonu”, AI destekli siber tehditlerin önlenmesi ve küresel siber güvenlik iş birliğinin artırılması yönünde stratejiler geliştirmektedir (ITU, 2023: 25). BM'nin bu

alandaki çalışmaları, uluslararası hukuk ve insan hakları normlarına uygunluk temelinde teknolojinin sorumlu kullanımını sağlamaya odaklanmaktadır (Schroeder, 2020: 34).

BM, AI teknolojilerinin etik ve sorumlu kullanımını destekleyerek, uluslararası toplumun dijital dönüşüm sürecinde güvenlik, adalet ve sürdürülebilirlik ilkeleri doğrultusunda hareket etmesini sağlamayı hedeflemektedir (Floridi, 2019: 50).

1.5.3. Avrupa Birliği

AB, ekonomik entegrasyon ve politik iş birliği amacıyla kurulmuş çok uluslu bir yapıdır ve günümüzde dijital dönüşüm ile teknolojik gelişmelerde lider bir aktör konumundadır (Smith, 2021: 30). AB, AI teknolojilerinin ekonomik büyüme, toplumsal fayda ve bireysel hakların korunması çerçevesinde geliştirilmesini ve düzenlenmesini önceliklendirmektedir (European Commission, 2020: 15a).

AB'nin AI yaklaşımı, etik standartlar ve düzenleyici çerçeveler oluşturma temeline dayanmaktadır. 2021 yılında yayımlanan “Yapay Zeka için Etik İlkeler” belgesi, şeffaflık, hesap verebilirlik, insan merkezilik ve veri koruma gibi temel değerleri vurgulamaktadır (European Commission, 2021: 7). Bu ilkeler, AB'nin Dijital Tek Pazar stratejisi kapsamında AI uygulamalarının güvenilir ve sorumlu kullanımını sağlamayı hedeflemektedir (González & Martínez, 2022: 44b).

AB ayrıca, AI'nın düzenlenmesi için kapsamlı bir yasal çerçeve sunan “Yapay Zeka Yönetmeliği Taslağı”nı (AI Yasası) 2021 yılında kamuoyuna sunmuştur. Bu yönetmelik, yüksek riskli AI uygulamalarına sıkı denetim getirmekte, kullanıcı haklarını korumakta ve yenilikçi teknolojilerin güvenle geliştirilmesini desteklemektedir (European Parliament, 2021: 12). Yönetmeliğin temel hedefleri arasında; AI'nın insan hakları ve temel özgürlüklerle uyumlu olması, ayrımcılığı önlemesi ve veri güvenliğini garanti altına alması bulunmaktadır (Kumar & Weber, 2023: 56). Bundan hareketle, AI Yasa'sı temelini oluşturan “risk temelli yaklaşım” aşağıdaki gibi dört kategoriye ayrılmıştır:

Tablo 1. Avrupa Birliği AI Yasa'sı Kapsamında Yapay Zeka Sistemlerinin Risk Sınıflandırması

Risk Seviyesi	Tanım / Örnek Uygulamalar	Yükümlülükler / Düzenlemeler
Kabul Edilemez(Unacceptable)	Sosyal Skorlama, davranış manipülasyonu, gerçek zamanlı biyometrik tanıma uygulamaları.	Yasak. Piyasaya Sürümleri Tamamen Engellenmiştir.
Yüksek Riskli(High Risk)	Sağlık, ulaşım, adalet gibi alanlarda kullanılan sistemler (örneğin biyometrik kimlik tespiti).	Katı testler, uygunluk değerlendirmesi, insan gözetimi, veri kalitesi ve teknik belgelendirme zorunludur.
Sınırlı Risk(Limited Risk)	Chatbot'lar, içerik üretimi sistemleri, deepfake uygulamaları gibi sistemler. Kullanıcıların AI ile etkileşimde olduklarını bilmeleri gereken sistemler.	Kullanıcı bilgilendirmesi ve şeffaflık yükümlülüğü uygulanır. Kullanıcı bilgilendirmesi; üretilen içeriğin AI tarafından üretildiğinin belirtilmesi.
Düşük / Hiç Risk(Minimal Risk)	Spam filtreleri, oyunlar gibi sıradan uygulamalar.	Düzenleme yoktur; genel mevzuata uyum yeterlidir.

Kaynak: Tablo, European Commission, 2021; Consilium, 2024; artificialintelligenceact.eu, 2024 verileri kullanılarak yazar tarafından oluşturulmuştur.

AB'nin AI düzenlemeleri çerçevesinde geliştirilen AI Yasası, teknolojik gelişmeleri yönlendirmenin ötesinde, bu gelişmelerin birey hakları ve toplumsal değerlerle uyumlu olmasını sağlamayı hedefleyen kapsamlı bir yaklaşımdır. Bu düzenleme, AI sistemlerini taşıdıkları risk düzeylerine göre dört kategoriye ayırmakta ve her bir kategoriye özgü yasal yükümlülükler getirmektedir (European Commission, 2021: 12). En yüksek risk grubunu oluşturan ve “kabul edilemez” olarak tanımlanan

sistemler, temel hakları ihlal etme potansiyeli nedeniyle tamamen yasaklanmıştır. Bu kapsamda sosyal skorlama uygulamaları, kamusal alanda gerçek zamanlı biyometrik tanıma sistemleri ve kullanıcıları manipüle eden algoritmalar yer almaktadır (European Commission, 2021: 15). Bu sistemlerin Avrupa pazarına girişi yasak olup, düzenleyici çerçevenin en katı kısmını oluşturmaktadır.

Öte yandan, sağlık, eğitim, kamu güvenliği ve adalet gibi alanlarda kullanılan AI sistemleri “yüksek riskli” olarak tanımlanmakta; bu sistemler için sıkı şartlar ve denetim mekanizmaları getirilmektedir. Bu yükümlülükler arasında veri kalitesinin sağlanması, insan gözetimi, teknik belgelerin oluşturulması ve şeffaflık gibi unsurlar yer almaktadır (European Commission, 2021: 20–22; Consilium, 2024). Daha düşük risk grubunda yer alan ve “sınırlı risk” olarak adlandırılan uygulamalar, kullanıcıyla doğrudan etkileşime giren ancak ciddi sonuçlar doğurmeyen sistemleri kapsamaktadır. Chatbot’lar, deepfake içerik üreticileri veya öneri sistemleri gibi teknolojiler bu kapsama dâhildir ve yalnızca kullanıcıların AI ile etkileşimde olduklarının açıkça belirtilmesi gerekmektedir (European Union, 2024).

Son olarak, “minimal veya yok denecek düzeyde risk” taşıyan sistemler ise genellikle düzenlemeye tabi tutulmamakta, yalnızca genel AB mevzuatına uygunluk beklenmektedir. Bu grupta oyun içi AI, spam filtreleri gibi gündelik kullanımda yer alan ve kullanıcı güvenliğini doğrudan tehdit etmeyen uygulamalar yer almaktadır (European Commission, 2021: 28d). AB’nin bu risk temelli yaklaşımı, AI teknolojisinin etik, güvenli ve toplumsal sorumluluk taşıyan bir şekilde gelişmesini sağlamayı amaçlamakta, aynı zamanda inovasyonu teşvik ederken temel hakların korunmasını garanti altına almaktadır. Böylece AB, yalnızca teknolojik liderlik hedefiyle değil, aynı zamanda küresel düzeyde dijital yönetim standartlarını belirleme iddiasıyla hareket etmektedir.

Buna ek olarak, AB Komisyonu 2020 yılında “Avrupa Yapay Zeka Stratejisi”ni yayımlayarak AI araştırmaları ve inovasyonuna önemli yatırımlar yapmayı taahhüt etmiştir. Bu strateji, AB’nin küresel AI yarışında rekabet gücünü artırmak ve dijital ekonomide lider konuma yükselmek için kritik bir yol haritası sunmaktadır (European Commission, 2020: 22b). Ayrıca, AB, AI alanında sınır ötesi veri paylaşımını

kolaylaştırmak ve dijital becerileri geliştirmek üzere çeşitli programlar yürütmektedir (Johnson & Smith, 2022: 78).

AB'nin AI politikaları, sadece teknolojik gelişmeyi desteklemekle kalmayıp aynı zamanda dijital hakların korunması, mahremiyetin sağlanması ve AI sosyal etkilerinin yönetilmesine odaklanmaktadır (Schmidt, 2021: 89). Bu çerçevede, AI'nın etik kullanımını güvence altına almak için GDPR gibi güçlü veri koruma düzenlemeleri de yürürlüktedir (European Parliament, 2018: 45a). GDPR ise, AB tarafından 2018 yılında yürürlüğe konmuş kapsamlı bir veri koruma ve gizlilik düzenlemesidir. Bu bağlamda, bireylerin kişisel verilerinin işlenmesini düzenleyerek, dijital çağda artan veri akışına karşı kullanıcıların haklarını güçlendirmeyi amaçlamaktadır. Bu tüzük, AB sınırları içinde faaliyet gösteren tüm kurum ve kuruluşların kişisel verileri nasıl topladığı, sakladığı ve kullandığı konusunda sıkı kurallar getirmektedir (European Parliament, 2018: 45b).

GDPR'nin temel amaçlarından biri, bireylere kişisel verileri üzerinde daha fazla kontrol sağlamaktır. Bu kapsamda, kullanıcılar verilerinin işlenmesine açıkça rıza verme hakkına sahiptir ve veri toplama süreçleri şeffaf olmalıdır. Ayrıca, bireyler istedikleri zaman verilerinin düzeltilmesini, silinmesini veya işlenmesinin kısıtlanmasını talep edebilirler. Kurumlar ise bu taleplere hızlı ve etkili biçimde yanıt vermekle yükümlüdür (European Commission, 2019: 23).

Tüzük, veri güvenliğini de ön planda tutarak; kişisel verilerin yetkisiz erişim, kayıp veya kötüye kullanım risklerine karşı korunması için teknik ve idari önlemler alınmasını zorunlu kılar. İhlal durumlarında ise veri sorumlularının belirli süreler içinde ilgili kurumları ve bireyleri bilgilendirmesi gerekmektedir (Wright & De Hert, 2020: 67).

Özellikle AI ve dijital teknolojilerin yaygınlaşmasıyla birlikte, GDPR'nin önemin daha da arttığı görülmektedir. Çünkü AI sistemleri büyük miktarda veri toplamakta ve analiz etmekte, bu da kişisel mahremiyet ve veri güvenliği açısından yeni riskler doğurmaktadır. GDPR, bu bağlamda AI uygulamalarının şeffaf, adil ve hukuka uygun olmasını sağlamaya yönelik güçlü bir çerçeve sunmaktadır (Binns, 2018: 112).

Böylece, GDPR öncülüğünde AB, sadece Avrupa’da değil, küresel ölçekte veri koruma standartlarının şekillenmesinde düzenleyici ve öncü bir üstlenerek dijital çağda birey haklarının korunması için önemli bir dayanak oluşturmaktadır (Kuner, 2017: 89). Aynı zamanda, teknolojinin insan odaklı, etik ve sürdürülebilir biçimde gelişmesini sağlamayı amaçlamaktadır (Floridi, 2020: 65). Bu yaklaşım, hem üye ülkelerin hem de küresel aktörlerin güvenli ve sorumlu AI kullanımı için önemli bir referans niteliğindedir (Brown & Müller, 2022: 53).

1.5.4 UNESCO

UNESCO (United Nations Educational, Scientific and Cultural Organization / Birleşmiş Milletler Eğitim, Bilim ve Kültür Örgütü), AI teknolojilerinin etik ve insan haklarına saygılı kullanımını sağlamak amacıyla küresel çapta önemli çalışmalar yürütmektedir. Dijital teknolojilerin hızla gelişmesi ve yaygınlaşmasıyla birlikte, UNESCO bu alanda etik standartların belirlenmesini ve devletler arası iş birliğinin artırılmasını hedeflemektedir (UNESCO, 2021: 7).

2021 yılında yayımlanan “Yapay Zeka için Etik İlkeler” belgesi, insan hakları, adalet, şeffaflık, sorumluluk, gizlilik ve kapsayıcılık gibi temel etik prensipleri ortaya koymaktadır. Bu ilkeler, AI sistemlerinin toplumsal hayata zarar vermeden, ayrımcılığa yol açmadan ve bireylerin mahremiyetini koruyarak kullanılmasını garanti altına almayı amaçlamaktadır (UNESCO, 2021: 15). Örneğin, ABD’de yüz tanıma teknolojilerinin ırksal önyargı yaratması gibi sorunlar, bu tür etik rehberlerin önemini ortaya koymaktadır (Garvie, Bedoya & Frankle, 2016: 23).

UNESCO, ayrıca AI’nın sosyal ve ekonomik eşitsizlikleri derinleştirebileceği endişesine dikkat çekmektedir. Özellikle gelişmekte olan ülkelerde dijital uçurumun kapanması ve AI teknolojilerine erişimin artırılması için eğitim ve kapasite geliştirme programları düzenlemektedir (Gasser & Almeida, 2017: 51). Örneğin, Afrika’da sürdürülebilir kalkınma için AI teknolojilerinin tarım ve sağlık alanında etik kullanımı üzerine pilot projeler yürütülmektedir (World Bank, 2022: 78).

Hali hazırda sistem içerisinde aktif olarak kullanılan projelerde yer almaktadır. Özellikle tarım alanında hastalık tespiti ve mahsul verimliliğini artırmak için geliştirilmiş uygulamalarla çiftçilere destek sağlanmaktadır. Kenya’da geliştirilen AI

tabanlı “PlantVillage Nuru” uygulaması, AI kullanarak yaprak hastalıklarını tespit etmekte ve çiftçilere erken müdahale imkânı sunmaktadır (Hughes et al., 2020). Sağlık sektöründe ise, özellikle Güney Afrika’daki bazı hastanelerde AI destekli tanı sistemleri kullanılmaya başlanmıştır. Bu teknolojiler, tüberküloz (TB / Tuberculosis) ve HIV (Human Immunodeficiency Virus / İnsan Bağışıklık Yetmezliği Virüsü) gibi yaygın ve ölümcül hastalıkların erken teşhisini önemli ölçüde hızlandırmakta ve tedavi süreçlerini iyileştirmektedir. Örneğin, KwaZulu-Natal Sağlık Departmanı ile Qure.ai işbirliğiyle yürütülen projede, AI destekli taşınabilir dijital röntgen cihazları sayesinde kırsal bölgelerde binlerce kişi taranmış ve erken dönemde TB vakaları tespit edilmiştir. Bu sayede, hem hastaların yaşam kalitesi artırılmış hem de hastalığın yayılması önlenmiştir (Qure.ai & KwaZulu-Natal Sağlık Departmanı, 2023).

UNESCO’nun bu çabaları, AI sistemlerinin sadece teknolojik bir mesele olmadığını, aynı zamanda kültürel ve toplumsal bir boyutu olduğunu vurgulamaktadır. Kuruluş, AI’nın insan onurunu koruması, kültürel çeşitliliğe saygı göstermesi ve kapsayıcı bir gelişim sağlaması gerektiğini belirtmektedir (Cath, 2018: 118). Örneğin, bazı ülkelerde yapay zeka sistemlerinin yerel diller ve kültürlerle uyumlu şekilde geliştirilmemesi, teknolojinin sosyal kabulünü zorlaştırmaktadır.

Bu bağlamda, UNESCO, AI alanında etik standartların küresel çapta benimsenmesi, insan haklarına saygı gösterilmesi ve sürdürülebilir kalkınmanın desteklenmesi için çalışmalarını yoğunlaştırmaktadır (Jobin, Ienca & Vayena, 2019: 312). Bu yaklaşım ileriye dönük olarak ise, teknolojinin hem fırsatlarını hem de risklerini dengeli bir şekilde yönetmeyi amaçlamaktadır.

1.6. Yapay Zeka Etiği, Veri Güvenliği ve Uluslararası Normlar

AI teknolojilerinin hızlı bir şekilde yaygınlaşması, veri güvenliği alanında hem önemli fırsatlar hem de karmaşık riskler ortaya çıkarmıştır. Bu teknolojiler, geniş veri ağlarını analiz ederek etkin karar alma ve tehdit tespiti yapabilme yeteneğine sahipken, aynı zamanda bu verilerin kötü niyetli kişilerce kötüye kullanılması veya siber saldırılara hedef olması ciddi güvenlik sorunlarına yol açmaktadır (Goodfellow, Bengio & Courville, 2016: 215). AI sistemlerinin özellikle aykırılık tespiti, saldırı öngörüsü ve

otomatik müdahale gibi alanlarda sağladığı avantajlar, kurumların siber tehditlere karşı daha proaktif ve etkili savunma mekanizmaları geliştirmesine imkân tanımaktadır.

Ancak, AI'nın veri alanındaki bu çift yönlü etkisi, riskleri de beraberinde getirmektedir. Özellikle kişisel verilerin hedef alınması durumunda, büyük ve karmaşık veri ağlarının saldırganlar tarafından kullanılması çok katmanlı güvenlik sorunları yaratmaktadır. Bu gerçeklik, kişisel verilerin korunmasına yönelik duyarlılığın artmasına ve bu alandaki düzenlemelerin öncelikli hale gelmesine neden olmuştur.

Veri güvenliğinin temel taşlarından biri, bireylerin veri sahipliği haklarını koruyan ve şeffaflık mekanizmalarını zorunlu kılan düzenlemelerdir. AB'nin kabul ettiği GDPR, veri işleme süreçlerinde şeffaflık ve hesap verebilirlik ilkelerini zorunlu kılarak, AI uygulamalarının etik sınırlar içinde kalmasını sağlamayı hedeflemektedir (Voigt & Von dem Bussche, 2017: 10-11). Ancak, AI algoritmalarının karmaşık yapısı ve karar verme süreçlerinin genellikle “kara kutu” olarak nitelendirilen gizlilik içinde gerçekleşmesi, bu düzenlemelerin etkin bir şekilde uygulanmasında önemli zorluklar doğurmaktadır (Doshi-Velez & Kim, 2017: 12).

Bu zorluklara fiziki örnekler vermek gerekirse, 2018 yılında Cambridge Analytica skandalına değinmek yanlış olmayacaktır. Bu olayda, Facebook kullanıcılarının kişisel verileri, siyasi reklam kampanyalarında hedefleme amaçlı olarak izinsiz kullanılmış ve AI destekli veri analizi yöntemleri ile kullanıcı profilleri oluşturulmuştur (Cadwalladr & Graham-Harrison, 2018: 3-5). Skandal, kişisel verilerin etik ve yasal sınırlar içinde korunmasının ne kadar hayati olduğunu göstermiş ve dünya çapında veri gizliliği yasalarının sıkılaştırılmasına yol açmıştır. Bu örnek, yapay zeka ve veri güvenliği alanında düzenleyici mekanizmaların geliştirilmesinin ve teknolojik şeffaflığın önemini açıkça ortaya koymaktadır.

Benzer şekilde, Facial recognition (yüz tanıma) teknolojilerinde etik tartışmalar giderek yoğunlaşmaktadır. Bu teknoloji, hem güvenlik hem de mahremiyet ihlalleri açısından tartışmalı bir konuma sahiptir. Yüz tanıma sistemlerinin hatalı eşleştirmeleri ve ırksal/etnik önyargıları tetiklemesi, ayrımcılığa yol açmakta ve insan hakları açısından ciddi endişeler yaratmaktadır (Garvie, Bedoya & Frankle, 2016: 23-26).

Ayrıca, bu teknolojilerin devletler veya özel aktörler tarafından izinsiz kullanımı, bireylerin mahremiyetine yönelik ihlalleri artırmaktadır.

AI'nın savaş alanında kullanımı da ciddi etik sorunları gündeme getirmektedir. Otonom silah sistemleri ve hedefleme algoritmaları, insan kontrolünün azalması nedeniyle sorumluluk ve hata paylarını tartışmaya açmıştır (Sharkey, 2019: 47-50). Bu durum, uluslararası hukuk normları ve etik ilkelerin yeniden değerlendirilmesini gerektirmektedir.

Bu tarz veri ihlalleri, AI'nın kişisel veriler üzerindeki etkisinden öte, siber güvenlik alanında da yeni ve karmaşık tehditlerin ortaya çıkmasına zemin hazırlamaktadır. AI teknolojilerinin siber güvenlikteki rolü hem koruyucu hem de tehdit oluşturu niteliktedir. Bir yandan, AI tabanlı sistemler ağ trafiğinde anormallik tespiti, saldırı önleme ve hızlı müdahale gibi alanlarda güvenliği artırmaktadır (Sommer & Paxson, 2010: 150-152). Öte yandan, siber saldırganlar giderek artan etkileriyle, AI tekniklerini kullanarak saldırı eylemlerini daha hedefe yönelik, karmaşık ve sistematik hale getirmekte, bu durum ise veri güvenliğini tehdit eden yeni saldırı biçimlerinin ortaya çıkmasına neden olmaktadır. Örneğin, özellikle günümüzde e-posta ve mesajlar aracılığıyla yapılan AI destekli oltalama (phishing) ve derin sahtekarlık (deepfake) saldırıları gün geçtikçe artış göstermektedir (Nguyen, Ngo & Park, 2020: 89-92).

AI destekli oltalama saldırıları, saldırganların e-posta, mesaj veya sosyal medya üzerinden hedeflerin güvenliğini kazanmak için otomatikleştirilmiş ve kişiselleştirilmiş içerikler oluşturduğu gelişmiş bir siber saldırı türüdür. Bu yöntem, geleneksel oltalamadan daha zor tespit edilir çünkü AI, hedefin davranışlarını ve iletişim tarzını analiz ederek daha inandırıcı tuzaklar kurar (Smith & Lee, 2022: 45). Ayrıca, AI sistemleri sayesinde saldırganlar milyonlarca potansiyel kurbanı hızlıca hedefleyebilmektedir (Johnson et al., 2023: 112). Bu durum, kurumların siber güvenlik önlemlerini güncel tutmasını zorunlu kılmaktadır.

Derin sahtekarlık ise, AI ve makine öğrenimi teknikleri kullanılarak gerçekçi ama sahte görüntü ve videoların üretilmesi sürecidir. Bu teknoloji, kişilerin sesini, yüzünü veya hareketlerini taklit ederek gerçekçi içerikler yaratır ve dezenformasyon yaymak için kullanılabilir (Kim et al., 2021: 88). Deepfake videolar, özellikle siyasi ve

sosyal manipölasyonlarda etkili bir araç haline gelmiş, toplumsal güveni zedeleyen yeni bir tehdit oluşturmuştur (Davis, 2022: 130). Bu nedenle, derin sahtekârlığın tespiti ve engellenmesi üzerine çalışmalar hızla artmaktadır.

AI modellerinin eğitildiği veri bütünlüğünün kalitesi, hem model performansını hem de güvenlik düzeyini doğrudan etkilemektedir. Veri setlerinde yer alan önyargılar veya hatalı bilgiler, AI'ın yanlış kararlar almasına ve ayrımcı sonuçlar üretmesine sebep olabilir; bu da veri güvenliği ve etik açıdan önemli riskler taşımaktadır (Barocas & Selbst, 2016: 143-147). Bu nedenle veri güvenliği politikaları, yalnızca veri korumasına değil, aynı zamanda veri kalitesinin ve model şeffaflığının artırılmasına odaklanmalıdır.

Büyük veri ve AI destekli sistemlerin politik süreçlerde, özellikle kritik kararlarında etkisi giderek artmaktadır. Bu durum, veri güvenliğinin önemini daha da ön plana çıkarmaktadır. Veri güvenliğinde yaşanan eksiklikler ve belirsizlikler, siyasi manipölasyon riskini artırmakta ve halkın demokratik süreçlere olan güvenini olumsuz yönde etkilemektedir (Tufekci, 2018: 200-204). Dolayısıyla, AI sistemlerinde güvenlik ve gizlilik standartlarının geliştirilmesi, teknoloji kullanımının sürdürülebilirliği için kritik bir gerekliliktir.

1.7. Gözetim Kapitalizmi ve Algoritmik Tahakküm

Gözetim kapitalizmi, kapitalizmin tarihsel evrimi içinde ortaya çıkmış ve toplumsal yaşamın çeşitli alanlarında köklü dönüşümlere yol açmıştır. Bu kavramı kapsamlı bir şekilde değerlendirebilmek için, öncelikle kapitalizmin temel dinamiklerine ve teknolojik gelişmelerin bu sistem üzerindeki etkilerine değinmek gerekmektedir.

Kapitalizm, özel mülkiyet ve serbest piyasa ilkelerine dayanan; üretim araçlarının bireyler ve özel şirketler tarafından kontrol edildiği bir ekonomik sistemdir. Bu sistem, Avrupa'da Rönesans dönemiyle birlikte gelişmeye başlamış, 16. yüzyıldan itibaren feodalizmin çözülmesi ve Sanayi Devrimi'nin etkisiyle önemli bir ivme kazanmıştır. Sanayi Devrimi, üretimi mekanize ederek daha büyük ölçekli üretim ve ticaret faaliyetlerini mümkün kılmıştır (Hobsbawm, 1994: 45). Üretimin merkezi fabrikalarda yoğunlaşması, iş gücünün organize edilmesini ve bu sürecin denetimini gerekli kılmış; bu da gözetim uygulamalarının yaygınlaşmasına zemin hazırlamıştır.

Bu bağlamda, Adam Smith'in *Ulusların Zenginliği* adlı eseri, serbest piyasa mekanizmasının işleyişini açıklarken, bireylerin kendi menfaatlerini takip ederken, görünmez bir el aracılığıyla topluma da dolaylı olarak hizmet ettiklerini savunmuştur (Liberus Yayınevi, 2020: 14). Buna karşılık, Marx'a göre kapitalist üretim sürecinde teknoloji, hem işgücünü sömürü aracına dönüştürmekte hem de toplumsal ve bireysel özgürleşme için potansiyel alanlar açmaktadır (Hardt & Negri, 1994: 10, 21; Hardt & Negri, 2000: 29–30, 364–369; Negri, 1991, s. 139–150, aktaran: Chandler & Fuchs, 2017: 215).

Kapitalist sistem, kâr oranlarını artırma ve ekonomik büyümeyi sürdürme amacıyla sürekli birikim ve yeniden üretim süreçlerini beraberinde getirir (Buğra, 2005: 16). Bu süreçler, zamanla finansal kapitalizmin gelişimini tetiklemiş ve neoliberal politikaların etkisiyle devletin ekonomik müdahaleleri sınırlandırılarak piyasa mekanizmaları ön plana çıkarılmıştır. Bu dönüşüm, şirketlerin tüketici verilerine erişimini kolaylaştırmış ve veri temelli stratejiler geliştirmelerine olanak tanımıştır. Bu bağlamda bireyler, yalnızca emek gücü olarak değil, aynı zamanda veri sağlayıcı tüketiciler olarak değerlendirilir hale gelmiştir.

Bu noktada teknolojinin belirleyici rolü öne çıkmaktadır. Dijitalleşme ve internet teknolojilerinin yaygınlaşması, veriye dayalı ekonomi modelinin doğuşunu hızlandırmıştır. Özellikle Google, Facebook ve Amazon gibi şirketler, klasik kapitalizmden farklılaşarak bireylerin dijital ortamda bıraktıkları izleri toplayıp analiz ederek, bu veriler üzerinden ekonomik değer üretmektedir. Bu faaliyetler, dijitalleşen üretim süreçleri ve büyük veri teknolojilerinin katkısıyla daha da karmaşık bir yapıya bürünmüş ve “gözetim kapitalizmi” olarak adlandırılan yeni bir ekonomik modeli ortaya çıkarmıştır.

Gözetim kapitalizmi kavramı, özellikle Shoshana Zuboff'un *The Age of Surveillance Capitalism* (Gözetim Kapitalizi Çağı, 2019) adlı çalışması ile akademik literatüre kazandırılmıştır. Zuboff, bu modelin, kullanıcıların çevrimiçi davranışlarını, tercihlerini ve etkileşimlerini analiz ederek kar amacı güden stratejilere dönüştürüldüğünü belirtmektedir (Zuboff, 2019: 93 - 97). Elde edilen veriler, hedeflenmiş reklamların yanı sıra üçüncü taraflarla da paylaşılmakta, bu durum mahremiyetin giderek daha fazla ihlal edilmesine yol açmaktadır. Bu bağlamda,

teknoloji devlerinin toplum üzerindeki denetleyici etkisinin giderek daha belirgin hâle geldiği ve bu durumun bireylerin karar alma süreçlerine müdahale ederek bireysel irade gücünü zayıflattığı görülmektedir. Bu süreç, yeni bir egemenlik alanının oluşmasına zemin hazırlamaktadır. Böylece gözetim kapitalizmi, yalnızca ekonomik bir sistem olmaktan çıkarak, toplumsal ilişkiler ve siyasal yapılar üzerinde de köklü bir dönüşüm yaratma kapasitesine sahip bir güç olarak ortaya çıkmaktadır.

AI ve algoritmalar, bu modelin temelini oluşturan teknolojik araçlardır. Gözetim kapitalizmi, yalnızca ekonomik değil, aynı zamanda politik bir yapıya da dönüşerek küresel bir norm halini almıştır. Bu bağlamda, Google, Meta (eski adıyla Facebook) ve Amazon gibi şirketler, dünya genelinde geniş veri ağlarına sahip olmaları sayesinde dijital hegemonyalarını pekiştirmektedir. Bu dönüşüm, geleneksel iş modellerinin yerini veri odaklı stratejilere bırakmasına neden olmuştur. Günümüzde veri, artık yalnızca bir yan ürün değil, ekonomik değeri yüksek birincil kaynak olarak kabul edilmektedir. Bu verilerin analiz edilmesiyle kullanıcı davranışlarının tahmin edilmesi, şirketlerin kârlarını artırmalarına olanak tanımaktadır (Zuboff, 2019: 101).

Gözetim kapitalizminin etkileri yalnızca ekonomik alanla sınırlı değildir. Büyük teknoloji şirketleri, veri toplama yoluyla elde ettikleri güç sayesinde sosyal ve politik etkilerini de artırmaktadır. Bunun yanında, bazı devletler dijital gözetimi kapsamlı sosyal kontrol mekanizmalarına dönüştürmektedir. Çin'in sosyal kredi sistemi, vatandaşların sosyal ve ekonomik davranışlarını dijital verilerle izleyip puanlayarak bireylerin erişim haklarını düzenlemekte ve böylece gözetim kapitalizminin devlet destekli bir formunu ortaya koymaktadır (Creemers, 2018: 112-115). Bu sistem, dijital gözetim mekanizmalarının sosyal davranışları şekillendirmek ve siyasi otoriteyi pekiştirmek için nasıl kullanıldığını göstermektedir. Bireylerin sosyal normlara uyum sağlaması amacıyla kişisel verilerin devlet tarafından izlenmesi ve değerlendirilmesine dayanmakta olup, mahremiyet ve bireysel özgürlükler açısından ciddi tartışmalara yol açmaktadır (Liang, Das, Kostyuk & Hussain, 2018: 9-12). Couldry ve Mejias (2018), dijital kapitalizmin eşitsizlikleri derinleştirdiğini ve verilerin şirketler ile devletler tarafından kontrol edilmesinin toplumsal adaleti tehdit ettiğini savunmaktadır. Gelişmekte olan ülkelerde, yerel dijital altyapıların yetersizliğinden faydalanan şirketler, bireylerin dijital bağımsızlığını zayıflatacak şekilde veri toplamaktadır. Bu bağlamda,

veri kolonizasyonu sadece emek sömürsü değil, sosyal yaşamın veri için kapitalist bir kaynağa dönüştürülmesi sürecidir.

Couldry ve Mejias (2019: 4), bu durumu “veri sömürgeciliği” olarak tanımlar ve büyük teknoloji şirketlerinin özellikle Küresel Güney’deki dijital eşitsizlikleri artırdığını vurgular. Dijital gözetim sistemleri yalnızca ekonomik ilişkileri değil, aynı zamanda toplumsal normları da yeniden şekillendirmektedir. O’Neil (2016: 132) ise, algoritmalar aracılığıyla yapılan içerik önerileri ve reklamlar, bireylerin siyasi tutumlarını ve toplumsal görüşlerini etkileyebilir hale geldiğini belirtmektedir. Bu bağlamda, Facebook’un Cambridge Analytica skandalı, gözetim kapitalizminin demokratik süreçlere nasıl müdahale edebildiğini göstermesi açısından önemli bir örnektir. Skandal, Brexit ve ABD başkanlık seçimleri gibi gündemde olan siyasi olaylarda kullanıcı verilerinin manipülasyon aracı olarak kullanıldığını ortaya koymuştur. Bu durum, internetin ilk aşamada bilgi paylaşımı amacıyla geliştirildiği ancak zaman içinde özne kullanıcı verilerinin ticari bir malzeme haline dönüştüğüne dair eleştirileri çoğaltmaktadır.

Dijital gözetimin bireylerin mahremiyetini zayıflatıldığını ve algoritmalar aracılığıyla ayrımcılığa dayalı denetimlerin arttığını belirtmektedir. Buradan hareketle, özellikle bireysel haklar ve özgürlüklerin geleceği açısından ciddi tehditler oluşturmaktadır (Lyon, 2018: 77), Diğer yandan, son dönem çalışmalar tüketicilerin çevrimiçi davranışsal reklamlara yönelik tutumlarını ve bu tutumların gözetim algısıyla nasıl şekillendiğini incelemiştir. “Çevrimiçi Davranışsal Reklama Yönelik Tutumun Tüketici Sinizmine Etkisinde Gözetim Algısının Aracılık Rolü” (Demir Demiralp & Tosun, 2025: 325-330) adlı çalışma, gözetim algısının arttıkça tüketicilerin reklamcılığa karşı daha şüpheci ve sinik bir tutum geliştirdiğini ortaya koyarak, gözetim kapitalizmi süreçlerinin psikolojik ve sosyokültürel boyutlarını gözler önüne sermektedir. Bu durum, veri odaklı reklam stratejilerinin yalnızca ekonomik değil, aynı zamanda tüketici davranışları açısından da karmaşık sonuçlar doğurduğunu göstermektedir.

Bu doğrultuda, Gözetim kapitalizmi, bireylerin dijital verilerinin ticari metaya dönüştüğü bir ekonomik sistem olarak dijital çağın belirleyici güçlerinden biri haline gelmiştir. Bu süreç, özellikle 1990’ların sonlarında internetin yaygınlaşmasıyla başlamış, 2000’li yıllarda reklamcılık sektörünün evrilmesiyle derinleşmiştir. Ancak

esas kırılma noktası, AI ve algoritmaların gelişmesiyle yaşanmıştır. Bu model, veri toplama, kullanıcı davranışlarını tahmin etme, verilerin satışı ve demokratik süreçlere müdahale gibi çok katmanlı etkiler üretmektedir (Zuboff, 2019: 20-24). Gözetim kapitalizmi yalnızca ekonomik değil, aynı zamanda toplumsal ve siyasal yapıları da şekillendiren bir güç haline gelmiştir. Teknolojik kapasitesi sınırlı olan ülkeler bu süreçte daha kırılgan hale gelirken, dijital altyapıya hâkim devletler için mahremiyet ve veri haklarının korunması ciddi bir ikilem oluşturmaktadır.

Aynı zamanda, gözetim kapitalizminin oluşumu, teknoloji devlerinin sadece ekonomik değil, aynı zamanda siyasi karar alma süreçlerinde de belirleyici aktörler haline gelmesine yol açmaktadır. Nick Couldry ve Ulises Mejías, (2019: 7)’ın da ifade ettiği gibi, bu durum devletlerin egemenlik yapısını dönüştürerek ve yeni bir küresel güç dengesi yaratmaktadır.

ÜÇÜNCÜ BÖLÜM

BREXIT SÜRECİNDE YAPAY ZEKA VE AKILLI ALGORİTMALARIN ROLÜ

1. BREXİT'İN SİYASAL VE TOPLUMSAL ARKA PLANI

Brexit, Birleşik Krallık'ın AB'nden ayrılma süreci olarak tanımlanır. Bu süreç uluslararası ilişkilerde önemli bir dönüm noktası olmakla kalmamış, aynı zamanda ülke içindeki siyasal ve toplumsal dinamiklerin derinleştiği bir zemini de açığa çıkarmıştır. 23 Haziran 2016 tarihinde gerçekleştirilen referandumda, seçmenlerin %51,9'u Birleşik Krallık'ın AB'den ayrılması yönünde oy kullanmıştır; kalan %48,1'lik kesim ise birlik içinde kalınmasını desteklemiştir (Electoral Commission, 2016). Bu sonuç, AB karşıtlığı, göçmenlik kaygıları ve ekonomik belirsizliklerin birleştiği karmaşık bir siyasal-toplumsal ortam içerisinde yer bulmuştur.

Birleşik Krallık içinde AB'nin karar alma süreçlerinde doğrudan etkili olamama düşüncesi zamanla belirginliğini göstermiştir. Bunun temel nedenlerinden biri, Birleşik Krallık'ın AB içindeki oy ağırlığının sınırlı olması ve bazı kritik kararların diğer büyük devletlerle birlikte ya da çoğunluk oyu ile alınmasıdır (Curtice, 2017: 113). Bu durum, ülkenin kendi çıkarlarına uygun olmayan politikaların dayatılabileceği endişesini gün yüzüne çıkartmıştır. Ayrıca, AB kurumlarının çıkardığı yasaların ulusal parlamentonun yasama yetkisini sınırladığı ve Birleşik Krallık'ın iç hukukunu tam anlamıyla kontrol edemediği düşünülmüştür (Curtice, 2017: 112). AB'nin ortak politikaları ve düzenlemeleri, özellikle ticaret, göç ve çevre gibi alanlarda ülkenin bağımsız karar alma kapasitesini azalttığı yönünde eleştiriler mevcuttu (Menon & Salter, 2016: 94). Bu nedenle, birçok seçmen ve siyasal aktör, ulusal egemenliği geri kazanmanın ancak AB'den ayrılarak mümkün olacağı görüşünü benimsemiştir (Clarke, Goodwin & Whiteley, 2017: 47).

Bu bağlamda referandumun temel çıkış noktalarından biri, özellikle egemenlik ve ulusal kimlik meseleleridir. Özellikle AB'nin karar alma mekanizmalarının, ülkenin kendi yasama yetkilerini sınırladığı düşüncesinden hareketle “Kontrolü geri almak” söylemi, bu bağlamda hem siyasal aktörler hem de seçmenler arasında güçlü bir

motivasyon kaynağı olmuştur (Clarke, Goodwin & Whiteley, 2017: 45). Bu bağlamda AB karşıtlığı, sadece ekonomik ya da hukuki nedenlere değil, aynı zamanda kültürel kimlik ve milliyetçilikle de ilişkilendirilmiştir.

Diğer önemli bir faktör ise göçmen karşıtlığıdır. 2004 yılından sonra Orta ve Doğu Avrupa ülkelerinden başlayan göç dalgası, iş gücü piyasasında ve sosyal hizmetlerde yoğun rekabet algısını artırmıştır. Bu durum, özellikle de sanayileşmenin gerilediği ve ekonomik sıkıntıların derinleştiği kuzey İngiltere gibi bölgelerde yaşayan, daha düşük gelirli işçi sınıfı üzerinde etkili olmuştur (Evans & Mellon, 2019: 88). “Leave” kampanyalarının kullandığı “Breaking Point” gibi görsel ve etkili ifade stratejileri, göçmenlerin ekonomik ve sosyal kaynakları tükettiği algısını güçlendirmiştir (Kaufmann, 2018: 29). Bu söylemler, göçmenlik karşıtlığını sadece ekonomik değil, aynı zamanda kültürel bir tehdit olarak da çerçevelemiştir.

Zamanla etkisini derinleştiren ekonomik kaygılar, Brexit kararının bir diğer temel boyutunu oluşturmuştur. Özellikle de henüz tam olarak endüstrileşmemiş bölgelerde yaşayan bireyler, küreselleşmenin getirdiği ekonomik dönüşümden olumsuz etkilenmiş ve kendilerini sistemin dışında kalmış hissetmişlerdir. İşsizlik, düşük ücretler ve azalan sosyal hizmetler, bu kesimlerin AB’ye olan güvenini sarsmış ve Brexit’i bir “kurtuluş” seçeneği olarak görmelerine yol açmıştır (Rodrik, 2018: 76; Goodwin & Heath, 2016: 78).

Bu ekonomik ayrışma, aynı zamanda bölgesel farklılıkları da derinleştirmiştir. Finans, hizmet sektörü ve uluslararası ticaret açısından ülkenin en önemli merkezleri olan Londra ve güneydoğu metropolleri, özellikle küresel finansın merkezi olarak AB pazarına erişim ve serbest dolaşımın sağladığı avantajlardan yoğun şekilde yararlanmıştır. Üyelik, sermaye akışını kolaylaştırmış, yatırımcı güvenliğini artırmış ve iş dünyasının küresel rekabet gücünü güçlendirmiştir. Bu nedenle, söz konusu bölgeler AB ile daha entegre ve ekonomik olarak güçlü bir profil sergilerken, kuzey ve doğu bölgeleri ise kaynak yetersizliği, ekonomik gerileme ve temel haklarının paylaşılması konusundaki endişeler nedeniyle daha fazla “Leave” oyuna yönelmiştir (Clarke et al., 2017: 53, Ford & Goodwin, 2014: 130).

Siyasal aktörler açısından bakıldığında, Brexit sürecinde özellikle iki parti ön plana çıkmıştır. Nigel Farage liderliğindeki Birleşik Krallık Bağımsızlık Partisi (UKIP / UK Independence Party), göçmen karşıtlığı ve AB eleştirisi üzerine inşa ettiği popülist söylemiyle referandumda önemli bir etki yaratmıştır (Ford & Goodwin, 2014: 142). Muhafazakâr Parti içinde ise, özellikle Avrupa Araştırma Grubu (ERG) adlı fraksiyon, AB karşıtı söylemi güçlendirmiş; Boris Johnson ve Michael Gove gibi isimler, “Vote Leave” kampanyasının yüzü olmuş ve kamuoyuna ekonomik faydalar vaat ederek desteği artırmışlardır (Shipman, 2016: 157).

Toplumsal bağlamda ise Brexit, yaş, eğitim ve bölgesel farklılıklar temelinde bir bölünmeyi de beraberinde getirmiştir. Genç ve yüksek eğitimli kesimler büyük ölçüde AB’de kalma yönünde oy verirken, yaşlı ve daha düşük eğitim düzeyine sahip gruplar ayrılmayı tercih etmiştir (Goodwin & Heath, 2016: 82). Benzer şekilde, metropolitan alanlar ve İskoçya gibi daha kozmopolit bölgeler Remain kampanyasını desteklerken, işçi sınıfının yoğun olduğu kuzey bölgeleri ve kırsal alanlar “Leave” oylarıyla öne çıkmıştır (Ford & Goodwin, 2014: 130).

Remain kampanyası, AB üyeliğinin ekonomik entegrasyon, yatırım çekme ve iş piyasasında istikrar sağlama gibi avantajlarına vurgu yaparak, özellikle eğitim seviyesi yüksek ve kentli seçmenler arasında destek bulmuştur (Goodwin & Heath, 2016: 80). Öte yandan, Leave kampanyası, yerel kontrolün yeniden kazanılması ve göçmen sayısının sınırlandırılması üzerine yoğunlaşmıştır. Sanayileşmenin gerilediği ve ekonomik sıkıntıların yaşandığı kuzey bölgeleri ve kırsal alanlarda yaşayan işçi sınıfı, küreselleşmenin getirdiği dönüşümlerin olumsuz etkilerini deneyimlemiş ve AB üyeliğini kendi ekonomik güvencesizliklerinin kaynağı olarak görmüştür (Evans & Mellon, 2019: 90).

Leave kampanyasının kullandığı söylemler, bu kesimlerin iş kaybı ve sosyal değişim endişelerini hedeflemiş ve böylece bu toplumsal katmanlarda güçlü destek bulmuştur (Kaufmann, 2018: 37). Bu bölünme, sadece siyasi tercihlerde değil, aynı zamanda toplumsal kimlik, değerler ve gelecek beklentilerinde de derin ve kalıcı farklılıklara yol açmıştır (Menon, 2016: 102).

Genel olarak değerlendirildiğinde, Brexit'in temelinde yatan siyasal ve toplumsal dinamikler, sadece teknolojik gelişmelerle açıklanamayacak kadar karmaşık ve çok boyutludur. Referandumun zemininde, ulusal egemenlik hassasiyetleri, ekonomik eşitsizlikler ve kültürel kimlik tartışmaları gibi birden fazla katmanın iç içe geçtiği görülmektedir. Bu bağlamda Brexit, küreselleşmeye karşıt hareketlerin ve yerel-toplumsal meselelerin uluslararası sistem dinamiklerine yansımalarının çarpıcı bir örneğini teşkil etmektedir (Rodrik, 2018: 88).

1.1. Medya ve Kültürel Temsiller: Belgeseller, Edebiyat, Algı Yönetimi

Toplumsal kararların şekillenmesinde yalnızca ekonomik ya da siyasi gerçeklikler değil, bu gerçekliklerin medya aracılığıyla nasıl sunulduğu da belirleyici bir rol oynamaktadır. Özellikle dijitalleşme çağında, bilgi akışının hızı, içeriğin güvenilirliğinden çoğu zaman daha öncelikli hâle gelmiş ve bu durum “gerçek sonrası” (post-truth) çağın temel özelliklerinden biri olarak tanımlanmıştır (McIntyre, 2018: 10). Seçmen davranışlarının, bireysel deneyimlerden çok dijital içeriklerle biçimlenen algılar üzerinden oluşması, demokratik karar alma süreçlerinin doğasına dair yeni tartışmaları gündeme getirmiştir (Sunstein, 2017: 45 - 53). Bu bilgilerden hareketle, medya içerisinde barındırdığı ve beslediği edebiyat, belgeseller ve kurgulanmış filmler ile birlikte hızla gelişen yayın hayatına entegre etmektedir.

Bu noktada karşımıza popüler kültür kavramı ve etkisi çıkmaktadır. Popüler kültür, bir toplumsal olayın halk nezdindeki algısını ve anlamlandırılmasını etkileyen güçlü bir mecradır. Brexit gibi siyasal kırılmalar, filmler, tiyatro eserleri ve medya içeriklerinde temsil edilerek kolektif hafızayı şekillendirir (Archer, 2021: 24). Ayrıca kültürel ürünler, politik söylemlerin dramatize edilip kişisel ve toplumsal düzleme taşınmasına aracılık eder (Cloarec, 2021: 6). Bu tür yapımlar, Brexit'in nedenleri, etkileri ve sosyal bölünmelere dair zihin haritaları oluşturur. Brexit özelinde hazırlanan “Brexit: The Uncivil War” ve “The Great Hack” adındaki iki önemli belgesel bu dinamiği analiz etmede kilit bir öneme sahiptir.

Brexit referandumu, yalnızca AB'den ayrılma sürecini başlatmamış, aynı zamanda demokratik katılım, siyasal iletişim ve algı yönetimi gibi alanlarda da köklü sorgulamaları gündeme getirmiştir. Bu sürecin karmaşıklığını anlamak için yalnızca

siyasal açıklamalar yeterli değildir; aynı zamanda bu olayların kültürel temsilleri ve medya aracılığıyla yeniden üretimi de incelenmelidir. Brexit: The Uncivil War (2019) belgeseli, Birleşik Krallık'ın AB'den ayrılma sürecini ve özellikle 2016 referandumunu merkeze alarak, siyasi kampanyaların ve dijital stratejilerin nasıl yürütüldüğünü derinlemesine incelemektedir (Brexit: The Uncivil War, 2019). Bu bağlamda, Channel 4 yapımı olan Brexit: The Uncivil War (2019) adlı belgesel film, referandum sürecinin perde arkasını ele alarak, siyasi kampanyaların nasıl yürütüldüğünü, veri analitiği ve hedefli iletişimin ne ölçüde belirleyici olduğunu gözler önüne serer (Graham, 2019: 12). Film, belgesel ve dram öğelerini harmanlayarak, post-truth çağında siyasetin nasıl şekillendiğine dair güçlü bir anlatı ortaya koyar.

James Graham tarafından kaleme alınan ve Toby Haynes tarafından yönetilen bu dramatize yapım, özellikle Vote Leave kampanyasının stratejik liderlerinden Dominic Cummings karakterine odaklanır. Benedict Cumberbatch'ın Cummings'i canlandığı film, referandum kampanyasının nasıl “veri odaklı”, duygusal ve manipülatif bir zeminde yürütüldüğünü göstermeyi amaçlar. Kampanya, yalnızca siyasi mesajları değil, seçmen davranışlarını da veri yoluyla modelleyerek, mikrotargeting (mikro hedefleme) teknikleri ile şekillendirilmiştir (Sadd, 2019: 43). Filmde “Take Back Control” sloganının, seçmenlerin bilinçaltına işlenen ülke üzerindeki hakların kontrolü ve bir kurtuluş vaadi olarak işlendiği ve bunun ekonomik ya da siyasi gerçeklerden çok, İngiliz toplumundan farklı algıya sahip olan kişiler ile gerçekleşen hâkimiyet yarışı gibi bir kültürel aidiyet ve kimlik kaygılarına hitap ettiği açıkça görülmektedir (Cloarec, 2021: 6).

Belgeselin temel amacı, Brexit sürecine dair kamuoyunda oluşmuş “basitleştirilmiş” anlatıların ötesine geçerek, kampanya stratejilerinin etik, teknolojik ve psikolojik boyutlarını görünür kılmaktır. Bu bağlamda Graham, filmin ideolojik bir anlatı değil, süreçleri soğukkanlılıkla analiz eden bir “politik portre” olduğunu vurgular (Graham, 2019: 14). Özellikle Cummings karakteri, ne kahraman ne de kötü adam olarak sunulur; aksine, modern siyasetin tekinsizliği içinde, kendi doğrularıyla hareket eden bir stratejist olarak resmedilir. Bu anlatım biçimi, izleyiciyi yalnızca bilgilendirmez; aynı zamanda düşünsel bir tartışmaya da davet eder.

“Brexit: The Uncivil War”, aynı zamanda algı yönetimi ve post-truth kavramlarının görsel anlatımla harmanlandığı nadir yapımlardan biridir. Filmde, seçmenlere doğruları sunmak yerine, onların duygularına hitap eden hikâyeler anlatmak tercih edilir. Bu durum, bilgi çağında gerçeğin yerini inançların ve hissiyatların almasının bir yansımasıdır (Perkins, 2019: 44). Seçmen davranışının rasyonellikten çok, duygusal güvenlik arayışlarıyla belirlendiği, özellikle göçmen karşıtlığı, ekonomik korkular ve ulusal egemenlik vurgusu üzerinden yansıtılmıştır. Belgesel, bu süreçte teknolojik araçların (özellikle Facebook ve veri analiz firmalarının) nasıl siyasi propaganda aracı haline geldiğini etkili bir şekilde gösterir (Suada et al., 2024: 106).

Bu belgesel ayrıca, kampanyaların hedef kitlelerini nasıl ayırttığını ve “kararsız seçmenleri” manipüle etmek için nasıl algoritmik yöntemlere başvurduğunu gözler önüne serer. Özellikle, kullanıcıların çevrimiçi davranışlarının izlenmesi ve buna göre kişiselleştirilmiş mesajların gönderilmesi, seçim sürecinin adil olup olmadığına dair etik soruları da beraberinde getirmiştir (Sadd, 2019: 45). Filmde, Cambridge Analytica’ya yapılan göndermeler dolaylı olsa da, veri firmalarının Brexit sürecinde oynadığı rolü ima eden sahneler, dijital gözetimin demokrasi üzerindeki etkilerine dair ciddi bir uyarı niteliğindedir.

Bir diğer önemli medya içeriği ise “The Great Hack” belgeseli olarak dikkatleri üzerine çekmektedir. The Great Hack (2019) belgeseli, dijital veri gizliliği, sosyal medya manipülasyonu ve demokrasi arasındaki karmaşık ilişkiyi derinlemesine irdeleyen önemli bir yapımdır. Yönetmenliğini Karim Amer ve Jehane Noujaim’in üstlendiği bu film, Cambridge Analytica skandalı üzerinden, kişisel verilerin siyasi amaçlarla nasıl toplandığını ve kullanıldığını gözler önüne serer (The Great Hack, 2019, 00:12:45). Belgesel, özellikle 2016 ABD başkanlık seçimleri ve Brexit referandumu gibi önemli siyasi süreçlerde, dijital algoritmaların seçmen davranışlarını nasıl şekillendirdiğine dair kapsamlı bir analiz sunar.

Teknolojik gelişmelerin siyasal iletişimdeki etkileri yanı sıra, veri ve medya kontrolünün modern siyaset için kritik hale gelmektedir (Epstein, 2001: 42). Bu perspektif, The Great Hack’in temel çıkarımlarını destekler niteliktedir; çünkü belgesel, veri toplama yöntemlerinin sadece teknik bir mesele olmadığını, aynı zamanda

demokratik deęerler ve bireysel özgürlükler açısından da ciddi sorunlar yarattığını ortaya koyar.

Belgeselde, Cambridge Analytica'nın sosyal medya kullanıcılarının çevrimiçi davranışlarını analiz ederek, seçmenlerin psikolojik profillerini çıkarıp, bu veriler ışığında kişiselleştirilmiş ve manipülatif mesajlar geliştirdiğı detaylı biçimde gösterilir (The Great Hack, 2019, 01:02:30). Bu mikro hedefleme uygulaması, sadece siyasi tercihler üzerinde deęil, aynı zamanda bireylerin gerçeklik algısı ve duygusal tepkileri üzerinde de derin etkiler bırakır. Algoritmalar aracılığıyla bilgi akışının kontrol edilmesi, post-truth siyasetin yükselişini destekleyen bir mekanizma olarak işlev görmektedir (Tüfekçi, 2015: 34).

Ayrıca belgesel, dijital gözetim ve veri ekonomisinin etik boyutlarına dikkat çeker. Bu bağlamda, sosyal medya platformlarının, veri tabanlı manipölasyonun ötesinde, demokratik süreçlerin güvenilirliğini zedeleyen bir “yönetim üçgeni” içinde yer aldığı savunulmaktadır (Gorwa, 2019: 90). The Great Hack'te bu durum, kullanıcıların verilerinin izinsiz ve şeffaf olmayan biçimde kullanılmasıyla ortaya çıkar; bu da bireylerin seçim özgürlüklerini tehlikeye atar (The Great Hack, 2019, 01:25:10).

Film, dijital çağda siyasal iletişimin sadece mesajların iletilmesi deęil, aynı zamanda bireylerin psikolojik ve davranışsal yönlerinin hedeflenmesi anlamına geldiğini gösterir. Bu bağlamda, dijital veri kullanımı hem bireysel mahremiyetin hem de demokratik katılımın önünde önemli bir engel haline gelmiştir. The Great Hack, böylece veri ekonomisinin ve sosyal medya algoritmalarının siyasal süreçler üzerindeki etkisini görünür kılarak, günümüz demokrasilerinde bilgi, iktidar ve etik arasındaki hassas dengeleri sorgulayan güçlü bir anlatı sunar. Bu anlatı, izleyiciyi sadece teknolojinin sunduğı olanakları deęil, aynı zamanda bu olanakların kötüye kullanımını da fark etmeye çağırır (Zuboff, 2019: 114).

Bu süreç kendisine sadece belgesellerde yer bulmamıştır. Toplumun kültürel hafızasında ve günlük yaşamında yarattığı sarsıntılarla birlikte kendisine dijital ortam, edebiyat ve tiyatro sahnelerinde de deęerlendirilmesi gereken çok katmanlı bir dönüşüm olarak yer bulmuştur.

Çağdaş İngiliz edebiyatı, Brexit sonrası ortaya çıkan kimlik krizini, göçmen karşıtlığını, ulusal aidiyet duygusunu ve toplumsal bölünmeleri hem tanıklık ederek hem de eleştirel bir bakış açısıyla ele almıştır. Hall (2020: 88) bu dönemin roman ve öykülerinin yalnızca siyasi bir tepki olmadığını, aynı zamanda toplumun duygusal ve düşünsel çalkantılarını yansıttığını vurgulamaktadır. Bireysel düzeyde yaşanan belirsizliklerin kararsızlıkla iç içe geçtiği bu eserler, toplumsal kimlik krizini görünür kılmakta; bu kırılma yalnızca kültürel nostalji ya da ekonomik endişe ekseninde değil, geçmişle kurulan ilişki ve gelecek kaygılarıyla da şekillenmektedir.

Bu temaları somutlaştıran ilk örnek, Ali Smith'in "*Autumn*" (2016) adlı romanı, referandumdan sadece birkaç ay sonra yazılan bu roman, Brexit sürecini doğrudan siyasi tartışmalar üzerinden değil, zaman ve duygu ekseninde, yaşam biçimi ve kimlik sorgulamaları aracılığıyla ele alır. Romandaki Elisabeth karakteri, İngiliz vatandaşlığını ve aidiyetini simgeleyen yenilenen pasaport işlemleri sırasında karşılaştığı karmaşık ve bürokratik engellerle yüzleşir. Pasaport yenileme sürecinde yaşadığı zorluklar, sadece resmi kimlik belgelerinin alınmasında bürokrasinin yarattığı güçlükleri değil, aynı zamanda Brexit sonrası İngiltere'de vatandaşlık ve aidiyet kavramlarının ne denli karmaşık ve tartışmalı hale geldiğini de simgeler. Bu deneyim, Elisabeth'in "kimin sesi daha fazla duyuluyor?" sorusunu derinlemesine düşünmesine yol açar ve bireylerin kimliklerini resmileştirme sürecindeki güçlükler, Brexit'in yarattığı toplumsal bölünmelerin ve aidiyet krizlerinin metaforu olarak roman boyunca işlenir (Smith, 2016: 45).

Benzer şekilde, Jonathan Coe'nin "*Middle England*" (2018) adlı romanı, İngiliz orta sınıfın Brexit sonrası ruh hâlini yansıtarak Midlands ile Londra arasındaki toplumsal kutuplaşmayı, aile içi ayrışmaları ve kuşaklar arası ideolojik çatışmaları ele alır (Coe, 2018: 123). Boyne ve diğer araştırmacılar, bu romanı "Brexit" in özüne nüfuz etmeyi başaran bir eser olarak tanımlar.

Benzer bir biçimde tiyatro da Brexit'in etkilerini dramatik anlatılar yoluyla gündeme taşıyan güçlü bir mecra olarak öne çıkar. Tiyatro, bu dönemde yalnızca sanat üretimi değil, aynı zamanda kamusal tartışmalar için bir alan sunmuştur. Brexit'in tiyatro sahnesindeki temsilleri çoğu zaman parçalanmışlık, ihanet, toplumsal çözülme ve liderlik krizleri etrafında şekillenmiş, seyircide empatik ve eleştirel bir bakış açısı

oluşturmayı hedeflemiştir. Bu noktada, Shakespeare'in klasik eserlerinin modern politik meselelerle yeniden yorumlanması kayda değerdir. Nitekim Shakespeare's Globe'un (2019) "*Making Sense of History*" başlıklı söyleşisinde, Adjoa Andoh'un yönettiği *Richard II* oyununun "ülke kimliği, egemenlik ve yönetim krizi" gibi meseleleri tartışmaya açtığı ve Brexit süreciyle bağlantı kurduğu belirtilmiştir. Politikacılar, oyundaki "Bu kutsanmış toprak, bu dünya, bu krallık, bu İngiltere" (This blessed plot, this earth, this realm, this England) gibi satırları ulusal bağımsızlık ve tarihsel yücelik mesajlarıyla ilişkilendirerek konuşmalarında sıkça kullanmış; böylece bu alıntılar, İngiltere'nin kendi kaderini tayin hakkına vurgu yapan duygusal birer sembole dönüşmüş ve geleneksel kültürel metinler güncel politik gündeme dâhil edilmiştir.

Sahne sanatlarında ise, özellikle Julius Caesar, King Lear ve Coriolanus gibi Shakespeare oyunları, Brexit bağlamında güncel politik okumalarla yeniden sahnelenmiştir. Julius Caesar'da ihanet ve halkın kolaylıkla yönlendirilebilmesi, referandum sürecindeki popülist stratejilere göndermede bulunur. King Lear, liderlik krizleri ve bölünmüş krallık anlatısıyla, Birleşik Krallık'ın içinden geçtiği otorite ve birlik sorunlarını yansıtır. Coriolanus ise halk-elit çatışması, sınıfsal kopuşlar ve siyasi iletişimsizlik gibi temalarla adeta Brexit sonrası oluşan sosyal fay hatlarına ayna tutar niteliktedir (Kerr, 2019: 43). Londra'daki The Globe gibi önemli tiyatro sahneleri bu oyunları sahneleyerek, klasik edebiyatın günümüz siyasetindeki yankılarını somutlaştırmıştır.

Tüm bu kültürel temsillerin dijital ortamda karşılık bulduğu alan ise sosyal medyadır. Dijital çağın en belirgin özelliği olan bilgi dolaşımının hızlanması, Brexit sürecinde sosyal medya platformlarını güçlü birer politik iletişim aracı haline getirmiştir. Hashtag kampanyaları, halkın hem mobilize edilmesinde hem de kutuplaşmasında merkezi bir rol oynamıştır. Özellikle "#TakeBackControl" ve "#StrongerIn" gibi etiketler, kullanıcıların Brexit'e dair tutumlarını sade ve etkili biçimde yansıttıkları sloganlara dönüşmüştür (Jackson & Green, 2019: 56). Bu tür dijital aktivizm biçimleri, sadece mesajın yayılımını değil, aynı zamanda duygusal tepkilerin ve aidiyetlerin inşasını da kolaylaştırmıştır. Lee (2020), bu süreçte sosyal medyada yürütülen kampanyaların, mikro hedefleme teknikleri sayesinde bireylerin

siyasi görüşlerini doğrudan etkileyecek şekilde tasarlandığını ve bu durumun demokrasiyi nasıl yeniden tanımladığına dikkat çeker.

Ancak sosyal medyanın bu süreçteki rolü, yalnızca demokratik katılımı teşvik eden bir alanla sınırlı kalmamış, aynı zamanda dezenformasyon, bilgi manipülasyonu ve dijital kutuplaşmanın da aracı haline gelmiştir. Sosyal medya algoritmalarının kullanıcıları belirli bilgi kümelerine maruz bırakmasının kamusal tartışmanın yapısını ciddi biçimde değiştirmektedir (Kaplan, 2021: 102). Bu da sosyal medya alanını yalnızca bir iletişim platformu değil, aynı zamanda kültürel temsillerin ve politik anlamların yeniden üretildiği bir mecra haline getirmiştir.

Brexit süreci, kültürel temsiller aracılığıyla sadece politik bir kırılma değil, aynı zamanda İngiliz kimliği ve toplumunun derinlemesine sorgulandığı çok katmanlı bir dönüşüm alanı haline gelmiştir. Bu dönüşümde, özellikle Shakespeare'in eserlerinin güncel politik bağlamlarda yeniden yorumlanması, hem politikacıların gündeminde hem de sanatın çeşitli dallarında önemli bir rol oynamış ve İngiliz kültürünün sürekliliği ile değişimini anlamamızda kilit bir unsur olmuştur (Bauer, 2021: 21-30).

1.2. Dijital Manipülasyonun Anahtarı: Cambridge Analytica ve Facebook Skandalı

Günümüzde bilgi akışının büyük ölçüde dijital platformlar üzerinden gerçekleşmesi, siyasal iletişimde yeni fırsatlar ve riskler ortaya çıkarmıştır. Dijital manipülasyon, kullanıcıların bilinçli tercihlerini etkilemek amacıyla sosyal medya ve veri analitiği gibi teknolojilerin kasıtlı olarak yönlendirilmesi sürecidir (Woolley & Howard, 2017: 22). Bu manipülasyon biçimi, geleneksel propaganda yöntemlerinden farklı olarak, bireylerin psikolojik ve davranışsal verilerini kullanarak daha hedefli ve kişiselleştirilmiş müdahaleler yapabilme kapasitesine sahiptir (Marwick & Lewis, 2017: 135). Böylece dijital manipülasyon, demokratik süreçlerin temel yapı taşlarından biri olan bilgiye erişim ve karar verme mekanizmalarını karmaşıktırmakta ve siyasetin doğrudan etkileme biçimlerini yeniden şekillendirmektedir.

Bu bağlamda Cambridge Analytica, 2013 yılında kurulan ve veri analitiği ile psikografik profillemeye alanında uzmanlaşmış bir siyasi danışmanlık şirkettir. Şirket, büyük veri ve AI tekniklerini kullanarak seçmen davranışlarını analiz etmiş ve

kampanyalara stratejik danışmanlık yapmıştır (Cadwalladr & Graham-Harrison, 2018: 112). Özellikle sosyal medya üzerinden toplanan geniş veri içeriklerini işleyerek, bireylerin psikolojik özelliklerine dayalı mikro hedefleme kampanyaları geliştirmiştir. Bu yöntemle Cambridge Analytica, politik iletişimde devrim niteliğinde bir dönüşüm sağlamış, ancak bu süreç etik ve yasal sınırları zorlayan tartışmaları da beraberinde getirmiştir.

2016 ABD başkanlık seçimleri ve Brexit referandumu sürecinde Cambridge Analytica'nın Facebook üzerinden topladığı kişisel verilerle yürüttüğü psikolojik profillemeye çalışmaları, dijital manipülasyonun yeni bir dönüm noktası olarak kabul edilmektedir (Cadwalladr & Graham-Harrison, 2018: 112). Cambridge Analytica, Facebook kullanıcılarının izni olmaksızın milyonlarca profil verisini toplayarak, bireylerin kişilik özelliklerini analiz etmiş ve bu verileri seçmen davranışlarını hedeflemek için kullanmıştır (Kirkpatrick, 2019: 78). Bu süreç, sadece seçmenlere yönelik özelleştirilmiş mesajlar üretmekle kalmamış, aynı zamanda bireysel psikolojinin derinlemesine incelenerek politik tercihlerin manipülasyonuna olanak sağlamıştır.

Özellikle psikografik profillemeye yöntemi, Big Five kişilik modeli üzerinden bireylerin kişilik özelliklerini ortaya çıkararak, bu özelliklere uygun mesajların hedeflenmesini mümkün kılmıştır (Matz et al., 2017: 3). Bu teknik, kullanıcıların sosyal medya davranışlarından çıkarılan veri setleri sayesinde, politik kampanyaların daha etkili ve birey odaklı hale gelmesini sağlamıştır. Ancak bu durum, demokratik süreçler açısından ciddi etik ve politik sorunlar doğurmuştur. Zira bireylerin rızası olmadan toplanan bu veriler, politik tercihlerinin yönlendirilmesinde araç olarak kullanılmış ve böylece seçimlerin meşruiyeti tartışmaya açılmıştır (Isaak & Hanna, 2018: 124).

Üstelik Cambridge Analytica skandalının ortaya çıkmasının ardından, hem Birleşik Krallık'ta hem de uluslararası arenada önemli politik ve toplumsal yankılar meydana gelmiştir. İngiltere'de bu skandal, Brexit referandumunun meşruiyeti üzerine ciddi soru işaretleri yaratmış ve halk arasında dijital veri güvenliği ile seçimlerin şeffaflığı konusunda artan bir güvensizliğe yol açmıştır (Cadwalladr, 2019: 215). Skandal, İngiliz parlamentosunda ve AB kurumlarında yoğun tartışmalara sebep olmuş, AB ülkeleri veri koruma ve seçim müdahaleleri konularında yeni düzenlemeler geliştirme ihtiyacı hissetmiştir (European Commission, 2018: 48).

AB genelinde, GDPR gibi veri gizliliği yasalarının sıkılaştırılması süreci hızlandırılmıştır. Bunun yanında, Cambridge Analytica olayı dijital propaganda ve seçim müdahalelerine karşı uluslararası iş birliği ve denetim mekanizmalarının gerekliliğini de ortaya koymuştur (Helmus & Bodine-Baron, 2020: 59). Özellikle Avrupa Parlamentosu seçimlerinde dijital manipülasyonun önlenmesine yönelik girişimler artmış, kamuoyunda seçim güvenliği ve bilgi kirliliğiyle mücadele öncelikli gündem maddeleri arasında yer almıştır.

Cambridge Analytica skandalı sonrasında, diğer demokrasi ülkelerine de uyarıcı bir örnek teşkil etmiş; ABD, Kanada ve Avustralya gibi ülkelerde dijital manipülasyonun sınırları ve etkileri üzerine kapsamlı araştırmalar başlatılmıştır. Bu ülkelerdeki parlamentolar, sosyal medyanın demokrasi üzerindeki etkilerini anlamak amacıyla soruşturmalar başlatmıştır. Öncelikleri veri gizliliği ihlallerini ve psikolojik hedeflemenin demokratik karar alma üzerindeki sonuçlarını incelemeye odaklanmak üzerine olmuştur (Oxford Internet Institute, 2019; Joint Select Committee on Foreign Interference, 2019; Lowy Institute, 2020).

ABD’de Federal Seçim Komisyonu ve Federal Ticaret Komisyonu (FTC) gibi kurumlar, sosyal medya şirketlerinin veri toplama ve reklam uygulamalarını denetlemeye başlamış, seçim güvenliği ile ilgili politikalar geliştirilmiştir (Mueller, 2019: 154). Kanada’da ise Dijital Demokrasi Komisyonu kurulmuş, kamuoyunun seçimlerde dijital müdahalelerden korunması için yeni yasal düzenlemeler ve şeffaflık mekanizmaları önerilmiştir (Smith & Adams, 2020: 67). Avustralya’da da benzer şekilde, dijital propaganda faaliyetlerinin tespiti ve önlenmesi amacıyla teknoloji şirketleri ile iş birliği yapılmış ve seçimlerde dijital dezenformasyonla mücadeleye yönelik stratejiler geliştirilmiştir (Brown & Nguyen, 2021: 89). Bu durum demokratik sistemleri derinden etkileyen bir dönüm noktası olarak kabul edilmektedir.

Bu bağlamda Cambridge Analytica vakası, veri odaklı siyasetin sadece teknolojik bir yenilik olmayıp, demokratik sistemler üzerinde derin ve kalıcı etkiler yaratan siyasi bir strateji olduğunu göstermektedir. Bireysel psikolojinin makine öğrenimi ve büyük veri analitiğiyle birleşmesi, geleneksel siyasal iletişim modellerini kökten dönüştürerek, seçmenlerin bilinçli tercih yapma kapasitesini zedelemiş ve karar süreçlerini görünmez manipülasyonlarla şekillendirmiştir (Tufekci, 2015: 89).

Bu dijital manipölasyonun ortaya çıkardığı tehditler karşısında, uluslararası alanda başlatılan kapsamlı araştırmalar ve düzenlemeler, demokratik süreçlerin kırılganlığını azaltmayı, seçmenlerin bilgiye erişimini güvence altına almayı ve sosyal medya platformlarının sorumluluklarını artırmayı amaçlamıştır. Böylece, Cambridge Analytica skandalı sonrası gelişen bu reaksiyonlar, dijital çağda demokratik sistemlerin korunması adına kritik bir dönüm noktası oluşturmuştur (Woolley & Howard, 2017: 23).

1.3. Algoritmik Kampanyalar ve Seçmen Hedefleme Yöntemleri

Dijitalleşmenin siyasal iletişime etkisi, özellikle algoritmik kampanya tekniklerinin yükselişiyle birlikte belirgin bir dönüşüm geçirmiştir. Bu tür kampanyalar, veri odaklı stratejilerle seçmenlerin tercihlerini tahmin etmeye ve bireysel düzeyde özelleştirilmiş mesajlar sunmaya odaklanır. Geleneksel propaganda biçimlerinden farklı olarak, algoritmik kampanyalar seçmene doğrudan hitap eden içerikler üretme kapasitesine sahiptir (Bennett & Segerberg, 2013: 746).

Bu yaklaşımda seçmen kitlesi, yalnızca yaş, cinsiyet veya coğrafi konum gibi yüzeysel verilerle değil; çevrimiçi davranış örüntüleri, içerik etkileşimleri ve psikolojik eğilimler gibi derinlemesine analizlerle sınıflandırılır. Kampanya stratejistleri, bu sınıflandırmalardan elde ettikleri içgörüler sayesinde, her alt gruba özel mesajlar üretebilir. Bu dönüşüm, siyasi iletişimi homojen kitlelerden bireysel farkındalıklara yönlendirmiştir (González-Bailón, 2017: 61).

Dijital propaganda ile geleneksel propaganda arasındaki en önemli farklardan biri, mesajın biçimi ve iletim tarzında ortaya çıkar. Geleneksel yöntemler kitlesel yayın araçlarıyla herkese aynı içeriği sunarken, dijital propaganda platformları kullanıcının davranışlarına ve ilgi alanlarına göre içerikleri uyarlama yeteneğine sahiptir. Bu sayede siyasal mesajlar yalnızca yayılmakla kalmaz, aynı zamanda hedef bireyin değer sistemine entegre olacak şekilde şekillenir (Kreiss, 2016: 45).

Bu sistemlerin teknik işleyişi üç temel aşamaya dayanır. İlk olarak, büyük veri analitiği yoluyla çevrimiçi platformlardan elde edilen kullanıcı davranışları sistematik biçimde toplanır ve işlenir. İkinci aşamada, makine öğrenimi algoritmaları bu verileri

analiz ederek seçmenlerin eğilimlerini tahmin eder. Son olarak, AI destekli modellemeler, elde edilen bulgulara göre mesaj içeriklerini kişiselleştirir, zamanlamayı optimize eder ve etkileşim düzeyini artıracak stratejiler belirler (Howard & Bradshaw, 2018: 9; Tufekci, 2014: 213).

Algoritmik kampanyaların demokratik süreçler üzerindeki etkileri ise çift yönlü bir tartışmayı beraberinde getirir. Bir tarafta, seçmenlerin daha ilgili ve kendileriyle örtüşen mesajlara maruz kalması, siyasal katılımı ve bilinç düzeyini artırabilme potansiyeline sahiptir. Diğer taraftan, veri mahremiyetinin ihlali, seçmen manipülasyonu ve yankı odalarının güçlenmesi gibi olgular, seçim süreçlerinin adaletinin ve şeffaflığının tehdit edilebilir bir konumda yer almasını sağlamaktadır. (Isaak & Hanna, 2018: 44).

1.3.1. Brexit Kampanyalarında Mikro-Hedefleme Stratejileri

Siyasi kampanyalarda seçmene ulaşmanın geleneksel yöntemleri uzun yıllar boyunca televizyon reklamları, mitingler, yazılı medya ve genel demografik veriler üzerinden şekillenmiştir. Ancak 21. yüzyılın ilk çeyreğinde dijital platformların yükselişi ve veri analiz tekniklerindeki gelişmeler, siyasi iletişimde yeni bir paradigmanın doğmasına yol açmıştır: mikro-hedefleme (Borgesius et al., 2018: 83; Zuiderveen Borgesius, 2020: 5).

Özellikle Brexit referandumunda mikro-hedeflemenin etkin biçimde kullanılması, dijital propagandanın bireysel düzeydeki etkilerini gözler önüne sermiştir (Grassegger & Krogerus, 2017: 45). Mikro-hedefleme stratejisini hâlâ “yeni bir fenomen” olarak tanımlamaktadır. Çünkü bu yöntem, geleneksel toplu iletişim yaklaşımlarından farklı olarak, bireylere ya da küçük seçmen gruplarına özel olarak tasarlanmış mesajların belirli dijital kanallar üzerinden zamanında iletilmesini amaçlamaktadır (Bodó, Helberger ve de Vreese, 2017: 1-5).

Bu bağlamda seçmen, salt bir “hedef kitle” değil; veriyle tanımlanmış, algoritmalar tarafından analiz edilip yönlendirilebilen bir birey haline gelir (Borgesius et al., 2018: 87). Mikro-hedefleme yalnızca iletişim stratejisi değil, siyasal psikoloji ve davranışsal ikna tekniklerini içeren karmaşık bir sistem olarak tanımlanabilir (Bennett & Segerberg, 2013: 74). Teknik açıdan mikro-hedefleme dört temel aşamadan oluşur:

veri toplama, segmentasyon, mesaj üretimi ve dağıtım optimizasyonu (Hersh, 2015: 14; Tufekci, 2014: 209).

İlk aşamada, bireylerin yaş, cinsiyet, eğitim düzeyi ve coğrafi konum gibi klasik demografik verileri toplanır. Ancak bu veriler günümüz algoritmik kampanya sistemlerinde yetersiz kalmaktadır. İkinci aşamada ise bireylerin çevrimiçi davranışları, beğeni ve sosyal medya etkileşimleri analiz edilerek psikografik profiller oluşturulur (Kosinski, Stillwell & Graepel, 2013: 5802). Bu verilerle seçmenler gruplandırılır (segmentasyon). Örneğin; göçmenlik konusunda hassas, ekonomik belirsizlik yaşayan orta yaş grubu bireyler bir segmenti oluşturur ve bu segment için “AB göç politikalarıyla kontrol elimizden alındı” gibi kaygıya hitap eden mesajlar hazırlanır (Grassegger & Krogerus, 2017: 52; Zuiderveen Borgesius et al., 2018: 89).

Bu süreç, siyasi mikro-hedeflemenin algoritmalar aracılığıyla seçmenlere kişiselleştirilmiş mesajlar ulaştırma süreci olarak belirtilmektedir (Bodó et al., 2017: 5-7). Mikro-hedeflemenin başarısı, mesajların ne denli kişiselleştirildiğiyle doğrudan ilişkilidir. Mesajların genellikle yaş, cinsiyet, konum, eğitim düzeyi, dil tercihleri, dijital alışkanlıklar, ilgi alanları ve çevrimiçi davranışlar temelinde özelleştirildiğini belirtir (Borgesius et al., 2018: 83-96). Örneğin, genç ve şehirli seçmenlere yenilikçi bir dil kullanılırken, kırsal ve yaşlı seçmenlere geleneksel değerlere vurgu yapan içerikler sunulur (Howard & Kollanyi, 2016: 7).

Kişiselleştirme yalnızca biçimsel değil, içerik düzeyinde de derinlemesine uyarlamaları kapsar. Seçmenin geçmişte hangi içerikleri paylaştığı, hangi reklamlara tıkladığı gibi veriler, onun hangi mesajlara daha açık olduğunu gösteren önemli göstergelerdir (Ghosh, 2018: 244). Bu sinyaller, Facebook, Google gibi dijital platformların algoritmaları tarafından analiz edilerek kampanya içerikleri optimize edilir. Bu yöntemin “seçmen davranışının önceden tahmin edilmesini ve duygusal tepkilerle yönlendirilmesini mümkün kıldığı” vurgulanmaktadır (Borgesius et al. 2018: 89).

Mikro-hedeflemenin en gelişmiş örneklerinden biri “lookalike audience” (benzer hedef kitle) modelidir. Bu model, mevcut destekçilerin veri profillerinden yola çıkarak benzer özellikteki yeni bireyleri tespit eder ve hedefler (Borgesius et al., 2018:

90). Facebook'un Lookalike Audiences özelliği bu yöntemin yaygın uygulamasıdır. Bu sayede kampanya bütçesi, ilgilenme ihtimali yüksek seçmenlere yoğunlaştırılır. Ancak bu yöntemin başarısı veri kalitesi ve algoritmanın doğruluğuna bağlıdır (Zuiderveen Borgesius, 2020: 6).

2016 Brexit sürecinde Cambridge Analytica adlı veri analiz şirketinin rolü, mikro-hedeflemenin politikadaki gücünü ortaya koyan önemli bir örnektir. Şirket, milyonlarca Facebook kullanıcısının verisini izinsiz toplayarak seçmenlerin psikolojik profillerini çıkarmış ve buna göre hedeflenmiş reklamlar geliştirmiştir (Grassegger & Krogerus, 2017: 60).

Cambridge Analytica'nın stratejisinde OCEAN (Openness, Conscientiousness, Extraversion, Agreeableness, Neuroticism / Açıklık, Sorumluluk, Dışadönüklük, Uyumluluk ve Duygusal denge) kişilik modeli temel alınmıştır (Kosinski et al., 2013: 5803). Böylece, her seçmene psikolojik yapısına uygun mesajlar iletilmiştir. Örneğin, yüksek "Neuroticism"(Nevrotiklik) puanı olan bireylere kaygı ve korku temalı içerikler, "Openness"(Açıklık) yüksek olanlara ise yenilik ve değişim çağrısı yapan mesajlar sunulmuştur (Grassegger & Krogerus, 2017).

Bu kişiselleştirilmiş yaklaşım, Brexit sürecinin karmaşık ve kutuplaştırıcı ortamında seçmen davranışlarını şekillendirmiştir (Bodó et al., 2017: 6). Ancak Cambridge Analytica olayı, veri gizliliği ihlalleri ve demokratik süreçlerin şeffaflığı açısından etik kaygıları beraberinde getirmiştir (Borgesius et al., 2018: 92).

Mikro-hedefleme stratejilerinin siyasi iletişimde yükselişi, seçmen davranışlarını daha ince ve dinamik biçimlerde analiz etmeye olanak tanımaktadır (Hersh, 2015: 22). Ancak, bu teknolojilerin demokratik süreçler üzerindeki etkileri hâlâ tartışmalı olup, şeffaflık ve hesap verebilirlik gerekliliği giderek daha fazla vurgulanmaktadır (Chadwick, 2017: 130). Bu bağlamda, mikro-hedeflemenin hem seçimlerin etkinliğini artırma potansiyeli hem de etik kaygılar doğurma ihtimali, alanın önemli bir araştırma konusu olmaya devam edeceğini göstermektedir (Hersh, 2015: 45). Brexit kampanyasında görüldüğü üzere, mikro-hedefleme giderek artan kişiselleştirilmiş ve veri odaklı yaklaşımların önemli bir göstergesidir (Bodó et al., 2017: 7). Dolayısıyla, bu

stratejilerin demokratik normlarla uyumu üzerine kapsamlı ve çok disiplinli çalışmalar yapılması gerekmektedir (Tufekci, 2014: 210).

1.3.2. Psikografik Profillemeye ve Veri Odaklı Seçmen Tanımlama

Günümüzde veri odaklı siyasi kampanyalar, demokratik süreçleri şekillendirme biçiminde devrim niteliğinde değişiklikler yaratmaktadır. Bu kampanyaların merkezinde, seçmenlerin yalnızca demografik ve sosyoekonomik göstergelere göre değil, aynı zamanda psikolojik eğilimlerine göre de sınıflandırılmasını hedefleyen psikografik profillemeye yöntemleri yer almaktadır. Psikografik profillemeye, geleneksel demografik analizlerin ötesine geçerek, bireylerin kişilik özellikleri, değer yargıları, motivasyonları ve yaşam tarzlarına dair derinlemesine veri analizine dayanır. Bu yaklaşımın temel amacı, seçmenlerin hangi tür mesajlara daha duyarlı olduğunu önceden tahmin ederek, iletişim stratejisini daha kişiselleştirilmiş ve etkili bir şekilde şekillendirmektir (Matz et al., 2017: 82). Bu bağlamda, psikografik profillemeye yalnızca siyasi alanla sınırlı kalmayıp, pazarlama, reklamcılık ve kamu politikalarında da etkisini artırmaktadır.

Psikografik profillemeye süreçlerinde sıklıkla kullanılan modellerden biri, OCEAN diğer bir deyişle Beş Büyük Faktör kişilik modelidir. Mikro-hedefleme stratejileri içerisinde de yer alan bu model, açıklık (Openness), sorumluluk (Conscientiousness), dışadönüklük (Extraversion), uyumluluk (Agreeableness) ve nevroitiklik (Neuroticism) olmak üzere beş temel kişilik boyutuna dayanarak bireyleri kategorize eder. Bu beş kişilik boyutu, sosyal medya etkileşimlerinden, çevrimiçi davranışlardan ve diğer dijital veri kaynaklarından türetilen verilerle birleştirilerek, hangi mesajların hangi bireyleri etkileyeceği yüksek doğrulukla tahmin edilebilir hale gelmiştir (Kosinski, Stillwell & Graepel, 2013: 5802). Modern AI algoritmaları ve makine öğrenimi teknikleri, bu veri setlerini analiz ederek karmaşık psikolojik profilleri oluşturmakta ve bu profiller ışığında özelleştirilmiş propaganda stratejileri geliştirilmektedir.

Teknolojik altyapı açısından, psikografik profillemeye büyük veri (big data) analitiği, NLP ve yapay sinir ağları gibi gelişmiş yöntemlerden yararlanmaktadır. Büyük veri (big data), hacmi, hızı ve çeşitliliği geleneksel veri işleme yazılımlarının kapasitesini aşan çok büyük ve karmaşık veri kümelerini ifade eder. Bu veriler, sosyal

medya, dijital platformlar ve diğer kaynaklardan gerçek zamanlı olarak toplanabilmektedir (Mayer-Schönberger & Cukier, 2013: 15). NLP, bilgisayarların insan dilini anlaması, yorumlaması ve üretmesini sağlayan AI alanıdır; sosyal medya paylaşımları, yorumlar ve metin tabanlı verilerin analizinde kritik rol oynar (Jurafsky & Martin, 2020: 45).

Psikografik profillemenin Brexit kampanyasında kullanıldığına dair iddialar, farklı türdeki güçlü kanıtlarla desteklenmektedir. Öncelikle Cambridge Analytica'nın eski çalışanı Christopher Wylie, İngiliz Parlamentosu Dijital, Kültür, Medya ve Spor Komitesi (DCMS / UK Parliament Digital, Culture, Media and Sport (DCMS) Committee session) oturumunda, Leave.EU kampanyası bağlamında Facebook verilerinin kullanılarak seçmen profillerinin çıkarıldığını net biçimde ifade etmiştir. Wylie, Cambridge Analytica ile birebir bağlantılı AggregateIQ adlı firmanın Leave.EU kampanyasında kullanıldığını belirtmiştir (Wylie, 2018: 5–6; AP News, 2018).

Bu tanıklığa ek olarak, ICO tarafından hazırlanan “Democracy Disrupted” (Demokrasinin Bozulması) Raporu da bu iddiaları resmi zemine taşımaktadır. ICO'nun yayımladığı raporda, Cambridge Analytica'nın ve bağlı şirketlerin siyasi kampanyalarda veri analizini ve psikolojik hedeflemeyi kullandığına dair güçlü bulgular yer almaktadır (ICO, 2018: 12).

Bu veriler ışığında, psikografik profillemeye algoritmik kampanyaların etkinliğini artıran temel bir bileşen olarak öne çıkarken, bu teknolojilerin şeffaflık, denetlenebilirlik ve etik sınırlar içerisinde uygulanması demokratik sistemlerin korunması açısından büyük önem taşımaktadır. Brexit kampanyasında yaşanan örnekler, veri temelli stratejilerin kitlesel ölçekte yönlendirme aracı haline gelebileceğini ve demokratik süreçlere potansiyel tehditler oluşturabileceğini göstermektedir (Zuboff, 2019: 276; Bennett & Lyon, 2019: 15). Bu nedenle, gelecekte bu tür teknolojilerin denetim mekanizmalarının güçlendirilmesi, veri mahremiyetinin korunması ve toplumsal farkındalığın artırılması gerekmektedir (Isaak & Hanna, 2018: 59).

1.3.3. AI Destekli Kampanya Optimizasyonu ve Tahmin Modelleri

Geleneksel siyasi kampanyalar, uzun yıllardır esas olarak kitle iletişim araçları ve anket verilerine dayalı biçimlerde yürütülmüştür. Ancak son dönemde AI ve ML (Machine Learning / Makine Öğrenimi) teknolojilerindeki hızlı gelişmeler, siyasal iletişimde stratejik bir dönüşümün habercisidir. AI'nın e-posta yazımı ve seçmenle birebir dijital etkileşim gibi kampanya uygulamalarında kullanılabilirliği de literatürde tartışılmaktadır (Foos, 2024: 8).

AI destekli sistemler, siyasi kampanyalarda seçmen davranışlarını modellemek, bireysel eğilimleri analiz etmek ve buna uygun kişiselleştirilmiş propaganda içeriği üretmek amacıyla etkin biçimde kullanılmaktadır. Özellikle, 2024 AB seçimlerinde yapılan araştırmalar, sosyal medyada yürütülen dijital kampanyaların mikro hedeflemeyle kamusal etkileşimi derinleştirdiğini ve manipülasyon riskini artırdığını göstermektedir (Sernani, Cossiri, Di Cosimo & Frontoni, 2025: 12).

ML algoritmalarının pratik uygulamalarına baktığımızda, büyük veri üzerinden karar ağaçları ve kümelenme analizleriyle seçmen segmentasyonu yapılmakta; NLP ile sosyal medya duygu analizleri gerçekleştirilmekte ve tahmine dayalı modellerle seçmen eğilimleri öngörülmektedir. Bu durum geleneksel “kitle iletişimi” yerine daha kişiselleştirilmiş propaganda stratejilerinin benimsenmesine yol açmıştır (Sernani, Cossiri, Di Cosimo & Frontoni, 2025: 12).

A/B testleri (A/B testing: aynı kampanya veya içerikten iki farklı versiyonun test edilerek hangisinin hedef kitle üzerinde daha etkili olduğunun ölçülmesi yöntemi), de dijital kampanyaların sessiz ama etkili araçlarından biridir. Farklı mesaj varyasyonlarının etki düzeyini test ederek hangi içeriklerin daha yüksek geri dönüş sağladığını belirlemeye olanak tanır. Özellikle mikro hedefleme uygulamaları, bu yöntemle mesajların hedef kitlenin duygusal tepkisine göre optimize edilmesini sağlamaktadır (Brennan Center, 2024: 22).

Dijital kampanyalarda AI destekli stratejilerin seçmen davranışlarını analiz ederek, mevcut seçmen tabanını korumaya ve potansiyel kayıpları minimize etmeye yönelik kullanıldığını vurgulamaktadır (Foos, 2024: 8). Bu çalışmadan hareketle, pazarlama literatüründen ödünç alınan “churn riski” kavramını siyasal bağlama

uyarlayarak seçmen kaybı riski olarak yeniden tanımlanabilmektedir. Bu bağlamda benim değerlendirmeme göre, AI destekli stratejiler sadece mevcut seçmen tabanını korumakla kalmayıp, oy kazanma stratejilerinin merkezine yerleştirilen kritik bir parametre hâline gelmektedir.

AI tabanlı kampanya yönetimini, seçmen davranışlarını analiz ederek iletişim stratejilerini optimize etmektedir. Brexit referandumu sürecinde, bu tür AI tabanlı stratejiler yalnızca mesaj içeriklerini optimize etmekle kalmamış; aynı zamanda seçmen davranışlarını doğrudan etkileyerek oy kazanma ve kaybetme dengesini yönlendirmiştir. Cambridge Analytica'nın mikro-hedefleme ve psikometrik analizler üzerinden yürüttüğü stratejiler, belirli bölgelerde “Leave” veya “Remain” oylarının artmasını hedeflemiş ve böylece AI'nin demokratik süreçlerde teknik bir araç olmanın ötesinde etkin bir aktöre dönüştüğünü göstermiştir (Foos, 2024: 8). Bu bağlamda, pazarlama literatüründen ödünç alınan “churn riski” kavramının siyasal bağlamda uygulanması, kampanya etkinliğini artıran ve seçmen davranışlarının stratejik yönlendirilmesini açıklayan önemli bir analitik çerçeve sunmaktadır. Ayrıca, AI tabanlı kampanya yönetimi yalnızca iletişim stratejilerini değil; ulusal egemenlik, kamuoyu inşası ve uluslararası sistem dinamiklerini de yeniden şekillendirebilecek güçte olduğunu kanıtlamaktadır.

1.4. Hukuki ve Düzenleyici Süreçler

Brexit süreci, AB ve Birleşik Krallık (İngiltere) arasındaki hukuki ve düzenleyici ilişkilerin yeniden şekillenmesine neden olmuş; özellikle veri koruma ve dijital haklar alanında önemli dönüşümler yaşanmıştır. AB'nin içerisinde yer alan GDPR, 2018 yılında yürürlüğe girmesiyle, kişisel verilerin işlenmesi ve korunması konusunda uluslararası standartları belirlemiş ve AI uygulamalarının etik ve yasal sınırlarını çizmiştir (Voigt & Von dem Bussche, 2017: 134-136). Ancak, Brexit sonrasında İngiltere, GDPR'dan ayrı olarak kendi veri koruma rejimini geliştirmeye başlamış ve 2021'de yürürlüğe giren “Veri Koruma Yasası 2018”'in (Data Protection Act 2018) revize versiyonlarıyla dijital hakları kendi ulusal bağlamında düzenlemiştir (Kuner, 2021: 215).

AI teknolojilerinin kişisel verilerin işlenmesindeki rolü arttıkça, GDPR kapsamında veri sahiplerinin haklarının korunması daha karmaşık bir hal almaktadır. Özellikle otomatik karar verme süreçleri ve profil oluşturma uygulamalarında şeffaflık ve hesap verebilirlik ilkeleri kritik önem taşımaktadır (Wachter, Mittelstadt, & Floridi, 2017: 417). Brexit sonrası İngiltere'nin GDPR ile olan uyumluluğunu sürdürme çabaları, veri akışlarının kesintisiz devamı açısından önemli bir adım olmakla birlikte, bazı farklılıkların ortaya çıkması uluslararası şirketler için hukuki belirsizlikler yaratmaktadır (Bradshaw, Millard, & Walden, 2019: 789).

Ayrıca, Cambridge Analytica skandalı, AI'nın ve büyük veri analizlerinin demokratik süreçler üzerindeki etkilerini gözler önüne sermiştir. Bu skandalın ardından İngiltere'de ve AB'de veri koruma ve dijital haklarla ilgili yargı süreçleri hız kazanmış; mahkemeler ve düzenleyici kurumlar veri gizliliğinin sağlanması için yeni standartlar geliştirmiştir (Cadwalladr & Graham-Harrison, 2018: 2-4). Bu yargı süreçleri, Brexit sonrasında İngiltere'nin dijital düzenlemelerinde kendi yol haritasını çizmesi sürecini de hızlandırmıştır (Taylor, 2020: 103).

Brexit sonrası hukuki ve düzenleyici süreçler, dijital hakların korunmasında uluslararası işbirliğinin önemini yeniden vurgulamıştır (Zuboff, 2019: 265). AI teknolojilerinin hızlı gelişimi, mevcut mevzuatların sürekli olarak gözden geçirilmesini zorunlu kılmaktadır (Cath et al., 2018: 30). Özellikle veri koruma alanında esnek fakat güçlü düzenleyici çerçeveler, bireysel hakların ve demokratik değerlerin korunmasında kritik rol oynamaktadır (Binns, 2018: 122). Bu bağlamda, hukuk ve teknoloji arasındaki etkileşim, geleceğin dijital toplumunun şekillenmesinde belirleyici olacaktır (Floridi, 2020: 74).

1.4.1 GDPR ve Brexit Bağlamında Dijital Haklar

AB'nin GDPR düzenlemesi, 2016 yılında kabul edilip 25 Mayıs 2018'de yürürlüğe girmiştir (Voigt & von dem Bussche, 2017: 7). Bu yönetmelik, bireylerin kişisel verilerine yönelik erişim, düzeltme, silme gibi hakları açıkça tanımlarken, veri işleyen kurumlara da amaca uygunluk, veri asgariyle sınırlandırma ve şeffaflık ilkeleri çerçevesinde sorumluluklar yükler. GDPR'ın yaptırım mekanizması ise oldukça caydırıcıdır: Uygunsuzluk halinde, öngörülen ceza miktarı 20 milyon Euro'ya kadar veya işletmelerin küresel cirosunun %4'üne kadar çıkabilmektedir (Voigt & von dem Bussche, 2017: 201–217).

GDPR sadece Avrupa içi değil, AB pazarını hedefleyen küresel kuruluşlara da uygulanır; bu sayede, üye ülke dışında konumlanan şirketler için de geçerli bir düzenleyici norm haline gelir. GDPR'ın temel amacı; veri sahiplerinin haklarını güçlendirmek, veri denetleyicilerinin yükümlülüklerini netleştirmek ve veri koruma alanında uluslararası düzeyde normatif bir çerçeve oluşturmaktır.

Birleşik Krallık, GDPR'ın yürürlüğe girişiyle uyumlu olacak şekilde 2018 tarihli Data Protection Act ile GDPR hükümlerini kendi hukuk sistemine dâhil etmiş ve böylece GDPR'a dayalı bir çifte çerçeve oluşturmuştur. Brexit sonrası ise, UK GDPR olarak adlandırılan versiyon, temel GDPR ilkelerini korumaya devam etmiştir. 2025 yılında çıkarılan Data Use and Access Act (DUA Act / Veri Kullanımı ve Erişimi Yasası - DUA Yasası) ile Birleşik Krallık, daha esnek bir regülasyon modeline geçmiştir. EU GDPR'da yer alan “essential equivalence” (Esas Eşdeğerlik) standardı yerine “not materially lower” (önemli ölçüde düşük değil) standardını benimseyerek veri koruma seviyesinin GDPR'a birebir eşit olması gerekliliğini gevşetmiştir (UK Government, 2025: 12). Ek olarak, DUA Act ile ICO (Information Commissioner's Office / Bilgi Komiserliği Ofisi) yeniden yapılandırılarak stratejik yönlendirmeye dayalı bir kamusal bilgi kurumuna dönüşmüş; ayrıca çerez ve elektronik iletişim ihlalleri için daha yüksek cezalar; örneğin PECR (Privacy and Electronic Communications Regulations / Gizlilik ve Elektronik İletişim Düzenlemeleri) kapsamında küresel cironun %4'ü olarak belirlenmiştir (UK Government, 2025: 37).

Birleşik Krallık'ta GDPR düzenlemelerinin uygulanması sürecinde kurumların genel olarak düşük bir farkındalık düzeyine sahip olduğu gözlemlenmektedir. Özellikle üst düzey yöneticiler arasında GDPR ve gelecek düzenlemeler hakkında bilgi eksikliği yaygındır. Büyük ve düzenlenmiş sektörlerde faaliyet gösteren kuruluşlar daha bilinçliyse, diğer birçok kurum yeterince haberdar değildir. İç personel eğitiminin yetersizliği, veri ihlalleri riskini artırmakta ve ciddi yaptırımlara yol açabilmektedir. GDPR'nın karmaşıklığı ve Brexit'in yarattığı belirsizlik, birçok kuruluşun mevzuata uyum sağlamasını geciktirmiştir. Ayrıca, gelişmekte olan teknolojilerin (AI, bulut bilişim vb.) kullanımına dair bilgi eksikliği, veri koruma süreçlerinin etkinliğini olumsuz etkilemektedir (Addis & Kutar, 2018: 19-21).

Büyük veri teknolojilerinin kullanımı, veri sahipleri üzerinde ayrımcı etkiler yaratabilmekte ve bu durum veri koruma yasalarının etik temellerini sorgulatmaktadır. Büyük veri analizlerinin özellikle korunmasız gruplar için önyargılı sonuçlar doğurabileceğine dikkat çekilmiştir; bu nedenle GDPR gibi düzenlemelerin sadece veri güvenliğini değil, aynı zamanda adil ve eşitlikçi veri işleme süreçlerini de sağlaması gerektiğini vurgulamıştır (Barocas & Selbst, 2016: 150-155).

Sanal ve artırılmış gerçeklik teknolojilerinin yaygınlaşması, mevcut veri koruma mevzuatının güncellenmesini zorunlu kılmaktadır. Bu teknolojilerin sunduğu yeni veri toplama yöntemlerinin ve kullanıcı etkileşimlerinin mevcut yasal çerçevelerle uyumsuz olduğu ve GDPR gibi düzenlemelerin bu alanlara özgü revizyonlar gerektirdiği gündemde belirtilmiştir (Brimsted, 2016: 4-7).

GDPR, büyük teknoloji firmalarının (Amazon, Google, Microsoft gibi) bulut bilişim pazarındaki hâkimiyetini artırma potansiyeline sahiptir. GDPR'nın getirdiği sıkı veri koruma yükümlülükleri özellikle küçük ve orta ölçekli işletmelerin rekabet gücünü azaltarak, bu dev şirketlerin pazar payını büyütme kapasitesine sahiptir (Burton, 2016: 9-12). Bu durum, dijital egemenlik ve regülasyon farklılaşması açısından kritik bir gelişme olarak değerlendirilebilir.

GDPR ve Birleşik Krallık'ın GDPR sonrası düzenlemeleri, uluslararası sistem dinamikleri açısından iki temel etki yaratmaktadır. Birincisi, normatif yayılım olarak bilinen ve sıklıkla “Brussels Effect” (Brüksel Etkisi) şeklinde adlandırılan bir fenomen

ile GDPR, küresel ölçekte veri koruma normlarının yükselmesinde referans bir çerçeve oluşturmuştur (Bradford, 2020: 45). Birleşik Krallık da bu örüntüyü UK GDPR ve DUA Yasası ile devam ettirmiştir. Bu durum, uluslararası aktörler arasında norm uyumunu destekleyen sağlam bir altyapı temelini oluşturmuştur.

İkincisi ise, egemenlik ve diverjans dengesi yaklaşımıdır. Birleşik Krallık, Brexit sonrası regülasyon esnekliği ile regülasyon özerkliğini vurgularken, aynı zamanda uluslararası işbirliği ve veri akışının sürdürülebilirliğine de önem vermiştir (Bradshaw & Millard, 2021: 87). Bu model, gelecekte regülasyon özerkliği ile küresel veri işbirliğini dengede tutmayı hedefleyen hibrit bir yaklaşımı temsil etmektedir.

1.4.2. Cambridge Analytica Davaları ve Yargı Süreci

Cambridge Analytica skandalı, dijital haklar ve veri koruma alanında uluslararası çapta önemli bir yasal ve etik sınav niteliği taşımıştır (Hu, 2020: 100). Bu süreç, hem ABD’de hem de Birleşik Krallık’ta veri koruma rejimlerinin etkinliğini ve sınırlarını gözler önüne sermiştir.

Akademik literatürde Margaret Hu’nun çalışması (2020), ABD FTC, Cambridge Analytica ve Facebook skandalına yönelik yaptırım modelini eleştirel bir biçimde incelemiştir. FTC’nin yetkisi yalnızca “ticaret üzerindeki haksız ya da aldatıcı uygulamalar” ile sınırlı olup, bu nedenle veri gizliliğine dair güçlü yaptırımlar uygulaması mümkün olmamıştır (Hu, 2020: 100–102). Bu durum, skandalın ABD’deki hukuki sonuçlarının sınırlı kalmasına yol açmıştır.

ABD’li akademisyen David Carroll, kişisel verilerine erişim talebine Cambridge Analytica tarafından hakaret içeren bir yanıt aldığını belirtmiştir. Carroll, şirketin kendisine “Taliban mağarasında yaşayan biri kadar hakkınız yok” dediğini aktararak, veri hakkı kavramının nasıl görmezden geldiğine dikkat çekmiştir (UK Parliament, 2019, aktaran The Guardian, 2019). Carroll ayrıca, dava süreciyle şirketin veri işleme yöntemlerine dair birçok gizemin çözüldüğünü ifade etmiştir.

Birleşik Krallık ICO, sürece daha aktif müdahil olmuştur. ICO’nun yayımladığı resmi raporlara göre, yaklaşık üç yıl süren soruşturma sonunda Cambridge Analytica’nın Brexit referandumunu doğrudan etkileyecek şekilde veri ihlali yaptığına dair kesin kanıtlar bulunamamıştır. Özellikle UKIP ile bağlantılı ilk araştırmaların

dışındaki incelemelerde, referanduma doğrudan müdahale iddiaları desteklenmemiştir (UK Parliament Digital, Culture, Media and Sport Committee, 2019: 15–17; ICO, 2018).

DCMS Komitesi önünde ifade veren Cambridge Analytica CEO’su Alexander Nix, GSR (Dr. Aleksandr Kogan’a bağlı) kaynaklı Facebook verisini ilk etapta yanlışlıkla itiraf etmiş, ancak daha sonra bu veriyi hiç kullanmadığını iddia ederek çelişkili ifadelerde bulunmuştur. Komite başkanı, bu ifadeye “İngiltere’de böyle bir uygulama yok” ve “Bu yüzden yasa dışı” diyerek tepki göstermiştir. Nix’in bu beyanı, veri koruma yasalarının İngiltere’deki hassasiyetini ortaya koymuştur. Ayrıca, Nix ham verilere erişimi olmadığını belirtse de, komite AIQ gibi alt yüklenicilerin hem model verisine hem de ham verilere erişimi olabileceği şüphesini dile getirmiştir (UK Parliament Oral Evidence, 2018; aktaran BBC, 2018).

Yargı süreci açısından, Cambridge Analytica’nın bağlı kuruluşu SCL Elections, akademisyen David Carroll’un kişisel veri erişim talebini yerine getirmediği için yasal yaptırımlarla karşılaşmıştır. ICO tarafından açılan dava sonucunda şirkete 15,000 sterlin ceza ve ek yasal giderler uygulanmıştır (ICO, 2019: 22–24). Carroll, karar sonrasında yaptığı açıklamada, “Bu dava sayesinde, şirketin verileri ne şekilde topladığı ve işlediğine dair birçok gizem çözülmüş oldu” diyerek veri erişim hakkının pratikteki etkisini vurgulamıştır (ICO, 2019; aktaran The Guardian, 2019). Facebook ise, 1998 Veri Koruma Yasası kapsamında maksimum 500,000 sterlin para cezasına çarptırılmıştır (ICO, 2018b: 24–25).

Ayrıca, Cambridge Analytica’nın eski CEO’su Alexander Nix, yedi yıl boyunca şirket yönetiminden men edilmiştir. Bu karar, bireysel sorumluluğun hukuki anlamda somut yaptırımlarla karşılanabileceğinin önemli bir göstergesidir (Insolvency Service, 2020). DCMS Komitesi, Nix’in kamuoyunu yanıltıcı ifadeler kullandığını belirterek, bu durumun yasal men kararına gerekçe teşkil ettiğini rapor etmiştir (UK Parliament, 2019).

Cambridge Analytica skandalı, dijital hakların korunmasında hukuki süreçlerin önemini gözler önüne sermiştir (Gonzalez Fuster, 2014: 85). Veri koruma kurumlarının yetkilerinin artırılması, bireylerin kişisel veriler üzerindeki kontrolünü güçlendirmek

için zorunlu görülmektedir (Kuner, 2017: 212). AB'nin içerisinde yer alan GDPR, bu alanda önemli bir dönüm noktası olmuştur ve veri denetim otoritelerinin yetkilerini genişletmiştir (Voigt & Von dem Bussche, 2017: 139). Bununla birlikte, dijital veri alanındaki hızlı gelişmeler, politika yapıcıların farkındalığını artırmak ve güncel düzenlemeler yapmak için sürekli çaba göstermesini gerektirmektedir (Bradshaw, Millard & Walden, 2011: 44). Hukuki süreçlerin şeffaflığı, kamusal güvenin tesis edilmesinde kritik rol oynar ve yasal düzenlemelerin etkin uygulanmasını sağlar (Bennett & Raab, 2006: 101).

Ayrıca, veri ihlallerine karşı etkili yaptırımların varlığı, demokratik sistemlerin dijital manipölasyonlara karşı direncini artırır (Richards & King, 2013: 160). Dijital hakların korunması sadece bireylerin gizliliği için değil, aynı zamanda seçimlerin adil ve şeffaf yapılabilmesi için de hayati öneme sahiptir (Zuiderveen Borgesius et al., 2018: 57). Hukuki ve etik düzenlemeler, teknoloji şirketlerinin veri politikalarını denetlemeyi kolaylaştırırken, sivil toplumun da bilinçlenmesine katkı sağlar (Custers et al., 2013: 78).

Cambridge Analytica vakası, bu alanlarda iyileştirmeler yapılmasının gerekliliğini ortaya koymuş ve veri koruma mevzuatlarının güçlendirilmesini tetiklemiştir (Bradshaw, Millard & Walden, 2011: 49). Bu doğrultuda, dijital hakların korunmasında hukuki mekanizmaların geliştirilmesi, demokratik sistemlerin teknoloji kaynaklı risklere karşı dayanıklılığını artırmak için temel bir gereklilik olarak gün yüzüne çıkmaktadır (Kloza & van der Sloot, 2017: 203).

1.5. Cambridge Analytica'nın Brexit Sürecindeki Rolü: Anket Verileri ve Dijital Algı

Cambridge Analytica, Facebook üzerinden yaklaşık 87 milyon kullanıcının verilerini toplayarak bireylerin psikolojik profillerini oluşturmuş ve bu verileri Brexit kampanyasında hedefli reklamlar için kullanmıştır. Ancak Birleşik Krallık ICO, firmayı doğrudan Brexit referandumunda veri ihlali yapmakla suçlamamış, yalnızca bazı ilk temasların gerçekleştiğini belirtmiştir. Brexit sürecinde dijital propaganda faaliyetlerinin seçmen davranışlarına etkisini anlamak amacıyla yapılan kamuoyu araştırmaları, akademik çalışmalar ve sosyal medya analizleri önemli bir kaynak sağlamaktadır.

Oxford Üniversitesi'ne bağı Computational Propaganda Project (Hesaplamalı Propaganda Projesi) kapsamında gerçekleştirdikleri çalışmada dijital propaganda stratejilerinin küresel çapta nasıl organize edildiğini ortaya koymuş ve Brexit referandumunun bu stratejilerin merkezinde yer aldığını vurgulamıştır. Araştırma anketlerinde katılımcıların %35'i sosyal medyada karşılaştıkları politik içeriklerin oy verme kararlarını etkilediğini belirtmiştir (Bradshaw & Howard, 2018: 8 - 9). Bu, mikro-hedefleme yöntemleriyle kullanıcıların kişilik profillerine uygun mesajların seçim sürecinde ne kadar belirleyici olduğunu göstermektedir.

Cambridge Analytica'nın veri kullanımına ilişkin önemli nitel verilerden biri, The Guardian için yaptığı araştırmadır. Bu çalışmada Facebook'tan sızdırılan verilerin Leave kampanyasında korkuya dayalı ve kişiselleştirilmiş mesajlar yaymak için kullanıldığı ve bu mesajların seçmenlerin dünya algısını değiştirecek ölçüde etkili olduğu belirtilmiştir. Bir röportajda katılımcı şöyle ifade etmiştir: “Karşımda sürekli göçmenler işimizi elimizden alıyor” mesajı vardı. Normalde bu konuda bu kadar endişem yoktu ama sürekli gördükçe inanmaya başladım.” (Cadwalladr & Graham-Harrison, 2018: 4).

Benzer bulgular, Channel 4 News tarafından hazırlanan Detering Democracy adlı belgeselde de dolaylı biçimde teyit edilmektedir. Belgeselde, Cambridge Analytica'nın özellikle ırksal azınlık gruplarını oy kullanmaktan caydırmaya yönelik psikolojik hedefleme yöntemleri kullandığı aktarılmış; bu stratejilerin benzerlerinin Brexit sürecinde de kararsız seçmenler üzerinde uygulandığı öne sürülmüştür (Channel 4 News, 2018). Belgeselin tam içeriğine erişim sınırlı olsa da, Birleşik Krallık ICO'nun 2018 soruşturma raporları (ICO, 2018: 6-7) ve Cadwalladr ile Graham-Harrison'ın The Guardian için hazırladığı haber dosyaları (2018), dijital müdahalelerin seçim süreçlerine etkisini ortaya koymaktadır.

ICO'nun bulgularına göre, Cambridge Analytica Facebook verilerini usulsüz analiz ederek siyasi kampanyalarda kullanmıştır; bu verilerin hangi ülkelere ve siyasi aktörlere satıldığı ise net olarak belirlenememiştir (ICO, 2018: 6-8). Channel 4 News'in başka bir haberinde, firmanın yöneticileri belirli grupları “oy kullanmaktan caydırmak” için doğrudan hedefli mesajlar uyguladıklarını itiraf etmiştir (Channel 4 News, 2018).

Sosyal medya üzerinden nicel ve nitel yöntemlerle yürütülen mikro-hedefleme stratejileri; özellikle ideolojik açıdan savunmasız grupların manipülatif içeriklerle sistematik şekilde hedef alındığını ortaya koymuştur (González-Bailón & Wang, 2016: 13–15). Bu, Cambridge Analytica’nın psikometrik verilerle oluşturduğu hedefleme modellerinin seçim sonuçlarına etkisini açıklamada önemli bir kanıttır. Diğer yandan, 1 milyon Facebook kullanıcısının paylaşım ağlarını analiz ederek kullanıcıların çoğunlukla kendi görüşlerini doğrulayan içeriklerle etkileşimde bulunulmuştur. Bu etkileşim “yankı odası” etkisinin toplumsal kutuplaşmayı artırdığını göstermiştir (Del Vicario et al., 2016: 554–558). Algoritmalar, kullanıcıların onayladıkları görüşlere uygun içerikleri önceliklendirerek bilgi çeşitliliğini azaltmakta ve propaganda mesajlarının etkisini artırmaktadır.

YouGov tarafından 2025 yılında yapılan bir anket, İngiltere vatandaşlarının %56’sının geriye dönüp baktıklarında AB’den ayrılma kararını yanlış bulduklarını göstermektedir (YouGov, 2025). Bu bulgu, dijital mikro-hedefleme ve propaganda faaliyetlerinin halkın karar verme süreçleri üzerindeki karmaşık etkisini tartışmak için önemlidir. Sosyal medyada yayılan dezenformasyonun seçim sürecine etkisini ortaya koyulan çalışmada; özellikle “yalan haberlerin” Leave kampanyası süresince sistematik olarak hedefli gruplara yönlendirildiğini belirtmiştir (Allcott & Gentzkow, 2017: 220–225).

British Election Study (BES) projesi, Brexit öncesi ve sonrası sosyal medya etkileşimlerini araştırarak, seçmenlerin %40’tan fazlasının göçmenlik ve egemenlik temalı kişiselleştirilmiş mesajlara maruz kaldığını ve bu mesajların oy tercihlerini etkilediğini ortaya koymuştur (John, Jennings & McLaren, 2020: 112–117). ESRC Brexit Diary Project ise bireysel anlatımlar üzerinden mikro-hedeflemenin seçmen algısındaki dönüşümünü detaylandırmıştır; katılımcılar dijital kampanya mesajlarının gündelik kaygılarını ve tutumlarını şekillendirdiğini ifade etmiştir (Taylor & Macmillan, 2019: 45–60). UK Data Service tarafından sağlanan veri setleri ise hedefli mesaj maruziyeti ile Brexit yanlısı oy oranları arasında anlamlı bir ilişki olduğunu göstermektedir (UK Data Service, 2023).

Bu dijital mikro-hedefleme ve algı yönetimi stratejilerinin seçmen davranışları üzerindeki etkisini daha iyi kavrayabilmek için, bölgelere göre Brexit referandumundaki

oy dağılımını gösteren tablo aşağıda sunulmuştur. Tablo, farklı bölgelerdeki sosyo-ekonomik yapılar ve demografik özelliklerin oy tercihlerindeki çeşitliliği ortaya koymakta ve dijital propaganda faaliyetlerinin yerel dinamiklerle nasıl etkileştiğini anlamamıza yardımcı olmaktadır (Goodwin & Heath, 2016: 323-332; Portes, 2016: 13-21)

Tablo 2. Bölgeye Göre Katılım, En Yüksekten En Düşüğe Doğru

Sayım Bölgesi	Kalsın Oyların %'si (Remain)	Ayrılsın Oyların %'si (Leave)	Katılım Oranı (% Seçmen)	Seçmen Sayısı
Güney Doğu	%48,2	%51,8	%76,7	6.465.404
Güney Batı ve Cebelitarık	%47,4	%52,6	%76,7	4.138.134
Doğu İngiltere	%43,5	%56,5	%75,7	4.398.796
Doğu Midlands	%41,2	%58,8	%74,1	3.384.299
Batı Midlands	%40,7	%59,3	%72,0	4.116.572
Galler	%47,5	%52,5	%71,7	2.270.272
Yorkshire ve Humber	%42,3	%57,7	%70,6	3.877.780
Kuzey Batı	%46,3	%53,7	%69,9	5.241.568
Londra	%59,9	%40,1	%69,6	5.424.768
Kuzey Doğu	%42,0	%58,0	%69,3	1.934.341
İskoçya	%62,0	%38,0	%67,2	3.987.112
Kuzey İrlanda	%55,8	%44,2	%62,7	1.260.955
Birleşik krallık	%48,1	%51,9	%72,2	46.500.001

Kaynak: Uberoi, E. (2016). European Union Referendum 2016, House of Commons Library, BRIEFING PAPER Number CBP 7639, 29 June 2016, ss. 24.

Tablo 2’de yer alan veriler doğrultusunda, 2016 Birleşik Krallık AB Referandumu sonuçları, bölgesel demografik ve ekonomik farklılıkların oy tercihleri üzerinde belirleyici olduğunu göstermektedir. Londra, yüksek göçmen nüfusu ve genç yaş grubu yoğunluğu sayesinde, eğitim, iş ve seyahat olanaklarına olan bağlılıkla %59,9 oranında Remain oyuna destek vermiştir (Uberoi, 2016: 24; ONS, 2018; Goodwin & Heath, 2016: 3). Güney Doğu, güçlü ekonomik yapısı ve yüksek istihdam oranlarıyla benzer şekilde Remain tercihinde öne çıkmıştır (ONS, 2017: 15). Bu durumun temel sebepleri arasında AB’nin serbest dolaşım hakkı sayesinde iş gücü piyasasının esnekliği, düşük ticaret maliyetleri ve geniş pazar erişimi yer almaktadır (Portes, 2016: 12). Güney Batı ve Cebelitarık, tarım ve turizm gibi sektörlere dayanan ekonomik yapısıyla %52,6 oranında Leave oyunu desteklediği görülmektedir. Bu bağlamda Güney

Batı bölgesinde ekonomik yapı, AB tarım sübvansiyonları ve turizm gelirleri nedeniyle karmaşık bir tercih oluşturmuştur; göçmenlerin iş piyasasında yarattığı rekabet korkusu Leave tercihini desteklemiştir (Centre for Cities, 2019: 7).

Doğu İngiltere’de üniversite şehirleri nedeniyle genç nüfusun orta düzeyde olmasına karşın, bölgedeki vasıfsız iş gücü yoğunluğu, düşük eğitim seviyesi ve mesleki becerilere sahip olmayan işçilerin imalat, depolama ve hizmet sektörlerinde yoğunlaşması anlamına gelmektedir (Blackaby & Drinkwater: 1 - 26). Bu tür işlerde çalışanlar genellikle iş güvencesizliği ve düşük ücretlerle karşı karşıya kalmakta, ekonomik belirsizlik nedeniyle AB üyeliğinin yerel iş olanaklarını azaltacağı ve göçmenlerin iş rekabetini artıracığı korkusuyla %56,5 oranında Leave tercihini desteklemektedirler (Portes, 2016: 10; Uberoi, 2016: 25).

Doğu Midlands ve Batı Midlands, yaşlanan nüfus ve sanayi sonrası ekonomik dönüşüm zorluklarıyla, sırasıyla %58,8 ve %59,3 oranlarında Leave tercihi göstermiştir (Portes, 2016: 14c; ONS, 2017: 22b). Kuzey Batı ve Kuzeydoğu, işsizliğin yüksek ve genç nüfus oranının orta seviyede olduğu bölgeler olarak, ekonomik güvencesizlik sebebiyle Leave oyu vermiştir (ONS, 2017: 18). Yorkshire ve Humber, sanayi geçmişinden kaynaklı ekonomik zayıflıklarla %57,7 Leave oyuna sahiptir (Portes, 2016: 13). Galler, işsizlik ve ekonomik çeşitlilik eksikliği nedeniyle %52,5 oranında Leave tercihi yapmıştır (Uberoi, 2016: 27). İskoçya ve Kuzey İrlanda ise nispeten daha genç ve istikrarlı nüfus profili ile Remain oylarını %62 ve %55,8 olarak korumuştur (Goodwin & Heath, 2016: 5).

Göçmen nüfusun yoğun olduğu bölgelerde, göçmenlerin AB vatandaşlığı avantajları nedeniyle Remain tercihi öne çıkarken, ekonomik güvencesizliğin yüksek olduğu yerlerde Leave oyları artmaktadır (Blackaby vd., 2020: 48). Genç nüfusun fazla olduğu bölgelerde AB’nin sunduğu fırsatlar daha çok benimsenmiş, bu da Remain oylarını artırmıştır (Hobolt, 2016: 9). Sosyal hizmetlerin yetersizliği ve gelir eşitsizliği gibi faktörler, birçok bölgede Leave tercihini desteklemiştir (Samson & Butler, 2017: 16). Brexit oyları, ekonomik, demografik ve kültürel faktörlerin karmaşık bir etkileşimi olarak ortaya çıkmaktadır (Clarke et al., 2017: 23). Uberoi’nin raporu da, bu ekonomik ve sosyal farklılıkların Leave tercihlerinde belirleyici olduğunu vurgulamaktadır (Uberoi, 2016: 28).

1.6. Brexit, Yapay Zeka ve Demokratik Düzen: Uluslararası Sistemdeki Yansımalar

Birleşik Krallık, Brexit referandumunu sonrası Cambridge Analytica skandalları gibi AI'nın demokratik süreçlerde yol açtığı tartışmalara rağmen, AI dışsallaştırmaktan uzak ve yenilikçi bir yaklaşım sergilemektedir (Woolley & Howard, 2019: 12). Bu yaklaşım, teknolojinin siyasal ve kamusal hayattaki potansiyelini dengeleyerek kontrollü biçimde kullanmayı amaçlamaktadır. Bu bağlamda, Birleşik Krallık'ta 2024 genel seçimlerinde Brighton Pavilion bölgesinde yarışan “AI Steve” adlı AI destekli avatar, seçim kampanyalarında AI'nın deneysel kullanımı olarak önemli bir örnek oluşturmuştur. AI Steve, seçmenlerle interaktif diyalog kurarak politika önerileri sunmayı hedeflemiş, ancak sınırlı bir başarı elde etmiştir (Hughes & Dahlström, 2020: 125). Bu deneyim, dijital propaganda ve AI'nın siyasi süreçlere etkisi üzerine yapılan çalışmalarla paralellik göstermektedir (Woolley & Howard, 2019: 14).

AI Steve gibi uygulamalar, AI'nın demokratik katılımı artırma potansiyelinin yanı sıra, etik ve hesap verebilirlik gibi önemli meseleleri de gündeme getirmiştir. İlginç bir şekilde, Arnavutluk'ta geliştirilen AI destekli dijital bakan “Diella” projesi, Birleşik Krallık'taki deneyimlerden esinlenerek kamu hizmetlerinde AI rolünü genişletmeyi amaçlamıştır (Albanian Government, 2025: 7). Diella, yolsuzlukla mücadele, şeffaflık ve kamu ihalelerinde adil uygulamaların sağlanması için tasarlanmış yenilikçi bir sistemdir ve bürokratik süreçlerin dijitalleşmesini hızlandırmaktadır (Microsoft, 2025: 14).

Birleşik Krallık ise, sadece seçim süreçlerinde değil, kamu yönetiminin farklı alanlarında da AI teknolojilerini etkin biçimde kullanmaktadır. “Humphrey” ve “Caddy” gibi AI destekli araçlar, kamu belgelerinin analiz edilmesi, özetlenmesi ve vatandaşlara danışmanlık sağlanması gibi görevlerde kamu görevlilerinin iş yükünü azaltmaktadır. Humphrey, doğal dil işleme algoritmaları kullanarak büyük metinleri anlamlandırmakta ve karar alma süreçlerini hızlandırmaktadır (UK Government Digital Service, 2023: 21). Caddy ise, vatandaşların sıkça sorduğu sorulara cevap verip, kamu hizmetlerine erişimi kolaylaştıran interaktif bir AI sohbet botudur (Public Sector AI Review, 2022: 16). Bu uygulamalar, bürokratik işlemlerin hızlanmasına ve vatandaş memnuniyetinin artmasına katkı sağlamaktadır (OECD, 2021: 45).

Aynı zamanda İngiltere hükümeti, kamu sektöründe yeniliği teşvik etmek amacıyla “Açık Kaynak AI Burs Programı”nı başlatmıştır. Program, AI mühendislerinin kamu kurumlarında açık kaynak kodlu çözümler geliştirmesini ve böylece kamu yönetiminde AI uygulamalarının yaygınlaşmasını sağlamayı hedeflemektedir (UK AI Council, 2023: 10). Diğer yandan, kamu çalışanlarının AI etik ve sorumlu biçimde kullanabilmesi için hazırlanan “Yapay Zeka Oyun Kitabı”(AI Playbook) ise, kamu görevlilerine rehberlik eden kritik bir kaynaktır (UK Cabinet Office, 2022: 7). Bu döküman, şeffaflık ve hesap verebilirlik ilkelerini vurgulayarak kamu sektöründe AI’nın doğru kullanılmasını teşvik etmektedir. AI Playbook, AI perspektifinde yaşam döngüsünün yönetimi, risk değerlendirmeleri ve insan kontrolünün korunması gibi kritik konulara odaklanarak kamu görevlilerinin bilinçli kararlar almasına rehberlik eder (Jobin, Ienca & Vayena, 2019: 5).

İngiltere’nin AI Playbook’u, kamu politikalarının dijitalleşmesinde AI uygulamalarının güvenli ve etkin entegrasyonunu sağlamak için somut bir örnek teşkil etmektedir (UK Government Digital Service, 2021). Bu bağlamda, etik AI kullanımını teşvik eden rehberlerin, devletlerin dijital dönüşüm stratejilerinde kritik bir rol oynadığı vurgulanmaktadır (Whittaker et al., 2018: 102).

Ayrıca bir diğer proje olan, “Yapay Zeka Topluluğu” (AI Community of Practice) isimli platform, kamu yönetiminde AI projelerinin deneyim edilmesi, bilgi alışverişi ve iş birliğini artırmayı amaçlamaktadır (AI Public Sector Network, 2023: 5). Bu platform, proje paylaşımlarının yanı sıra en iyi uygulamaların, zorlukların ve yenilikçi çözümlerin tartışıldığı bir alan sunarak, kamu yönetiminde AI entegrasyonunun yaygınlaşmasını teşvik etmektedir ve aynı zamanda kamu çalışanlarının AI konusunda bilgi ve becerilerini artırmaya yönelik eğitim ve atölye çalışmaları organize etmekte, böylece dijital dönüşüm süreçlerinin insan kaynağı boyutunu güçlendirmektedir (Digital Government Institute, 2021).

Bu gelişmelerin ülke sistemi üzerindeki etkileri çok yönlüdür. Kamu yönetiminde verimlilik ve şeffaflığın artması, devlet mekanizmalarının etkinliğini artırmakta ve vatandaşların devlete olan güvenini yükseltmektedir (European Commission, 2022: 18). AI’nın bürokratik süreçleri hızlandırması, kamu hizmetlerinin kalitesini artırmakta ve vatandaşların daha hızlı hizmet almasını sağlamaktadır (OECD,

2021: 53). Öte yandan, seçimlerde ve kamu hizmetlerinde AI'nın kullanılması demokratik katılımın yeni yollarla genişlemesine imkân tanımakta, ancak etik, hesap verebilirlik ve veri gizliliği gibi önemli meseleleri de beraberinde getirmektedir (Tufekci, 2018: 10). AI teknolojilerinin kamu alanındaki yaygınlaşması, devlet yönetim sistemlerinde belirgin bir evrimi işaret etmektedir. Geleneksel bürokrasi yapıları daha esnek, veri odaklı ve hızlı karar alan sistemlere dönüşmektedir (Margetts & Dorobantu, 2019: 610). AI destekli karar alma süreçleri, insan kaynaklı sınırlamaları azaltarak kamu politikalarının etkinliğini artırmaktadır (Kroll et al., 2017: 11). Bu dönüşüm, hukuki ve etik düzenlemelerin güncellenmesini zorunlu kılarak modern devlet anlayışının yeniden tanımlanmasına öncülük etmektedir (Cath et al., 2018: 517).

Bunun yanı sıra, uluslararası güç dengesi bağlamında AI, devletlerin rekabetinde stratejik bir faktör olarak öne çıkmaktadır. AI teknolojileri ulusal güvenlik ve dış politika stratejilerinin merkezinde yer almakta, devletler arası güç dengesini önemli ölçüde değiştirmektedir (Horowitz, 2018: 36). Bu bağlamda, Birleşik Krallık'ın AI üzerine yaptığı yatırımlar, sadece iç kamu yönetimi için değil, aynı zamanda küresel arenadaki konumunun güçlendirilmesi için de kritik öneme sahiptir.

AI destekli sistemler, istihbarat, siber güvenlik ve diplomasi alanlarında kullanılarak, Birleşik Krallık'ın uluslararası rekabette avantaj sağlamasına katkıda bulunmaktadır (Nye, 2011: 53; Webb, 2019: 142). Görüldüğü üzere bu teknolojilerin küresel düzeydeki etkisi, devletlerin iç işleyişini dönüştürmenin yanı sıra uluslararası ilişkilerin dinamiklerini de derinden değiştirmektedir. “*AI and Diplomacy: International Relations in the Age of Disruptive Technologies*” (SELA, 2024)'in Herrera tarafından yazılmış bölümü olan rapor, AI alanının kamu diplomasisinde yeni iletişim stratejileri ve algoritmik içerik önerileri aracılığıyla devletlerin küresel arenadaki imajlarını güçlendirdiğini ve diplomasi süreçlerini yeniden şekillendirdiğini vurgulamaktadır (Herrera, 2024: 45).

Dominik Cumhuriyeti'nin kariyer diplomatı Manuel Morales Lama da AI'nın, hedef kitleye yönelik kişiselleştirilmiş içerik üretimi ve etkileşim stratejileriyle ülkelerin değer ve çıkarlarını daha etkili yansıtmasına olanak sağladığını ifade etmektedir (Morales Lama, 2023: 10). Buna ek olarak, AI uluslararası güvenlik ve kriz yönetimi alanlarında karar destek sistemleri sunarak devletlerin hızlı ve etkili müdahale

kapasitelerini arttırmaktadır (Zhang & Chen, 2023: 123). Kamu çalışanları da, AI destekli veri analizi ve risk yönetimi araçlarını kullanarak, krizlere daha hızlı ve bilinçli müdahale etme yeteneklerini geliştirmekte; böylece devletlerin diplomatik süreçlerdeki etkinliği artmaktadır (Herrera, 2024: 46). Ancak, bu teknolojinin etik karar alma süreçlerine tam entegre edilememesi, siber güvenlik tehditleri ve uluslararası düzenlemelerdeki eksiklikler gibi zorluklar, uluslararası ilişkilerde önemli riskler yaratmaktadır. Bu bağlamda, AI'nın şeffaf, etik ve hesap verebilir bir şekilde kullanılması, demokratik değerlerin korunması için devlet politikalarının sürekli gözden geçirilmesi gerekmektedir (Herrera, 2024: 50).



SONUÇ

Dijitalleşme çağında AI ve akıllı algoritmalar, uluslararası sistemin işleyişini çok katmanlı biçimlerde etkileyerek, siyasal yapıların ve karar alma süreçlerinin dönüşümünü derinleştirmektedir. Brexit süreci özelinde gerçekleştirilen vaka analizi, AI destekli algoritmaların salt teknik araçlar olmaktan çıkarak siyasal süreçlerin doğrudan şekillendirilmesinde etkin ve belirleyici güç unsurları haline geldiğini göstermeye gayret etmiştir. Cambridge Analytica gibi aktörlerin sosyal medya ve büyük veri analizlerini kullanarak seçmenlerin psikolojik profillerine yönelik kişiselleştirilmiş mesajlar iletmesi, dijital mikro-hedefleme ve algı yönetimi stratejilerinde yeni bir paradigma oluşturmuştur. Bu stratejiler, sadece geniş demografik kategorilere değil, aynı zamanda bireylerin psikolojik eğilimleri ve duygusal hassasiyetlerine göre hedeflemeyi mümkün kılarak seçmen davranışlarının öngörülebilirliğini önemli ölçüde artırmıştır. Burada algoritmaların kişisel veri üzerinden oluşturduğu dijital profillemeye, siyasal iradeyi yalnızca etkilemekle kalmamış; bireysel karar alma süreçlerini yönlendiren ve manipüle eden bir araç işlevi görmüştür.

Nitekim, 2016 Birleşik Krallık AB Referandumu'nda "Leave" oylarının yüksek olduğu Doğu Midlands (%58,8) ve Batı Midlands (%59,3) gibi bölgeler, sosyo-ekonomik açıdan kırılgan nüfuslara ve göçmen karşıtı duyguların yoğun olduğu alanlara işaret etmektedir. Bu bölgelerde mikro-hedefleme yoluyla uygulanan mesajlaşma stratejileri, dijital propaganda faaliyetlerinin yerel dinamiklerle nasıl iç içe geçtiğini göstermektedir. Özellikle düşük eğitim seviyesi, ekonomik güvencesizlik ve vasıfsız iş gücünün yoğun olduğu bu bölgelerde, AI destekli iletişim yöntemleri korkuya, belirsizliğe ve aidiyet krizine dayalı kampanya söylemleriyle birleşerek seçmen tercihlerinde belirleyici olmuştur. Buna karşın, göçmen nüfusun yoğun, genç yaş grubunun baskın ve yüksek eğitim seviyesine sahip bireylerin yoğun olduğu Londra gibi bölgelerde %59,9 oranında "Remain" oyu çıkması, aynı tekniklerin farklı demografik yapılarda farklı karşılıklar bulduğunu ortaya koymaktadır.

Bu durum, yalnızca teknolojik araçların etkinliğiyle değil; bu araçların içine yerleştirildiği sosyal, kültürel ve ekonomik bağlamlarla birlikte anlaşılmalıdır. Algoritmaların mesaj içeriğini yerel hassasiyetlere göre uyarlayabilme kapasitesi, onları geleneksel propaganda yöntemlerinden ayırmakta; böylece seçmen davranışları veri

odaklı, bireyselleştirilmiş ve duygusal olarak manipüle edilebilir hale gelmektedir. Bu bağlamda, siyasal iletişim süreçlerinde yaşanan dönüşüm yalnızca teknik değil, aynı zamanda etik, hukuki ve toplumsal düzeyde de derin sonuçlar doğurmaktadır.

Öte yandan, AB tarafından kabul edilen AI Yasası gibi düzenlemeler, AI uygulamalarını risk düzeylerine göre sınıflandırmakta; bu sistemler, kabul edilemez, yüksek, sınırlı ve asgari risk olmak üzere dört ana kategoriye ayrılmaktadır. Yüksek riskli sistemler sıkı denetime tabi tutulurken, sınırlı risk grubundaki uygulamalar için yalnızca şeffaflık ve kullanıcı bilgilendirme yükümlülükleri öngörülmekte; asgari risk grubundaki teknolojilere ise herhangi bir yasal kısıtlama getirilmemektedir. Bu çerçevede, özellikle “kabul edilemez” olarak tanımlanan sistemlerin örneğin sosyal skorlama, davranış manipülasyonu ve gerçek zamanlı biyometrik tanıma gibi doğrudan yasaklanması, dijital araçların siyasal süreçlerdeki etkisine yönelik artan farkındalığın açık bir göstergesidir. Ancak, sınırlı risk kategorisinde yer alan teknolojilere yalnızca yumuşak düzenlemelerle (örneğin şeffaflık yükümlülüğü) müdahale edilmesi, bu sistemlerin potansiyel olarak doğrudan ve derin etkileri karşısında yetersiz kalmaktadır. Brexit örneğinde olduğu gibi, bu tür düzenleyici boşluklar veya zayıflıklar, uzun vadede demokratik meşruiyetin aşınmasına yol açabilmektedir.

AI ile dijitalleşme siyasal düzenin ve ekonomik yapılarının dönüşümünü radikal düzeyde gerçekleştirmektedir. Geleneksel medya araçlarının yerini dijital platformların aldığı bu süreçte, seçmenlere doğrudan ve kişiselleştirilmiş şekilde ulaşılması, siyasal kampanyaların yapısını kökten değiştirmiştir. Sosyal medya platformları üzerinden yürütülen hedefli kampanyalar, geleneksel siyasal elitlerin konumunu zayıflatırken, algoritmik araçlara sahip olan aktörlerin etkisini artırmıştır. Özellikle mikro-hedefleme yöntemlerinin ekonomik kaygıları olan seçmen grupları üzerindeki etkisi, güç dengelerinin teknolojik kapasiteye dayalı olarak yeniden şekillendiğini göstermektedir.

Araştırma, AI destekli algoritmaların uluslararası ilişkilerde devletlerin stratejik tercihlerinde ve güç dengelerinde belirleyici bir rol oynadığını da göstermektedir. Brexit yalnızca iç politika dinamikleriyle değil, aynı zamanda Birleşik Krallık’ın AB’den ayrılarak uluslararası konumunu yeniden tanımladığı bir dönüşüm sürecidir. AI destekli analiz araçları ve algoritmik propaganda teknikleri, bu tercihin şekillenmesinde stratejik bir rol oynamıştır. Özellikle veri analitiği yoluyla seçmen psikolojisinin

yönlendirilmesi, yalnızca seçim sonuçlarını değil, aynı zamanda Birleşik Krallık'ın dış politika pozisyonunu da dönüştürmüştür. Brexit sonrası oluşan jeopolitik denge değişiklikleri, algoritmik araçların uluslararası düzeyde stratejik etkilerini ortaya koymaktadır.

Ayrıca, dijital manipülasyon ve kişisel veri üzerinden yürütülen kampanyaların demokratik süreçlerin şeffaflığını ve meşruiyetini zayıflattığını göstermektedir. Cambridge Analytica örneğinde görüldüğü üzere, kişisel verilerin rıza dışı şekilde kullanılması ve manipülatif içeriklerle seçmen davranışlarının yönlendirilmesi, demokratik normlar açısından ciddi sorunlara yol açmıştır. Seçim kampanyalarının şeffaf olmaması, algoritmaların hesap veremezliği ve yanlış bilginin yayılması, demokratik süreçlerin güvenilirliğini zayıflatmıştır. AB AI Yasası kapsamında ‘‘kabul edilemez risk’’ kategorisine giren uygulamaların davranış manipülasyonu ve sosyal skorlama gibi yaygın şekilde kullanılması, bu tehdidin ciddiyetini gözler önüne sermektedir.

Aynı zamanda, ulus-devletlerin bu dönüşüm karşısında yeni güvenlik politikaları geliştirerek AI temelli tehditlere karşı stratejik uyum sağlama çabaları da gözlemlenmiştir. AB'nin AI Yasası ve GDPR gibi düzenlemeleri bu bağlamda önemli girişimlerdir. Ancak uygulamada bu düzenlemelerin kapsamı ve etkinliği sınırlı kalmakta, küresel düzeyde tutarlı bir dijital güvenlik politikası oluşturulamadığı görülmektedir. Brexit sonrası İngiltere'nin kendi veri koruma rejimini oluşturma süreci, bu uyum arayışının parçalı ve bölgesel nitelikte olduğunu göstermektedir.

Çalışma, algoritmik müdahalelerin bireylerin siyasi karar alma süreçlerine gizli müdahaleler yaparak özgür iradenin sınırlarını dolaylı biçimde yönlendirdiğini de doğrulamaktadır. AI ve algoritmik araçların sunduğu kişiselleştirilmiş mesajlar, bireylerin seçim kararlarını doğrudan etkilemekte, hatta çoğu durumda manipüle etmektedir. Özellikle psikometrik analizler ile bireyin korkuları, değerleri ve zaafları üzerinden kurgulanan mesajlar, bireyin kendi tercihleriyle hareket ettiği yanılsamasını yaratmakta, ancak özgür irade üzerinde doğrudan yönlendirici bir etki yaratmaktadır. Bu durum, siyasi karar alma süreçlerini etik ve felsefî açıdan da sorgulanabilir hâle getirmektedir.

Sonuç olarak, bu çalışma AI ve dijital algoritmaların yalnızca teknik gelişmeler olmadığını, siyasal karar alma süreçlerine doğrudan müdahale edebilecek kadar güçlü, yönlendirici ve dönüştürücü unsurlar hâline geldiğini göstermiştir. Brexit örneği üzerinden yapılan değerlendirme, dijital propaganda araçlarının yerel sosyo-ekonomik dinamiklerle nasıl bütünleşerek seçmen davranışlarını etkilediğini ortaya koymuş; bu etki biçimlerinin ulus-devletlerin dış politika tercihleri ve uluslararası konumlanmaları üzerinde dahi belirleyici olabileceğini kanıtlamıştır. Bulgular, AI destekli algoritmaların yalnızca iç politika dinamiklerinde değil, uluslararası düzeyde stratejik pozisyonlanmalar üzerinde de etkili olduğunu açıkça göstermektedir.

Ayrıca, araştırma AI destekli algoritmaların klasik siyasal kuramların ötesinde, yeni bir dijital güç siyaseti inşa ettiğini ve uluslararası ilişkilerin doğasını yeniden tanımladığını ortaya koymaktadır. Algoritmik karar destek sistemleri, diplomatik hamlelerden ekonomik önceliklere kadar birçok stratejik tercihin yönünü etkileyebilmektedir. Bu durum, sadece teknolojik bir evrimi değil, aynı zamanda uluslararası sistemin aktörleri arasındaki güç dağılımının yeniden inşa edildiği bir geçiş sürecini işaret etmektedir.

Çalışma, yalnızca mevcut sorunları teşhis etmekle kalmayıp, ulusal ve uluslararası düzeyde geliştirilecek etik, hukuki ve yönetsel çerçevelerin gerekliliğine de işaret etmektedir. AB'nin AI Yasası ile risk temelli bir sınıflandırma sistemi oluşturması, ulus-devletlerin dijitalleşmenin getirdiği güvenlik, şeffaflık ve meşruiyet sorunlarına yönelik yanıt üretmeye başladığını göstermektedir. Ancak bu düzenlemelerin hâlâ parçalı, sınırlı ve uygulamada yetersiz kaldığı görülmektedir. Elde edilen bulgular, teknolojik ilerlemenin yönünün rastlantısal olmayıp, politik çerçeveye doğrudan bağlantılı ve karşılıklı etkileşim içerisinde şekillendiğini güçlü biçimde desteklemektedir. Bu bağlamda, gelecekte dijital teknolojilerin demokratik değerlerle uyum içinde evrilmesi, yalnızca bu araçların nasıl geliştirildiği değil, kimin kontrolünde olduğu ve hangi amaçlarla kullanıldığı sorularına verilen yanıtlarla şekillenecektir. Bulgular, dijital çağda siyasal şeffaflık, etik hesap verebilirlik ve hukuki düzenlemelerin önemini güçlü biçimde ortaya koymaktadır.

KAYNAKÇA

- Acemoğlu, D. (2024). Power and progress: Our thousand-year struggle over technology and prosperity. Crown Publishing Group.
- ACEMOĞLU, D. & blac, J. (2012). Why Nations Fail: The Origins of Power, Prosperity, and Poverty. New York: Crown Business, ss. 45–67.
- Addis, M., & Kutar, M. (2018). “GDPR and emerging technologies: A UK perspective”. UKAIS Conference Proceedings, 19-21. “Çevrimiçi” <https://aisel.aisnet.org/ukais2018/28>, Erişim:02/08/2025.
- AKILLI, E. (2025, April 18). “Rewiring diplomacy in the technopolar world”. SETA Opinion. “Çevrimiçi” <https://www.setav.org/en/rewiring-diplomacy-in-the-technopolar-world> Erişim: 12.08.2025.
- ALBANIAN GOVERNMENT. (2025). “Diella: Yapay zeka destekli dijital bakan projesi.” Tiran. “Çevrimiçi” <https://www.kryeministria.al/newsroom/diella> Erişim: 20.08.2025
- Allam, Z., & Newman, P. (2018). “Cities and the digital revolution: Aligning technology and humanity”. Springer International Publishing.
- ALLCOTT, H. & GENTZKOW, M. (2017). “Social Media and Fake News in the 2016 Election”, Journal of Economic Perspectives, Vol. 31, No. 2, ss. 211–236. “Çevrimiçi” <https://www.aeaweb.org/articles?id=10.1257/jep.31.2.211> Erişim: 21.09.2025.
- Allison, G. (2020). “Destined for War: Can America and China Escape Thucydides’s Trap?” Houghton Mifflin Harcourt.
- Altman, R. (2019). “Artificial Intelligence and International Security”. Oxford University Press.

- Anstead, N. (2017). Data-driven campaigning in the 2015 UK general election. *Internet Policy Review*, 6(4), ss. 1–19, “Çevrimiçi” <https://doi.org/10.14763/2017.4.777>, Erişim: 10/05/2025.
- Anstead, N. (2017). Predictive analytics and political campaigning: The rise of machine learning in elections. *Journal of Political Marketing*, 16(1), ss. 25-40, “Çevrimiçi” <https://doi.org/10.1080/15377857.2016.1247841> Erişim: 08/05/2025
- ARANÍBAR, R. (2024). “Veri Egemenliği ve Diplomasi İçinde Yapay Zeka ve Diplomasi Raporu”, ss. 9–15. *Latin American and Caribbean Economic System (SELA), Rapor*. “Çevrimiçi” <https://www.sela.org/> Erişim: 04.09.2025.
- ARCHER, T. (2021). “Brexit and the Cultural Politics of Populism”. *Journal of Contemporary European Studies*, Vol. 29, No. 1, ss. 24.
- Aslan, M. – Yıldız, A.A. (2021) “Yapay Zeka’nın Uluslararası İlişkiler Alanında Yarattığı Değişimler”, *Üçüncü Sektör Sosyal Ekonomi Dergisi*, 56(4), 2401-2416.
- Atmaca, Y., & Karaçay, F. (2020). “TÜRKİYE’DEKİ KAMU YÖNETİMİ REFORMLARINDA DİJİTALLEŞME VE E-YÖNETİŞİM”. *International Journal of Management and Administration*, 4(8), 260-280. “Çevrimiçi” <https://doi.org/10.29064/ijma.779263>, Erişim: 05/10/2025.
- Avundukluoğlu, B. (2020). “Dijitalleşme ve kamu hizmetlerinde yapay zeka: Etkinlik ve katılımcılık”. *Dijitalleşmenin Birey ve Toplum Üzerindeki Hegemonyası: Dijital Hegemonya*, 794.
- Bartholomew, C., Borochoff, B., Cleveland, R., Fiedler, J., Friedberg, A., Goodwin, C. P., Mann, J., Schriver, R., Scissors, D., & Wessel, M. R. (2022). “U.S.-China Economic and Security Review Commission”, 2022 Annual Report to Congress. “Çevrimiçi” https://www.uscc.gov/sites/default/files/2022-11/2022_Annual_Report_to_Congress.pdf, Erişim: 02/06/2025.

- Balel, C. (2024). “Savaş Haberlerinin Bir Propaganda Aracı Olarak Kullanımına İlişkin Eleştirel Bir Çalışma: 2003 Irak Savaşı Örneği”. *Florya Chronicles of Political Economy*, 10(1), 37–68.
- Barocas, S., & Selbst, A. D. (2016). Big data's disparate impact. *California Law Review*, 104(3), ss. 671–732, “Çevrimiçi”
<https://doi.org/10.2139/ssrn.2477899>, Erişim: 10/04/2025.
- Ben-Israel, I., & Matania, E. (2020). “Harnessing innovation: Israeli perspectives on AI ethics, governance and national security (report for CAHAI / Institute for National Security Studies)”. Institute for National Security Studies.
- Benkler, Y., Faris, R., & Roberts, H. (2018). “Network Propaganda: Manipulation, Disinformation, and Radicalization in American Politics”. Oxford University Press.
- Bennett, C. J. (2018). *The privacy advocates: Resisting the spread of surveillance*. MIT Press.
- Bennett, C. J., & Lyon, D. (2019). “Data-driven political campaigns and democracy: Ethical challenges and regulatory frameworks”. *Journal of Information Ethics*, 28(1), 10-18.
- Bennett, C. J., & Raab, C. D. (2006). *The Governance of Privacy: Policy Instruments in Global Perspective*. MIT Press.
- Bennett, W. L. (2018) “Algorithms, automation, and politics: The rise of computational propaganda”, *Journal of Communication*, 68(2), ss. 40-50, “Çevrimiçi”
<https://doi.org/10.1093/joc/jqy003>, Erişim: 11/04/2025.
- Berners-Lee, T. (1999). “Weaving the Web: The original design and ultimate destiny of the World Wide Web by its inventor”. HarperSanFrancisco.
- Biddle, S. (2021). “Nonstate Warfare: The Military Methods of Guerillas, Warlords, and Militias”. Princeton University Press.

- Binnendijk, A., Marler, P. & Bartels, E. (2020). Artificial Intelligence and Open-Source Intelligence: Enhancing Security through Data Analytics. RAND Corporation, ss. 38.
- Binns, R. (2018). “Fairness in machine learning: Lessons from political philosophy”. Proceedings of the 2018 Conference on Fairness, Accountability, and Transparency, 149-159.
- Blackaby, D. H., & Drinkwater, S. (2004). “Migration and labour market differences: The case of Wales” (IZA Discussion Paper No. 1275, ss. 1 - 26). Institute for the Study of Labor (IZA).
- Blaszczyk, M., Popovic, M., Zajdel, K., & Zajdel, R. (2023). Implications of the COVID-19 pandemic on the organization of remote work in IT companies: The managers’ perspective. Sustainability, 15(15), 12049. “Çevrimiçi” <https://doi.org/10.3390/su151512049>, Erişim: 04/08/2025.
- Bodo, B., Helberger, N., & de Vreese, C. H. (2017). “Political micro-targeting: a Manchurian candidate or just a dark horse? Internet Policy Review”, 6(4). “Çevrimiçi” <https://doi.org/10.14763/2017.4.776> Erişim: 05.10.2025.
- BRADSHAW, S.; NEUDERT, L.-M.; HOWARD, P. N., (2018) “Government Responses to Malicious Use of Social Media”, Riga, NATO STRATCOM COE. “Çevrimiçi” [Nato-Report.pdf](#) Erişim: 5.10.2025.
- Bradshaw, S., & Howard, P. N. (2019). “The Global Disinformation Order: 2019 Global Inventory of Organised Social Media Manipulation”. Oxford Internet Institute. “Çevrimiçi” <https://demtech.oii.ox.ac.uk/wp-content/uploads/sites/12/2019/09/CyberTroop-Report19.pdf> Erişim:05.10.2025.
- BROWN, T. & NGUYEN, H. (2021). “Digital Disinformation and Electoral Integrity in Australia”. Australian Journal of Politics and History, Vol. 67, No. 1, ss. 89.

- Bryson, J. J. & Theodorou, A. (2021) ‘‘AI and International Relations: The Use of Simulation in Foreign Policy’’ Cambridge: Cambridge University Press, ss. 17.
- Buğra, A. (2005). ‘‘Türkiye’de yeni kapitalizm: Devlet, piyasa ve sınıf’’. İletişim Yayınları.
- BURROWS, M. & MUELLER KALER, J. (2021). ‘‘Smart Partnerships Amid Great Power Competition’’, Atlantic Council Report ‘‘Çevrimiçi’’
<https://www.atlanticcouncil.org/in-depth-research-reports/report/smart-partnerships-amid-great-power-competition/> Erişim: 21.09.2025.
- CADWALLADR, C. (2019). The Cambridge Analytica Files. London: Guardian Books, ss. 215.
- CADWALLADR, C. & GRAHAM-HARRISON, E. (2018). ‘‘Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach’’. The Guardian, 17 Mart 2018, ss. 112. ‘‘Çevrimiçi’’
<https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election>, Erişim: 14/07/2025
- Cafarella, M., Halevy, A., Noy, N. & Widom, J. (2019) ‘‘Data-driven Diplomacy: Harnessing Big Data for Foreign Policy’’ Stanford: Stanford University Press, ss. 4.
- CALO, R. (2015). ‘‘Robotics and the Lessons of Cyberlaw’’, California Law Review, Vol. 103, No. 3, ss. 405–458 ‘‘Çevrimiçi’’
<https://scholarship.law.berkeley.edu/californialawreview/vol103/iss3/2/> Erişim: 21.09.2025.
- Carnegie Endowment for International Peace. (2024, Temmuz 24). ‘‘France’s AI Summit Is a Chance to Reshape Global Narrative’’. ‘‘Çevrimiçi’’
<https://carnegieendowment.org/posts/2024/07/france-ai-summit-reshape-global-narrative?lang=en>, Erişim: 14/07/225.
- Catells, M. (2010). ‘‘Communication Power’’. Oxford University Press.

- Cath, C., Wachter, S., Mittelstadt, B., Taddeo, M., & Floridi, L. (2018) “Artificial intelligence and the ‘good society’”: The US, EU, and UK approach. *Science and Engineering Ethics*, 24(2), “Çevrimiçi” 505–528.
<https://doi.org/10.1007/s11948-017-9901-7> Erişim: 14.07.2025.
- Cath, C. (2018). “Governing artificial intelligence: Ethical, legal and technical opportunities and challenges.” *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 376(2133), 20180080.
“Çevrimiçi” <https://doi.org/10.1098/rsta.2018.0080> Erişim: 20/08/2025
- Centre for Cities. (2019). “Cities Outlook 2019”. “Çevrimiçi”
<https://www.centreforcities.org/wp-content/uploads/2019/01/19-01-28-Cities-Outlook-2019>, Erişim: 28/08/2025.
- Chadwick, A. (2017) “The Hybrid Media System: Politics and Power”, Oxford University Press.
- Chandler, D. and Fuchs, C. (eds.) 2019. “Digital Objects, Digital Subjects: Interdisciplinary Perspectives on Capitalism, Labour and Politics in the Age of Big Data”. London: University of Westminster Press, License: CC-BY-NC-ND 4.0, “Çevrimiçi” <https://doi.org/10.16997/book29>, Erişim: 05/10/2025.
- CHANNEL 4 NEWS (2018) “Cambridge Analytica Uncovered: Secret filming reveals election tricks”, “Çevrimiçi” <https://www.channel4.com/news/cambridge-analytica-uncovered-secret-filming-reveals-election-tricks> Erişim: 15.07.2025.
- Chesney, R., & Citron, D. K. (2019). “Deep fakes: A looming challenge for privacy, democracy, and national security”. *California Law Review*, 107, 1753–1819.
“Çevrimiçi” <https://doi.org/10.2139/ssrn.3213954>, Erişim: 02/08/2025.
- CLARKE, H., GOODWIN, M. & WHITELEY, P. (2017). *Brexit: Why Britain Voted to Leave the European Union*. Cambridge: Cambridge University Press, ss. 45–53.

CLOAREC, J. (2021). “Narrating Brexit: Media, Culture and Identity”. *European Journal of Cultural Studies*, Vol. 24, No. 1, ss. 6.

COE, J. (2018). *Middle England*. London: Viking, ss. 123.

Ditter, (2025). “PRC Concepts for UAV Swarms in Future Warfare”. CNA.
“Çevrimiçi” <https://www.cna.org/reports/2025/07/PRC-Concepts-for-UAV-Swarms-in-Future-Warfare.pdf>, Erişim: 05/06/2025.

Copeland, B. J. (2015). “Artificial Intelligence: A Philosophical Introduction”.
Cambridge: Polity Press.

CRAWFORD, K. (2021). “Atlas of AI: Power, Politics, and the Planetary Costs of Artificial Intelligence New Haven”, Yale University Press, ss. 186.

Cummings, M. L. (2020). “Artificial intelligence and international security.” Chatham House.

CURTICE, J. (2017). “Why Leave Won the UK’s EU Referendum”. *Journal of Common Market Studies*, Vol. 55, No. S1, ss. 112–113.

Çifçi, O. (2024). “Güvenlik Paradigmasının Dönüşümü ve 21. Yüzyılda Uluslararası Güvenliğin Yeni Gündemi”. *Liberal Düşünce Dergisi*, 29(113), 143–170.
“Çevrimiçi” <https://doi.org/10.36484/liberal.1335666>, Erişim: 05/10/2025.

Danaher, J. (2016). “The threat of algocracy: Reality, resistance and accommodation”. *Philosophy & Technology*, 29(3), 245–268. “Çevrimiçi”
<https://doi.org/10.1007/s13347-015-0211-1>, Erişim: 18/07/025.

Danks, D., & London, A. J. (2017). “Algorithmic bias in autonomous systems”. *Proceedings of the 26th International Joint Conference on Artificial Intelligence*, 4691 - 4697.

- Darıcı, A. (2020) “Yapay Zeka ve Uluslararası Güvenlik: Fırsatlar ve Riskler”
Uluslararası İlişkiler Dergisi, 17(66), ss. 67.
- Dastin, J. (2018). “Amazon scraps secret AI recruiting tool that showed bias against women”. Reuters. “Çevrimiçi” <https://www.reuters.com/article/us-amazon-com-jobs-automation-insight-idUSKCN1MK08G>, Erişim: 14/08/2025.
- De Filippi, P., & Wright, A. (2018). “Blockchain and the law: The rule of code”.
Harvard University Press.
- DEL VICARIO, M., BESSI, A., ZOLLO, F., PETRONI, F., SCALA, A.,
CALDARELLI, G., STANLEY, H. E. & QUATTROCIOCCHI, W. (2016).
“The spreading of misinformation online”, Proceedings of the National Academy of
Sciences (PNAS), Vol. 113, No. 3, ss. 554–559. “Çevrimiçi”
<https://www.pnas.org/doi/10.1073/pnas.1517441113> Erişim: 02.08.2025.
- Demir, C. (2025). “Kalkınmanın iktisadi, sosyal ve kültürel boyutlarında yapay zeka”.
Pamukkale Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, 36(2), 215–230.
- Diakopoulos, N. (2016). “Accountable algorithms.” Communications of the ACM,
59(2), 56–62. “Çevrimiçi” <https://doi.org/10.1145/2844110> Erişim:
02/08/2025
- Doshi-Velez, F., & Kim, B. (2017) “Towards a rigorous science of interpretable
machine learning”, “Çevrimiçi” <https://doi.org/10.48550/arXiv.1702.08608>,
Erişim: 05/04/2025.
- EICK, S. A., (2022) The Political and Aesthetic Productivity of Shakespearean
Ambiguity in Brexit Discourse, Anglistik, Jahrgang 33 (2022), Ausgabe 2,
Heidelberg, Universitätsverlag WINTER GmbH.
- ELECTORAL COMMISSION (2016). “EU Referendum Results”. “Çevrimiçi”
<https://www.electoralcommission.org.uk/who-we-are-and-what-we->

do/elections-and-referendums/past-elections-and-referendums/eu-referendum/results-and-turnout Eriřim: 01.09.2025

EPSTEIN, R. (2001). “The Democracy of Data: Political Communication in the Digital Age”. New Media & Society, Vol. 3, No. 1, ss. 42.

Erol, A. (2024). “Yapay zeka ve kamu ynetimi: Hizmetlerin etkinlik ve maliyet optimizasyonu” Yapay Zekanın Kamu Ynetimine Etkisi, “evrimii” <https://dergipark.org.tr/en/download/article-file/3898555> Eriřim: 10/08/2025

EVANS, G. & MELLON, J. (2019). “The Political Divide: Brexit, Class and Culture in the UK”. British Journal of Sociology, Vol. 70, No. 1, ss. 88–90.

Eubanks, V. (2018). “Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor”. St. Martin’s Press.

EUROPEAN COMMISSION (2018). “Impact of the Cambridge Analytica Case on Data Protection and Democracy”. Brussels, European Union, ss. 48
“evrimii” https://commission.europa.eu/law/law-topic/data-protection/reform/impact_en, Eriřim: 21/07/2025.

European Union (2016). “General Data Protection Regulation (GDPR). Regulation (EU) 2016/679 of the European Parliament and of the Council”, “evrimii” <https://eur-lex.europa.eu/eli/reg/2016/679/> Eriřim: 10.07.2025.

Farid, H. (2019). “Photo Forensics and Artificial Intelligence: Detecting Deepfakes”. MIT Press.

Floridi, L., & Cowls, J. (2019). “A unified framework of five principles for AI in society”. Harvard Data Science Review, 1(1). “evrimii” <https://doi.org/10.1162/99608f92.8cd550d1>, Eriřim: 09.07.2025.

Foos, F. (2024). The use of AI by election campaigns. LSE Public Policy Review, 3(3)
“evrimii” <https://doi.org/10.31389/lseppr.112> Eriřim:12.07.2025.

FORD, R. & GOODWIN, M. (2014). *Revolt on the Right: Explaining Support for the Radical Right in Britain*. London: Routledge, ss. 130–142.

Gabelein, Bundeswehr Office for Defence Planning. (2022). “Multi-Domain Operations for the Bundeswehr: Developing an approach for the Bundeswehr (Brochure). Bundeswehr”. “Çevrimiçi”
<https://www.bundeswehr.de/resource/blob/5753432/11123cfdc6a7117559625ae08cec7b31/brochuere-engl-data.pdf>, Erişim: 01/08/2025.

Gillespie, T. (2018). “Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media”. Yale University Press.

GOODWIN, M. & HEATH, O. (2016). “Brexit Vote Explained: Poverty, Low Skills and Lack of Opportunities”. Joseph Rowntree Foundation, ss. 78–82.
"Çevrimiçi" <https://www.jrf.org.uk/report/brexit-vote-explained-poverty-low-skills-and-lack-opportunities> Erişim: 05.08.2025

Goodfellow, I., Bengio, Y., & Courville, A. (2016) “Deep learning”, MIT Press.

GONZALEZ FUSTER, G. (2014). *The Emergence of Personal Data Protection as a Fundamental Right of the EU*. Cham, Springer, ss. 85.

GORWA, R. (2019). “The Platform Governance Triangle: Conceptualising the Role of Social Media Platforms in Democratic Politics”. *Internet Policy Review*, Vol. 8, No. 2, ss. 90.

GRAHAM, J. (2019). “Brexit: The Uncivil War” [Film Script]. London: Faber & Faber, ss. 12–14.

Green, J. & Issenberg, S. (2021) “The Rise of Artificial Intelligence in Global Politics” Oxford: Oxford University Press, ss. 14.

Greenwald, G. (2014). “No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State”. Metropolitan Books.

Gstrein, O. J., et al. (2024). “European AI Regulation: Brussels Effect versus Human Dignity”. “Çevrimiçi”

https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4214358,

Erişim:02/08/2025.

HALL, S. (2020). “Brexit and Contemporary British Fiction”. Literature & Politics, Manchester: Manchester University Press, Vol. 12, No. 2, ss. 88.

HELMUS, T. & BODINE-BARON, E. (2020). “Russian Social Media Influence: Understanding the Cambridge Analytica Effect”. RAND Corporation, ss. 59.

“Çevrimiçi” https://www.rand.org/pubs/research_reports/RR3160.html

Erişim: 12.07.2025

HERNÁNDEZ, M. (2024). “Avrupa Birliği’nin Yapay Zeka Düzenlemeleri ve LAC Bölgesi” içinde Yapay Zeka ve Diplomasi Raporu, SELA Yayını, ss. 53–58.

Herrera, G. L. (2024). “Artificial intelligence and diplomacy International relations in the era of disruptive technologies”. SELA. “Çevrimiçi”

<https://www.sela.org/en/publicaciones/ai-and-diplomacy-international-relations-in-the-era-of-disruptive-technologies/> Erişim: 02.08.2025

Hobsbawm, E. J. (1994). “Age of extremes: The short twentieth century”, 1914–1991. London: Michael Joseph.

HOLSTI, K. J. (1992). International Politics: A Framework for Analysis, 5th Edition, New Jersey, Prentice Hall.

Horowitz, M. C. (2018) “Artificial intelligence, international competition, and the balance of power” Texas National Security Review, 1(3), 36–57 “Çevrimiçi”

<https://tnsr.org/2018/05/artificial-intelligence-international-competition-and-the-balance-of-power/> Erişim:12.08.2025.

Howard, P. N., & Kollanyi, B. (2016) ‘Bots, StrongerIn, and Brexit: Computational propaganda during the UK-EU referendum. Social Science Computer Review’,

36(4), ss. 385-401, “Çevrimiçi” <https://doi.org/10.1177/0894439317717254>, Erişim: 10/06/2025.

Howard, P. N. (2013) “Democracy’s Fourth Wave? Digital Media and the Arab Spring” Oxford: Oxford University Press, ss. 45–55.

Hu, M. (2020). “The limits of the FTC’s authority to police privacy violations”. Harvard Journal of Law & Technology, 33(1), 100–130.

Hu, M. (2020). “Cambridge Analytica’s Black Box: Process accountability in data breach governance”. Big Data & Society, 7(2), 100–117. “Çevrimiçi” <https://doi.org/10.1177/2053951720938091>, Erişim: 02/05/2025.

Hughes, A., & Dahlström, M. (2020). “AI Steve: Exploring AI avatars in political campaigns” Journal of Political Innovation, 5(2), 120–135.

Human Rights Watch. (2024, Eylül 10). “Gaza: İsrail ordusunun dijital araçları sivil zarar riskini artırıyor”. “Çevrimiçi” <https://www.hrw.org/news/2024/09/10/gaza-israeli-militarys-digital-tools-risk-civilian-harm>, Erişim: 02/08/2025.

Israel Aerospace Industries (IAI). (t.y.). “Harop - Advanced loitering munition system”. “Çevrimiçi” <https://www.iai.co.il/p/harop>, Erişim: 05/06/2025.

ICO (2018). “Investigation into the use of data analytics in political campaigns”, Information Commissioner’s Office, July 2018, ss. 24–25. “Çevrimiçi” <https://ico.org.uk/media/action-weve-taken/2259369/investigation-into-data-analytics-20180703.pdf>, Erişim: 20/08/2025.

ICO (2019). “Monetary penalty notice: SCL Elections Ltd”, Information Commissioner’s Office, 2019, ss. 22–24. “Çevrimiçi” <https://ico.org.uk/media/action-weve-taken/mpns/2615150/scl-elections-mpn-20191024.pdf>, Erişim: 21/08/2025.

Ienca, M., & Andorno, R. (2017). “Towards new human rights in the age of neuroscience and AI”. *Life Sciences, Society and Policy*, 13(5).

Information Commissioner’s Office. (2018, November). “Investigation into the use of data analytics in political campaigns (Final report)”. “Çevrimiçi”
<https://ico.org.uk/media2/migrated/2260271/investigation-into-the-use-of-data-analytics-in-political-campaigns-final-20181105>, Erişim: 02/08/2025.

INSOLVENCY SERVICE (2020). “Former director of Cambridge Analytica disqualified” Press Release, 24 September 2020. Çevrimiçi:
<https://www.gov.uk/government/news/former-director-of-cambridge-analytica-disqualified> Erişim: 12.08.2025.

ISAAC, J. & HANNA, M. (2018). “User Data Privacy and the Cambridge Analytica Scandal”. *Computer Law & Security Review*, Vol. 34, No. 3, ss. 124.

JACKSON, D. & GREEN, J. (2019). “Brexit and Social Media: Hashtags, Campaigns and Digital Activism”. *Political Communication*, Vol. 36, No. 2, ss. 56.

JARRÍN, A. (2024). “Artificial Intelligence and Diplomacy: International Relations in the Era of Disruptive Technologies” içinde Yapay Zeka ve Diplomasi Raporu, SELA Yayını, ss. 18.

Jobin, A., Ienca, M., & Vayena, E. (2019). “The global landscape of AI ethics guidelines” *Nature Machine Intelligence*, 1(9), 389–399.

JOHN, P., JENNINGS, W. & McLAREN, L. (2020). “British Election Study (BES) and the Role of Social Media in the Brexit Referendum”, *Journal of Elections, Public Opinion and Parties*, Cilt 30, Sayı 2, ss. 112–117.

Johnson, B., & Verdicchio, M. (2017). “AI, ethics, and the future of political campaigning”. *AI & Society*, 32(3), 361–370.

Joint Select Committee on Foreign Interference through Social Media. (2020). “Report on foreign interference through social media”. Law Council of Australia.

“Çevrimiçi” <https://lawcouncil.au/publicassets/3f5463be-579a-ea11-9434-005056be13b5/3796%20-%20Joint%20Select%20Committee%20on%20Foreign%20Interference%20through.pdf> Erişim: 05.10.2025.

Kafkasyalı, A. & Oğuzhan, M. (2025) “Dijital Hegemonya: Yapay Zeka, Veri ve Uluslararası İlişkiler” Ankara: Nobel Yayınları, ss. 55–57.

Kalin, I. (2019). “Siber Güvenlik ve Uluslararası İlişkilerde Yeni Tehditler.” İstanbul: SETA Yayınları, ss. 58.

Kanat, S., & Akoğuz, H. (2023). “Küresel eşitsizlikler ve yapay zeka teknolojilerinin etkileri” Uluslararası İlişkiler ve Yapay Zeka. Çevrimiçi: <https://dergipark.org.tr/tr/download/article-file/3983565> Erişim: 02/07/2025

KAPLAN, A. (2021). “Social Media Algorithms and the Polarisation of Public Debate”. Media, Culture & Society, Vol. 43, No. 5, ss. 102.

KAUFMANN, E. (2018). “Whiteshift: Populism, Immigration and the Future of White Majorities” London: Allen Lane, ss. 29–37.

Kello, L. (2017). “The virtual weapon and international order” Yale University Press.

KERR, D. (2019). “Brexit on Stage: Shakespeare and Political Theatre in Britain”. Shakespeare Bulletin, Vol. 37, No. 1, ss. 43.

KIRKPATRICK, D. (2019). “The Cambridge Analytica Files”. New York: The New York Times, ss. 78.

Khalil, L. (2024). “Overcoming digital threats to democracy”. Lowy Institute. “Çevrimiçi” <https://www.lowyinstitute.org/publications/overcoming-digital-threats-democracy> Erişim: 05/10/2025.

Khan, R. (2023). “Artificial Intelligence and Global Governance: Opportunities and Challenges.” London: Routledge, ss. 23.

- Khan, S. (2021). “Emotional framing and political persuasion: Brexit campaign case study”. *Journal of Political Communication*, 38(3), ss. 198-215, “Çevrimiçi” <https://doi.org/10.1080/10584609.2021.1875234>, Erişim: 10/05/2025.
- Kogan, A. (2014). “GSR and Psychometrics in Digital Behavior Research”. Cambridge University.
- Korkusuz, M. H., & Kutluk, E. (Eds.). (2023). “Siyaset, kamu yönetimi ve uluslararası ilişkiler bağlamında yapay zeka tartışmaları”. Ekin Yayınları.
- Kosinski, M., Matz, S. C., Gosling, S. D., Popov, V., & Stillwell, D. (2015) “Facebook as a personality test: Using social media to predict personality”, *Journal of Research in Personality*, ss. 58, 39–45, “Çevrimiçi” <https://doi.org/10.1016/j.jrp.2015.05.003>, Erişim: 09/05/2025.
- Kosinski, M., Stillwell, D., & Graepel, T. (2013) ‘Private traits and attributes are predictable from digital records of human behavior’, *Proceedings of the National Academy of Sciences*, 110(15), ss. 5802–5805, ‘Çevrimiçi’ <https://doi.org/10.1073/pnas.1218772110> Erişim: 08/05/2025.
- Koubi, V. (2019). “Climate change and conflict”. *Annual Review of Political Science*, 22, 343–360. “Çevrimiçi” <https://ssrn.com/abstract=3394063>, Erişim: 04/06/2025.
- Krauss, R. & Wang, Y. (2022). “Artificial Intelligence and Foreign Policy: Strategic Applications in China” *Journal of Contemporary International Affairs*, 8(2), ss. 134-136.
- KROLL, J. A., et al. (2017). “Accountable algorithms” *University of Pennsylvania Law Review*, 165(3), 633–705.
- Kshetri, N. (2020). “Blockchain’s roles in strengthening cybersecurity and protecting digital democracy”. *Journal of Cybersecurity*, 6(1), 112–115.

- Kumar, A., et al. (2018). “Comparative evaluation of instrument segmentation and tracking methods in minimally invasive surgery”. Proceedings of the International Conference on Medical Image Computing and Computer-Assisted Intervention (MICCAI), 21, 1–9.
- Kuner, C. (2017). The General Data Protection Regulation: A Commentary. Oxford University Press.
- Kurnaz, A., & Ünver, H. A. (2025). “Büyük dil modelleriyle diplomatik metin analizi: Hesaplamalı sosyal bilimlerde hibrit bir yaklaşım”. İletişim ve Diplomasi, 4(1), 1–15.
- Latonero, M. (2018). “Governing Artificial Intelligence: Upholding Human Rights & Dignity”, Data & Society.
- Lempert, R. J. (2019). “Strategic foresight in public policy: Using models to anticipate risks and uncertainties”. Routledge.
- Lyon, D. (2018). “The culture of surveillance: Watching as a way of life”. Polity Press.
- MARGETTS, H., & Dorobantu, C. (2019). “Rethinking public administration in the digital age” Public Administration Review, 79(4), 609–619.
- MARWICK, A. & LEWIS, R. (2017). “Media Manipulation and Disinformation Online”. Data & Society Research Institute, ss. 135. “Çevrimiçi” <https://datasociety.net/library/media-manipulation-and-disinfo>, Erişim: 14/07/2025
- Marx, K. (1867). “Kapital: Politik iktisadın eleştirisi”, (A. Bilgi, Çev.). İstanbul: Erişim Yayınları. (Orijinal eser 1867'de yayımlanmıştır). “Çevrimiçi” <https://www.marxists.org/turkce/m-e/kapital/kapital1>, Erişim: 10/07/2025.
- MATZ, S. C., KOSINSKI, M., NAVE, G. & STILLWELL, D. J. (2017). “Psychological Targeting as an Effective Approach to Digital Mass Persuasion”. PNAS, 114(48), ss. 3.

MCINTYRE, L. (2018). Post-Truth. Cambridge, MA: MIT Press, ss. 10.

McKinsey & Company. (2022). “The CHIPS and Science Act: Implications for U.S. Competitiveness” New York: McKinsey & Company, ss. 4. “Çevrimiçi” <https://www.mckinsey.com/industries/semiconductors/our-insights/the-chips-and-science-act> Erişim: 20/07/2025.

Meleouni, C., & Efthymiou, I. P. (2023). “Artificial intelligence and its impact in international relations”. Journal of Politics and Ethics in New Technologies and AI, 2(1), 1–18. “Çevrimiçi” <https://doi.org/10.12681/jpentai.35803> Erişim: 05/10/2025.

MENON, A. & SALTER, J. (2016). “Brexit: Initial Reflections”. International Affairs, Vol. 92, No. 6, ss. 94–102.

Microsoft. (2025). “Diella projesi: Kamu hizmetlerinde yapay zeka uygulamaları”. Redmond.

Miller, J. H., & Törnberg, P. (2023). “The Social Science of Complexity”. In Seeing Like a Platform (pp. 21–42). Routledge.

Mittelstadt, B., Allo, P., Taddeo, M., Wachter, S., & Floridi, L. (2016). “The ethics of algorithms: Mapping the debate” Big Data & Society, 3(2), 1–21, “Çevrimiçi” <https://doi.org/10.1177/2053951716679679>, Erişim: 28/08/2025

Mobilio, S. (2024). “GenAI in the 2024 Taiwan Presidential Election: Lessons for Democracies” Cyber Defense Review, 9(3), 52–53, “Çevrimiçi” https://cyberdefensereview.army.mil/Portals/6/Documents/2024-Fall/Mobilio_CDRV9N3-Fall-2024.pdf, Erişim: 20/09/2025

Mohamed, S., Png, M. T., & Isaac, W. (2020). “Decolonial AI: Decoloniality and AI” Futures, 117, 102507, “Çevrimiçi” <https://doi.org/10.1016/j.futures.2020.102507>, Erişim: 02/10/2025

- Morales Lama, M. (2023). AI in diplomacy: Personalized content and engagement strategies. *Diplomatic Review*, 18(1), 7–15.
- MUELLER, R. (2019). “The Mueller Report”. Washington DC: U.S. Department of Justice, ss. 154 “Çevrimiçi” <https://www.justice.gov/storage/report.pdf>, Erişim: 05/07/2025
- National Science Foundation (NSF). (2022). “CHIPS and Science Act of 2022: Strengthening America’s STEM Workforce” Washington, DC: NSF, ss. 6. “Çevrimiçi” <https://new.nsf.gov/funding/initiatives/chips>, Erişim: 19/08/2025.
- National Cyber Security Centre. (2023). “NCSC Yıllık Raporu 2023”. “Çevrimiçi” https://www.ncsc.gov.uk/files/Annual_Review_2023, Erişim: 24/08/2025.
- NATO (2022). “NATO’s Artificial Intelligence Strategy” Çevrimiçi: https://www.nato.int/cps/en/natohq/official_texts_187617.htm, Erişim: 10/07/2025.
- Ndzendze, B. & Marwala, T. (2023). “Artificial Intelligence and Global Security: Emerging Patterns in International Relations”, Johannesburg: Wits University Press, ss. 58.
- NEOM. (t.y.). “Changing the future of Technology & Digital”. NEOM. “Çevrimiçi” <https://www.neom.com/en-us/our-business/sectors/technology-and-digital>, Erişim: 02/09/2025.
- Nguyen-Duc, A., Khanna, D., Greer, D., Wang, X., Zaina, L. M., Matturro, G., Melegati, J., Guerra, E., Le, G. H., Kettunen, P., Hyrynsalmi, S., Edison, H., Sales, A., Aldaej, A., Mikkonen, T., Garbajosa, J., & Abrahamsson, P. (2022). “Work-from-home and its implication for project management, resilience and innovation: A global survey on software companies”. “Çevrimiçi” <https://doi.org/10.48550/arXiv.2202.04950>, Erişim: 04/08/2025.
- Nguyen, T., Smith, J., & Lee, H. (2018) “Real-time sentiment analysis for political campaigns on social media. *Social Network Analysis and Mining*”, 8(5), ss.

145-160, “Çevrimiçi” <https://doi.org/10.1007/s13278-018-0534-6>, Erişim: 20/04/2025.

Nguyen, T. T., Ngo, Q. D., & Park, Y. (2020) “Deep learning-based phishing detection: A survey. Electronics”, 9(10), 1664, “Çevrimiçi” <https://doi.org/10.3390/electronics9101664>, Erişim: 04/02/2025.

Nix, A. (2018). Cambridge Analytica and the 2016 election: Testimony before the UK Parliament.

Nye, J. S. (2011). The future of power. New York: PublicAffairs.

OECD. (2021). “Artificial intelligence in public services: Enhancing efficiency and citizen engagement”. Paris.

OECD (2021). “Digital Government Index 2021” Çevrimiçi: <https://www.oecd.org/gov/digital-government/digital-government-index-2021.htm>, Erişim: 20/08/2025.

O’Neil, C. (2016). “Weapons of math destruction: How big data increases inequality and threatens democracy” Crown Publishing.

ONS (2017). “Regional labour market statistics in the UK: August 2017”, Office for National Statistics, 16 August 2017, “Çevrimiçi” <https://www.ons.gov.uk/employmentandlabourmarket/peopleinwork/employmentandemployeetypes/bulletins/regionallabourmarket/august2017>, Erişim: 18/08/2025.

ONS (2017). “Annual Population Survey: Labour market status by age – North West and North East”, Nomis/Office for National Statistics, “Çevrimiçi” <https://www.nomisweb.co.uk/datasets/aps170> Erişim: 18/08/2025.

Öztemel, E. (2020). “Yapay zeka ve insanlığın geleceği”. In M. Şeker, Y. Bulduklu, C. Korkut, & M. Doğrul (Eds.), Bilişim teknolojileri ve iletişim: Birey ve toplum güvenliği (ss. 90 - 111). Türkiye Bilimler Akademisi.

- Parlak, B., Doğan, K.C. (2019) “E-Yönetişim: Kuramsal Bir Analiz. B. Parlak ve K.C. Doğan”. (Eds.). E-Yönetişim. İstanbul: Beta Yayıncılık, 7-18.
- Public Sector AI Review. (2022). “Caddy: AI chatbots in public service”. London.
- Pasquale, F. (2015) “The Black Box Society: The Secret Algorithms That Control Money and Information”, Harvard University Press.
- Perez, M. & Lee, C. (2024). “AI for Global Cooperation: Tackling Climate, Pandemic and Economic Crises.” New York: Springer, ss. 30.
- PERKINS, R. (2019). “Post-Truth Politics and Media Narratives”. European Journal of Communication, Vol. 34, No. 1, ss. 44.
- Pomerantsev, P. (2019). “This Is Not Propaganda: Adventures in the War Against Reality”. Faber & Faber.
- PORTES, J. (2016). “How the regions voted, and why”, National Institute of Economic and Social Research (NIESR) Blog, 5 July 2016, “Çevrimiçi” <https://www.niesr.ac.uk/blog/how-regions-voted-and-why>, Erişim: 21/09/2025.
- Qure.ai. (2024). “How AI is Turning the Tide Against Tuberculosis in South Africa”. Qure.ai. “Çevrimiçi” https://www.qure.ai/impact_stories/how-ai-is-turning-the-tide-against-tuberculosis-in-south-africa?utm_source, Erişim: 14/08/2025.
- Qure.ai & KwaZulu-Natal Sağlık Departmanı. (2023). “Transforming South Africa's TB Care Landscape with AI2”. Qure.ai. “Çevrimiçi” https://www.qure.ai/insights/transforming-south-africas-tb-care-landscape-with-ai?utm_source, Erişim: 14/08/2025.
- RASMUSSEN, R. (2018). “Brexit and the Uses of Shakespeare”. Shakespeare Survey, Vol. 71, ss. 92–95.
- Reuters. (2025, 8 Nisan). “Taiwan says China using generative AI to ramp up disinformation and 'divide' the island”. Reuters. “Çevrimiçi” <https://www.reuters.com/world/asia-pacific/taiwan-says-china-using->

[generative-ai-ramp-up-disinformation-divide-island-2025-04-08/](https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/sovereign-remedies-between-ai-autonomy-and-control/),

Eriřim:04/1072025.

Ray, Trisha. (2025, Nisan 3). Sovereign Remedies: Between AI Autonomy and Control.

Atlantic Council, GeoTech Center. “Çevrimiçi”

<https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/sovereign-remedies-between-ai-autonomy-and-control/>,

Eriřim:02/05/2025.

Rid, T. (2021). “Active measures: The secret history of disinformation and political warfare” Farrar, Straus and Giroux.

RODRIK, D. (2018). “Populism and the Economics of Globalization”. Journal of International Business Policy, Vol. 1, No. 1, ss. 76–88.

Roxburgh, C., & Warnes, M. (2019) ‘Algorithmic Diplomacy: AI in International Relations. Ethics and International Affairs’, 33(1), ss. 127-140.

Russell, S., & Norvig, P. (2021). “Artificial Intelligence: A Modern Approach” (4th ed.). Pearson.

SADD, C. (2019). “Brexit and the Politics of Data: A Cinematic Perspective”. Film & Politics Review, Vol. 4, No. 2, ss. 43–45.

Schneider, J., & Lucas, G. R. (2020). Ethics of Autonomous Weapons Systems. Philosophy & Technology, 33(1), 45–63.

SELA (2024) “Yapay Zeka ve Diplomasi: Yıkıcı Teknolojiler Çağında Uluslararası İliřkiler (Artificial Intelligence and Diplomacy: International Relations in the Era of Disruptive Technologies)”, Latin American and Caribbean Economic System (SELA), Rapor. “Çevrimiçi” <https://www.sela.org/>, Eriřim: 02/09/2025.

- Sernani, P., Cossiri, A., Di Cosimo, G., & Frontoni, E. (2025). “Analyzing digital political campaigning through machine learning”: An exploratory study for the Italian campaign for European Union Parliament election in 2024.
- Shakespeare’s Globe. (2019, February 28). “Making sense of history: Adjoa Andoh and Lynette Linton on Richard II”. Medium, “Çevrimiçi”
<https://medium.com/@shakespearesglobe/making-sense-of-history-3ccaffee1920>, Erişim: 04/10/2025.
- Shannon, C. E. (1950). “ Programming a computer for playing chess”. Philosophical Magazine, 41(314), 256–275.
- SHIPMAN, T. (2016). “All Out War: The Full Story of How Brexit Sank Britain’s Political Class”. London: William Collins, ss. 157.
- Singer, P. W. (2019). “LikeWar: The weaponization of social media.” Houghton Mifflin Harcourt.
- Solove, D. J. (2021). “Understanding Privacy” (2nd ed.). Harvard University Press.
- Smite, D., Moe, N. B., Hildrum, J., Gonzalez Huerta, J., & Mendez, D. (2022). “Work-from-home is here to stay: Call for flexibility in post-pandemic work policies”. “Çevrimiçi” <https://doi.org/10.48550/arXiv.2203.11136>, Erişim: 08/07/2025.
- Smith, A. (2016). Autumn. London: Hamish Hamilton.
- SMITH, A., (2020) Milletlerin Zenginliği, Çev. Prof. Dr. Mustafa Acar, İstanbul, Liberus Yayınevi.
- SMITH, J. & ADAMS, P. (2020). “Digital Democracy and Electoral Manipulation in Canada”. Canadian Journal of Political Science, Vol. 53, No. 1, ss. 67.
- Sommer, R., & Paxson, V. (2010). “Outside the closed world: On using machine learning for network intrusion detection”. 2010 IEEE Symposium on Security and Privacy, ss. 305–316, “Çevrimiçi” <https://doi.org/10.1109/SP.2010.25>, Erişim: 20/01/2025.

- Spazian, A., Holland Michel, A., & Anand, A. (2021). “UNIDIR on Lethal Autonomous Weapons: Mapping Our Research to the Discussions of the GGE on LAWS.” Geneva: UNIDIR. “Çevrimiçi”: <https://unidir.org/wp-content/uploads/2023/05/UNIDIR-on-Lethal-Autonomous-Weapons-Final.pdf> Erişim: 18/07/2025.
- Spazian, A., Anand, A., & Persi Paoli, G. (2021). “Table-Top Exercises on the Human Element and Autonomous Weapons Systems: Summary Report.” Geneva: UNIDIR. “Çevrimiçi” <https://unidir.org/wp-content/uploads/2023/05/Table-Top-Exercises-on-the-Human-Element-and-Autonomous-Weapons-Systems-Summary-Report-UNIDIR-Final.pdf>, Erişim: 20/08/2025.
- ST JOHN, G., (2008) “Victor Turner and Contemporary Cultural Performance: An Introduction”, “Çevrimiçi” [Victor20Turner20and20Contemporary20Cultural20Performance20-20An20Introduction20by20Graham20St20John202008.pdf](https://unidir.org/wp-content/uploads/2023/05/Victor20Turner20and20Contemporary20Cultural20Performance20-20An20Introduction20by20Graham20St20John202008.pdf), Erişim: 05/10/2025.
- SUADA, M., LEE, C. & KIM, H. (2024). “Digital Propaganda and Brexit: Cambridge Analytica Revisited”. Journal of Political Communication Studies, Vol. 12, No. 2, ss. 106.
- SUNSTEIN, C. (2017). “#Republic: Divided Democracy in the Age of Social Media”. Princeton: Princeton University Press, ss. 45–53.
- Sutherland, J. (2019) “Psychometrics, microtargeting, and political campaigns: An ethical analysis”. Ethics and Information Technology, 21(2), ss. 123-135, “Çevrimiçi” <https://doi.org/10.1007/s10676-019-09500-9>, Erişim: 03/12/2024.
- Şafak Etike (2023) “Yapay Zeka ve Haber Üretim Süreci: Tanımlar ve Uygulamalar”, Bozok Üniversitesi.

- Tallberg, J., Sommerer, T., Jönsson, C., & Scholte, J. (2023). “Global governance and AI: Ethical and legal challenges” International Studies Review, 25(3), viad040. “Çevrimiçi” <https://doi.org/10.1093/isr/viad040>, Erişim: 29/09/2025
- TAYLOR, R. & MACMILLAN, H. (2019) “Brexit Diary Project: Micro-targeting and Voter Perceptions”, ESRC Research Paper, ss. 45–60.
- Tetlow, G., & Pope, T. (2020) “Digital campaigns and democratic governance: The case of Brexit. Journal of Information Technology & Politics”, 17(1), ss. 20-35, “Çevrimiçi” <https://doi.org/10.1080/19331681.2020.1712132>, Erişim: 12/04/2025.
- THE GUARDIAN (2019). “Cambridge Analytica fined for failing to disclose data”, The Guardian, 24 January 2019 “Çevrimiçi” <https://www.theguardian.com/technology/2019/jan/24/cambridge-analytica-fined-data>, Erişim: 15/08/2025.
- THE GREAT HACK (2019). “The Great Hack” [Film]. Directors: Karim Amer & Jehane Noujaim, Netflix, 01:25:10.
- The Great Hack (2019). Yönetmen: Karim Amer & Jehane Noujaim. Netflix. [00:12:45; 01:02:30; 01:25:10]. TÜFEKÇİ, Z. (2015). “Algorithmic Harms Beyond Facebook and Google: Emergent Challenges of Computational Agency”. Colorado Technology Law Journal, Vol. 13, No. 1, ss. 34–89.
- Time. (2022, Ekim 5). “The Chips That Make Taiwan the Center of the World”. “Çevrimiçi” <https://time.com/6219318/tsmc-taiwan-the-center-of-the-world/>, Erişim: 05/10/2025.
- Tıgılı, E. (2021). Kitap İncelemesi: Branko Milanovic, “Küresel Eşitsizlik: Küreselleşme Çağı İçin Yeni Bir Yaklaşım”. Bilge Uluslararası Sosyal Araştırmalar Dergisi, 5(1): 52-58.
- Trades Union Congress. (2025, 27 Ağustos). “TUC calls for “step change” in UK approach to AI as poll finds majority of public are concerned over jobs”.

- “Çevrimiçi” <https://www.tuc.org.uk/news/tuc-calls-step-change-uk-approach-ai-poll-finds-majority-public-are-concerned-over-jobs>, Erişim:05/06/2025.
- Trellix. (2025). “The CyberThreat Report: April 2025”. Trellix Advanced Research Center. “Çevrimiçi” <https://www.trellix.com/advanced-research-center/threat-reports/april-2025/>, Erişim: 02/08/2025.
- Trellix. (2024). “The CyberThreat Report: November 2024”. Trellix Advanced Research Center. “Çevrimiçi” <https://www.trellix.com/advanced-research-center/threat-reports/november-2024/>, Erişim: 02/08/2025.
- Tsygankov, A. (2020) “Russia and the West in the Era of Digital Rivalry”, London: Routledge, ss. 102–118.
- Turing, A. M. (1950). “Computing machinery and intelligence”. Mind, 59(236), 433 - 460. “Çevrimiçi” <https://doi.org/10.1093/mind/LIX.236.433>, Erişim:02/05/2025.
- TURNER, J. (2021). “Brexit and Theatre: Performing Political Division”. Contemporary Theatre Review, Vol. 31, No. 2, ss. 67
- Tufekci, Z. (2015) “Algorithmic Harms Beyond Facebook and Google: Emergent Challenges of Computational Agency”, Colorado Technology Law Journal, 13, ss. 203-218.
- TUFEKCI, Z. (2018). “Twitter and Tear Gas: The Power and Fragility of Networked Protest” New Haven, Yale University Press, ss. 94.
- TUFEKCI, Z. (2018, 10 Mart). YouTube, the great radicalizer. The New York Times Magazine“Çevrimiçi”<https://www.nytimes.com/e-the-great-radicalizer.html>, Erişim: 20/07/2025.
- UBEROI, E. (2016) “Analysis of the EU Referendum results 2016”, House of Commons Library Briefing Paper Number CBP 7639, 29 June 2016, ss. 24.

“Çevrimiçi” <https://commonslibrary.parliament.uk/research-briefings/cbp-7639/>, Erişim: 21/09/2025.

UK AI Council. (2025, July 14). “UK launches open-source AI fellowship to boost public sector innovation”. London. “Çevrimiçi” <https://ukai.co/uk-launches-open-source-ai-fellowship-to-boost-public-sector-innovation>, Erişim: 05/06/2025.

UK DATA SERVICE (2023) “British Election Study Internet Panel Waves 1–24, “Çevrimiçi” <https://beta.ukdataservice.ac.uk/datacatalogue/series/series?id=200010>, Erişim: 21/09/2025.

UK Government Digital Service. (2023). “Humphrey: AI tools for public document analysis”. London.

UK Parliament. (2020). “Brexit: The EU Data Protection Package” ss. 15 - 17. UK Parliament.

UK PARLIAMENT (2019). “Disinformation and ‘fake news’: Final Report, Eighth Report of Session 2017–19”, Digital, Culture, Media and Sport Committee, House of Commons, 18 February 2019. “Çevrimiçi” https://publications.parliament.uk/pa/cm201719/cmselect/cmcmums/1791/1791_1, Erişim: 20/08/2025.

UK Government Digital Service. (2021). “AI Playbook and ethical AI guidelines”. London “Çevrimiçi” <https://www.gov.uk/government/publications/ai-playbook> Erişim: 15/08/2025.

Uluç C., Eyüpoğlu C., (2025), “GÜVENLİK VE TEKNİK İSTİHBARATTA YAPAY ZEKA”, İstanbul Ticaret Üniversitesi Teknoloji ve Uygulamalı Bilimler Dergisi, Cilt 8, No 1, s. 169-183 DOI: 10.56809/icujtas.1638325.

United Nations. (2022). “Harnessing Artificial Intelligence for Sustainable Development”. United Nations Publications.

UN Secretary-General. (2020). “Roadmap for Digital Cooperation”. United Nations.

“Çevrimiçi” <https://www.un.org/en/content/digital-cooperation-roadmap/>,

Erişim: 02/06/2025.

UNESCO (2021). “UNESCO Recommendation on the Ethics of Artificial

Intelligence”, “Çevrimiçi”

<https://unesdoc.unesco.org/ark:/48223/pf0000381137>, Erişim: 18/08/2025.

United Nations (2015). “Transforming our world: the 2030 Agenda for Sustainable

Development” “Çevrimiçi” <https://sdgs.un.org/2030agenda>, Erişim:

16/07/2025.

Uzun, A. (2019). “Dijital Çağda E-Yönetişim: Konsept, Pratik Ve Gelişim”. B. Parlak

ve K.C. Doğan. (Eds.). E-Yönetişim. İstanbul: Beta Yayıncılık, 33-55.

Ünver, H. A. (2018). “Digital diplomacy in the age of Twitter: A comparative analysis

of the digital diplomacy practices of Turkey, the US and Russia”. Turkish

Policy Quarterly, 17(3), 121–134.

Vaccari, C., & Chadwick, A. (2020). “Deepfakes and disinformation: Exploring the

impact of synthetic political video on online misinformation”. Social Media +

Society, 6(1), 1–13. “Çevrimiçi” <https://doi.org/10.1177/2056305120903408> ,

Erişim: 14/08/2025.

Varnalı, T. (2025). “Türkiye’de E-Belediyecilik: Yerel Yönetimlerin Dijitalleşme Yolu

ve Uygulama Analizi”. International Anatolia Academic Online Journal Social

Sciences Journal, 11(1), 237-259.

Voigt, P. & Von dem Bussche, A. (2017). The EU General Data Protection Regulation

(GDPR): A Practical Guide. Cham, Springer, ss. 134–136 “Çevrimiçi”

<https://doi.org/10.1007/978-3-319-57959-7>, Erişim: 20/07/2025.

Von der Leyen, U. (2020). “Shaping Europe’s Digital Future. European Commission”.

“Çevrimiçi” Shaping Europe’s Digital Future – European Commission,

Erişim: 18.07.2025

- Webb, M. (2019). “The impact of artificial intelligence on international affairs”
International Affairs, 95(6), 1399–1420. “Çevrimiçi”
<https://doi.org/10.1093/ia/iiz256>, Erişim: 19/07/2025.
- Weber, J. & Sharkey, N. (2020) “AI and Security: The Role of Deep Learning in
Military Intelligence”, Journal of Strategic Studies, Vol. 43, No. 2, ss. 243.
- Weiss, T. G. (2019). “What’s Wrong with the United Nations and How to Fix It”.
Polity Press.
- West, D. M. (2018). “The Future of Work: Robots, AI, and Automation”. Brookings
Institution Press.
- White House. (2022, Mayıs 4). “National Security Memorandum on Promoting United
States Leadership in Quantum Computing While Mitigating Risks to
Vulnerable Cryptographic Systems”. “Çevrimiçi”
<https://www.whitehouse.gov/wp-content/uploads/2022/05/NSM-10>,
Erişim:04/08/2025.
- Whittaker, M., Crawford, K., Dobbe, R., Fried, G., Kaziunas, E., Mathur, V., &
Schwartz, O. (2018). “AI now report 2018”. AI Now Institute. New York.
- Williams, H., & Burns, A. (2019) ‘Machine learning and voter persuasion: Techniques
and effects in Brexit campaigns’, Political Studies Review, 17(1), 78-90,
“Çevrimiçi” <https://doi.org/10.1177/1478929918821907> Erişim: 25/12/2024.
- WOOLLEY, S. & HOWARD, P. (2017). “Computational Propaganda Worldwide:
Executive Summary”. Oxford Internet Institute, ss. 22–23. “Çevrimiçi”
[https://comprop.oii.ox.ac.uk/research/working-papers/computational-
propaganda-worldwide-executive-summary/](https://comprop.oii.ox.ac.uk/research/working-papers/computational-propaganda-worldwide-executive-summary/), Erişim: 03/08/2025.
- World Economic Forum. (2016). “The future of jobs: Employment, skills and
workforce strategy for the fourth industrial revolution”. World Economic
Forum. “Çevrimiçi” http://www3.weforum.org/docs/WEF_Future_of_Jobs,
Erişim: 21/08/2025.

- Yang, G., & Qian, X. (2020). “Digital authoritarianism in China: Technological control and political stability”. *Journal of Contemporary China*, 29(124), 1–18.
- Yıldırım, A. (2019) “Yapay Zeka ve Küresel Siyaset” İstanbul: Beta Yayıncılık, ss. 56.
- Yılmazel, S. C. (2022). “Yapay zeka çağında diplomasi”. *Türk Dünyası Araştırmaları*, 132(260), 91–112. “Çevrimiçi” <https://doi.org/10.55773/tda.1153159>, Erişim: 10.08.2025.
- YOUGOV (2025). “Nine years after the EU referendum, where does public opinion stand on Brexit?”, YouGov “Çevrimiçi” <https://yougov.co.uk/politics/articles/52410-nine-years-after-the-eu-referendum-where-does-public-opinion-stand-on-brexit>, Erişim: 02/09/2025.
- Zetter, K. (2014). “Countdown to Zero Day: Stuxnet and the launch of the world’s first digital weapon”. New York: Crown Publishers.
- Zeytinli, F. E. (2025). “Dijitalleşme ve yapay zekanın kamu yönetimindeki dönüşüm etkileri”. *The Journal of Academic Social Science*, 4(166), 419–430. “Çevrimiçi” <https://doi.org/10.29228/ASOS.82428>, Erişim: 02/10/2025
- Zhang, Y., & Chen, L. (2023). “AI decision support in international security and crisis management. *Journal of Conflict Resolution*”, 67(1), 120–135.
- Zhou, L. & Roberts, M. (2021). “AI, Bias and Global Security Risks”, *International Security Review*, 12(3), ss. 99-100.
- ZUBOFF, S. (2019). “The Age of Surveillance Capitalism”. London: Profile Books, ss. 114.